Technical Panel
of the
Nebraska Information Technology Commission
Tuesday September 11, 2001 - 9:00 a.m.
Varner Hall - Board Room
38th and Holdrege, Lincoln, Nebraska

AGENDA

Meeting Documents:
Click the links in the agenda
or click here for all documents (.pdf file; 2 MB).

1. Roll Call and Meeting Notice

2. Public Comment

3. Approval of Minutes* - August 22, 2001

4. State Enterprise Architecture*

   Standards and Guidelines
   - Video Architecture - Video Standards
   - Hardware Architecture: Minimum Workstation Configuration Guidelines

   Resource Materials
   - Security Architecture: 1) IS Technical Staff Handbook; 2) Security Officer Instruction Guide; and 3) Computer User's Security Handbook

5. Project Reviews

   Discussion of Information Technology Infrastructure Fund Review Process (ITIF Statutes)

6. Regular Informational Items and Work Group Updates (as needed)

   - Wireless project
   - Network Architecture Work Group (NETCOM)
   - Security Architecture Work Group
   - Accessibility Architecture Work Group
   - E-Government Architecture Work Group
   - Video Standards Work Group

7. Other Business

8. Future Meeting Dates

   October 9, 2001, 9:00 a.m.
   October 23, 2001, 9:00 a.m.

9. Adjourn

* Denotes Action Items

NITC and Technical Panel Websites: http://www.nitc.state.ne.us/
Meeting notice posted to the NITC Website: 23 AUG 2001
Meeting notice posted to the Nebraska Public Meeting Calendar: 4 SEP 2001
Agenda posted to the NITC Website: 7 SEP 2001

Technical Panel
Nebraska Information Technology Commission
Wednesday August 22, 2001 - 9:00 a.m.
Varner Hall - Board Room
38th and Holdrege, Lincoln, Nebraska
PROPOSED MINUTES

MEMBERS PRESENT:

Bob Huber, Nebraska Educational Telecommunications Commission (alternate for Mike Beach)
Brenda Decker, Department of Administrative Services, State of Nebraska
Christy Horn, Compliance Officer, University of Nebraska-Lincoln
Steve Schafer, Chief Information Officer, State of Nebraska
Walter Weir, Chief Information Officer, University of Nebraska

OTHERS PRESENT:

Rick Golden, University of Nebraska
Ruth Michalecki, Network Reliability and Interoperability Council V, Federal Communications Commission
Tom Rolfes, Office of the CIO/NITC
Steve Henderson, Department of Administrative Services, State of Nebraska
Ron Bowmaster, Nebraska Intergovernmental Data Communications Advisory Council
Gene Hand, Public Service Commission
Wayne Fisher, Internet Specialist Distance Learning Planning, Department of Education

ROLL CALL AND MEETING NOTICE

The chair, Walter Weir, called the meeting to order at 9:05 a.m. Roll call was taken. Five members were present. A quorum existed to conduct official business. The meeting notice posted to the N.I.T.C. and Nebraska Public Meeting Calendar Web sites on August 2, 2001. The agenda was posted to the N.I.T.C. Website on August 17, 2001.

PUBLIC COMMENT

There was no public comment.

APPROVAL OF JULY 10, 2001 MINUTES

Mr. Schafer made the following corrections:

- Under Statewide Technology Plan's E-Government Architecture subsection, the second sentence should read, "A grant application will be submitted to the Government Technology Collaboration Fund to continue the work on E-Government".
- Under Updates. Change E-Government to E-Government Architecture.

Ms. Decker moved to approve the corrected minutes. Mr. Huber seconded the motion. Roll call vote: Huber-Yes, Decker-Yes, Horn-Yes, Schafer-Yes and Weir-Yes. Motion was carried by unanimous vote.

UPDATE ON LB 833 IMPLEMENTATION

Wayne Fisher, Internet Specialist Distance Learning Planning, Department of Education

Mr. Fisher distributed map indicating Nebraska's Educational Service Units and the Status of Distance Learning Sites. Two-thirds of state's schools have distance learning education sites. The list of schools without distance learning education sites was also provided. The bill has allocated $3 million for FY02 and FY03 – not to exceed $1.5 million per year of lottery monies. The Nebraska Department of Education is the fiscal agent. The draft of the

“ADDITIONS TO RULE 89 DUE TO LB 833” will be ready today to submit to the State Board of Education for review and approval at the next meeting. Districts without distance education will be requested to provide a letter of intent to participate in the process. After discussion the Technical Panel made the following recommendations and requests:

- The Technical Panel requested to be involved with the review of the RFP.
- The Technical Panel recommended including a statement referencing the State’s development of a migration strategy for the video standards.
- The Technical Panel requested a draft of the migration strategy for the next meeting.

FORMS FOR STATE AGENCIES REVISIONS - AGENCY COMPREHENSIVE INFORMATION TECHNOLOGY PLAN
Steve Schafer, Chief Information Officer, State of Nebraska

The Technical Panel made the following recommendations:

- Section 3.D Security. Enhance awareness of state agencies regarding the security architectures developed by the Technical Panel (are you aware of these, implementation plans, etc.)
- Section 3.F. Accessibility. Include the set of questions asked of federal agencies. Ms. Horn will send these to Mr. Becker.
- J.D. Edwards requirements. The question was raised as to whether these should be included in the document. Mr. Becker will follow-up with Mr. Conroy for his input and suggestion.

FORMS FOR STATE AGENCIES - PROJECT PROPOSAL FORM
Steve Schafer, Chief Information Officer, State of Nebraska

The Technical Panel made no changes or recommendation to the document.

STATE ENTERPRISE ARCHITECTURE - Status Report

Accessibility Architecture:
The Accessibility Checklists will be an appendix to the policy. The following changes and/or additions were made to the Accessibility Policy:

- Sections C.6.a. and C.7.3. - delete the questions marks
- Section F.3 - insert information from Mark Schultz regarding the Assistive Technology Partnership.

Mr. Schafer moved to approve the draft guidelines with the suggested changes to be posted for a 30-day public comment period. Ms. Horn seconded the motion. Roll call vote: Weir-Yes, Schafer-Yes, Horn-Yes, Decker-Yes, and Huber-Yes. Motion was carried by unanimous vote.

Mr. Schafer suggested the development of a training CD would be beneficial for training agencies. It could be a grant project for submission to the Government Technology Collaboration Fund.

Network Architecture: Cabling Guidelines
Ron Bowmaster, NIDCAC

Mr. Bowmaster, in conjunction with the Division of Communications and Information Management Systems, developed the guidelines. Members expressed a concern in regards to setting 5e, as the minimum standard.Ms. Decker offered to have Dave Keele, Field Services Manager of the Division of Communications, further develop the document for review by the Technical Panel at the next meeting.

*Hardware Architecture: Minimum Workstation Configuration Guidelines**

Members expressed concerns regarding the need to include statements in the Purpose and Objectives that:

- Simplify and clarify the technical support of minimum guidelines,
- Guidelines are needed to provide a “secure” environment,
- Agencies must analyze their specific software requirement needs, applications and hardware before purchasing,
- Document is not intended for justification to request increased budget dollars.

It was decided to table action on the document. Mr. Henderson will further develop the document for review at the next meeting.

PROJECT REVIEWS

State Records Board Grant Application - UNL - Conservation and Survey Division

The Technical Panel, having reviewed the grant application entitled “Archiving and Digital Access to the Conservation and Survey Division Aerial Photography Collection,” finds that:

- The project is technically feasible.
- The proposed technology is appropriate for the project.
- The technical elements can be accomplished within the proposed time frame and budget.

Mr. Schafer moved to forward the Technical Panel's review of the UNL-Conservation and Survey Division grant to the State Records Board. Ms. Decker seconded the motion. Roll call vote: Huber-Yes, Decker-Yes, Horn-Yes, Schafer-Yes and Weir-Yes. Motion was carried by unanimous vote.

Government Technology Collaboration Fund Review Process
Rick Becker, Government Information Technology Manager, CIO/NITC

Mr. Becker reminded members that grant applications are due August 31st and that at least one Technical Panel member, along with 2-3 other persons, served as a reviewers for each grant.

REGULAR INFORMATIONAL ITEMS AND WORK GROUP UPDATES

Wireless Project. Ms. Decker reported that the request for bids is out and will be due in November. The first series of questions has been completed. Potential vendors have been doing site visits. The second round of questions is due tomorrow. A project proposal for the $1.5 million will be coming to the Technical Panel for their review.

NETCOM. Ms. Decker reported that bids are due Monday, August 27th. A team of 9 persons has been established to review the bids. The finalist will be announced Sept 7th with presentations scheduled to occur September 10th-12th.

Security Architecture Work Group. Mr. Schafer reported that the next meeting is scheduled for August 28th to put the final touches on the templates. The Technical Panel indicated that the templates should be formally adopted by the N.I.T.C. A representative from the State Patrol will be at the next Work Group meeting to discuss the Patrol’s process for incident reporting. The Work Group has also been discussing conducting and organizing a security forum.

Accessibility Architecture Work Group. Ms. Horn reported that the draft is complete and that she will attempt to organize a Work Group meeting for next week.

E-Government Architecture Work Group. Mr. Schafer reported that a grant application will be submitted for the Government Technology Collaboration Fund to continue work on E-government Architecture. The E-government

Conference is scheduled for November 6th at the Cornhusker Hotel.

Video Standards Work Group. Mr. Huber reported that testing is almost complete and the Work Group will be making recommendations soon. Members encouraged the Work Group to have recommendations ready for adoption by the Technical Panel at the September or October meeting for final approval at the October 31st N.I.T.C. meeting.

OTHER BUSINESS

Mr. Huber informed the panel that John Stritt, new Director for the TriValley Distance Learning Consortium, was approved to replace John Horvath to serve on the Video Standards Work Group at the August 17th Education Council meeting.

FUTURE MEETING DATES AND ADJOURNMENT

The next meeting dates of the Technical Panel will be September 11, 2001, 9:00 a.m., October 9, 2001, 9:00 a.m., and October 23, 2001, 9:00 a.m.

Ms. Decker moved to adjourn. Ms. Horn seconded the motion. All were in favor. Motion was carried by voice vote. The meeting was adjourned at 11:50 a.m.

Minutes were taken by Lori Lopez Urdiales and reviewed by Rick Becker, Office of the CIO/N.I.T.C.

Title	**Video Standard for Distance Learning**
Category	**Video Architecture**
Date Adopted	**(DRAFT)**
Date of Last Revision	**September 11, 2001**

A. Authority

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

Section 86-1506 (7) authorizes the technical panel to, “establish ad hoc technical advisory groups to study and make recommendations on specific topics.” Pursuant to this the Technical Panel established the Video Standard Workgroup on 9 January 2001. The stated purpose of the group was to, “determine the next video standard for the distance learning networks of the state of Nebraska.”

B. Purpose and Objectives

The purpose of this document is to define and clarify policies, standards, and guidelines that will enable all existing and future interactive distance learning facilities to achieve interoperability and an acceptable quality of service for all educational applications.

C. Standards and Guidelines

The Video Standard Workgroup has selected two finalist protocols based on criteria adopted and approved by the Technical Panel. These two finalists are MPEG-2 and H.323 with H.263 video. The workgroup is currently conducting detailed testing per the established criteria regarding bandwidth and pre-determined quality level requirements.

The judging criteria include:

Costs
Site - any uniquely required hardware/software cost at a site
Hub - if a hub such as an MCU is required, hardware/software cost
Operational - maintenance requirements, technicians, connectivity bandwidth, scheduling personnel, etc.

Bandwidth
Minimum quality - rate required for NVCN / Network 3 like quality
High quality - rate required for full-motion / broadcast quality
Lip readable – rate required for language classes
ASL readable – rate required for American Sign Language
Flexibility - range available, and rate agile v. steps

Negotiation - automatic / manual bandwidth negotiation between points

Connectivity
Ubiquity - supported delivery methods (IP, ATM, dedicated line, PVC, etc.)
Broadcast / multicast - one-to-many without interactivity
Point-to-point - two interactive sites
Teleconference - several interactive sites (MCU/Switch required?)
Dial up / dial out - the ability for an external site to connect into a conference and not have to be brought in
Latency - amount of delay introduced by encoding process

Compatibility
Standard type - software standard or hardware standard
Backward compatibility - nature of compatibility
Installed base - How prolific is this standard already?
Life Cycle - ability to upgrade

Once a single standard is determined, all synchronous distance learning entities in the state must adopt this new video and audio standard to use state-owned networks, or to request future state funds regarding synchronous distance learning network projects. Given that all users cannot fiscally adopt the standard immediately, the workgroup will follow the technical standard adoption with recommended implementation strategies that will permit a phased migration over time. The ultimate intent of this process is to establish statewide interoperability of all synchronous distance learning networks while minimizing the fiscal impact.

This standard will not prohibit purchase of equipment that does not meet the standard providing:

1. No state funds are used.
2. The entity does not intend to pass the traffic across state owned networks.
3. A specific purchase can be grand fathered to a previous standard if it meets criteria as set forth in the implementation and migration strategies to be recommended by the Technical Panel and adopted by the NITC.

For background tutorial material on H.323/H.263, see:
http://www.cis.ohio-state.edu/~jain/cis788-99/h323/ and
http://www.4i2i.com/h263_video_codec.htm

For background material on MPEG-2, see:
http://www.bbc.co.uk/rd/pubs/papers/paper_14/paper_14.html and
http://www.crs4.it/~luigi/MPEG/mpeg2.html#What%20is%20MPEG-2

These resource materials are provided as a public service. Accuracy of content is neither implied nor guaranteed by the NITC or its advisory groups.

D. Key Definitions

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Electronic and information technology includes information technology and any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications products (such as telephones) information kiosks, and transaction machines, World Wide Web sites, multimedia, and office equipment such as copies and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.
3. Information technology is any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
4. Telecommunications are the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.
5. MPEG is the Motion Picture Experts Group. This association has created the standard protocol under consideration.
6. NVCN is the Nebraska Video Conference Network. It is a terrestrially based teleconference system operated by the State Division of Communications.
7. Network 3 is a satellite based teleconference system operated by the Nebraska Educational Telecommunications Commission.
8. MCU is a multi-conferencing unit. This device allows more than two sites to participate in a teleconference simultaneously.
9. ATM means asynchronous transfer mode. It is a terrestrial data transmission protocol.
10. IP means Internet protocol. It is a communications protocol used on networks for exchange of information.

E. Applicability

GENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Each agency or operational entity must develop detailed procedures to implement broad policies and standards. Compliance with these technical policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC. Compliance may be used in audit reviews or budget reviews.

COMPLIANCE AND ENFORCEMENT STATEMENT

The Governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information standardization and interoperability efforts. Such policies should be reasonable and effective. The NITC intends to incorporate adherence to technical standards policies as part of its evaluation and prioritization of funding requests. The NITC recommends that the Governor and Legislature give due consideration to requests for technical standardization and interoperability improvements during the budget process.

F. *Responsibility*

An effective program for video standards compliance involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate quality of service and uniformity for information systems through adoption of policies, standards, and guidelines.
2. Technical Panel Video Standards Work Group. The NITC Technical Panel, with advice from the Video Standards Work Group, has responsibility for recommending video standard policies and guidelines and making available best practices to operational entities.
3. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for interoperability of information resources that are consistent with this policy. The authority may delegate this responsibility but delegation does not remove the accountability.
4. Information Technology Staff. Technical staff must be aware of the opportunities and responsibility to meet the goals of interoperability of information systems.

G. *Related Policies, Standards and Guidelines*

None currently in place.

Title	**Minimum Workstation Configuration Guidelines**
Category	**Hardware Architecture**
Date Adopted	
Date of Last Revision	**September 7, 2001**

A. *Authority*

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, **guidelines**, and architectures upon recommendation by the technical panel created in Section 86-1511."

B. *Purpose and Objectives*

The purpose of this document is to ~~define and clarify guidelines,~~ describe **minimum** ~~performance~~ configurations, ~~and establish purchasing guidelines~~ for personal computers, in order to simplify technical support and enable a secure desktop environment. These guidelines are not intended to endorse or support any single hardware or software vendor. ~~They are presented to promote conformity and to ensure compatibility with future state initiatives.~~ These guidelines are subject to periodic review and revision.

As minimum configurations, these guidelines are recommendations to be considered in conjunction with other factors, including financial constraints, performance requirements of specific applications, and an agency's networking environment.

The primary objective of these guidelines include recommendations to:

1. Improve versatility and compatibility of desktop systems;
2. Provide a guide to agency on when to upgrade existing personal computers;
3. Reduce ~~maintenance~~ technical support problems; and,
4. ~~Provide agencies with a set of purchasing guidelines that should satisfy future state initiatives~~ Provide a secure desktop operating system.

As the State of Nebraska begins to develop Internet enabled applications, and e-Government and e-Business applications that are delivered over public and private Intranets and the Internet, it is imperative that agencies maintain desktop clients that can efficiently run these new applications. Agency desktop personal computers should be able to:

1. Execute network applications;
2. Support Internet technologies;
3. Extend the desktop communications to the state telecommunications backbone;
4. Support e-Business and e-Government applications; and,
5. Provide desktop security, encryption, and virus protection services when connected to the state telecommunications systems.

A. *Standards and Guidelines*

1) Existing Personal Computers:

In order to avoid obsolescence, agencies should develop a plan to upgrade or replace existing personal computers if they do not support the following minimum system requirements:

Minimum Hardware Guidelines for Existing Personal Computers
- (1) CPU: 133 MHz or higher Pentium-compatible CPU
- (2) Memory: 64 MB RAM
- (3) Hard Disk: 2 GB hard disk with a minimum of 650MB of free space
- (4) Operating System:
  - (a) Windows 98, 2nd Edition (physical security policies should be in place)
- (5) LAN Connection:
  - (a) Ethernet 10/100
  - (b) 4MB Token Ring

2) **Minimum** New Personal Computer Purchasing Guidelines:

When purchasing new personal computers, an agency should consider the following minimum guidelines.

- a. Standard Desktop Hardware
  - (1) CPU: 500 MHz Pentium-compatible CPU or higher
  - (2) Memory: 128 MB RAM or higher
  - (3) Disk: 6 GB or larger
  - (4) LAN Connection: Ethernet: 10/100
  - (5) Operating System:
    - (a) Windows 2000 (recommended)
    - (b) Windows NT 4.0 Service Pack 6a, (with 128 MB RAM and 128 bit encryption)
    - (c) Windows XP (requires 256 MB RAM)
- b. GIS Workstation Desktop Hardware
  - (1) CPU: 500 MHz Pentium-compatible CPU or higher (650 MHz or higher recommended)
  - (2) Memory: 128 MB RAM (256 MB RAM recommended)
  - (3) Disk: 10 GB Fast Open or larger (e.g., SCSI)
  - (4) LAN Connection: Ethernet: 10/100
  - (5) Operating System:
    - (a) Windows 2000 (recommended)
    - (b) Windows NT 4.0 Service Pack 6a, (with 128 MB RAM and 128 bit encryption)
    - (c) Windows XP (requires 256 MB RAM)
- c. Server Hardware:
  - (1) CPU: 500 MHz Pentium-compatible CPU or higher (650 MHz or higher recommended)
  - (2) Memory: 256 MB RAM minimum up to 4 gigabytes (GB) maximum (the higher the memory, the better the performance)
  - (3) Disk: 10 GB Fast Open or larger (e.g., SCSI)
  - (4) CPU Support: Up to four CPUs on one machine

(5) LAN Connection: Ethernet: 10/100 minimum (Fast Ethernet if available)
(6) Operating System:
(a) Windows 2000 (recommended)
(b) Windows XP Server

d. Software Recommendations:
(1) Office Productivity: MS Office 2000 Standard Edition (recommended)
(2) Simple Terminal Emulation:
(a) TELENET3270
(b) TELENET5250
(3) Advanced 3270/5250 Terminal Emulation with Host Addressable Printing
(a) IBM Host Client Access Package
(4) Internet Browser:
(a) MS Explorer 5.0 or higher with 128-bit encryption, and XML compliance.
(b) Netscape 6.4 or higher with 128-bit encryption, and XML compliance.
(5) Virus Protection:
(a) Anti-Virus software (Norton Anti-Virus recommended)
(b) Anti-Virus subscription service to protect against newest attacks

3) All agencies and local government agencies that utilize networking services of the Nebraska Department of Administrative Services' Information Management Services Division and/or the Division of Communications should migrate to Windows NT 4.0 or Windows 2000 Professional in order to support network security.

4) Any agency or local government agency that operates a direct connection to the public Internet shall install firewall services between their public Internet connection and any connection to the state telecommunications network.

5) All agencies that receive public Internet e-mail service shall require virus protection on the desktop or mail server.

D. Key Definitions

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Networking Services shall mean any system that transmits any combination of voice, video, and/or data between users.

E. Applicability

These guidelines are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska.

Agencies should follow these guidelines whenever they intend to support networking services on the desktop. The guidelines may not apply whenever the desktop does not share network services, when there is no connection to state or local networking services, or whenever an application requires a different hardware and software configuration to function.

F. *Responsibility*

1. Division of Communications
2. Information Management Services Division
3. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate accessibility for information systems through adoption of policies, standards, and guidelines.

G. *Related Policies, Standards and Guidelines*

Category 5e Cabling Standards
Other Network Architecture Standards (to be developed)

State of Nebraska

Information Systems Security (ISS)

IS Technical Staff **Template**

This template provides the foundation from which to build your organizations ISS rules. You can use the template Rules as they are, add your own Rules, or delete those that do not apply.

Final Draft
August 24, 2001

State of Nebraska

Information Security Systems (ISS)

{Your Organization Name} **IS Technical Staff Handbook**

"A complete ISS program for the IS professional".

State of Nebraska
Information Security Guidelines

These Information Security Templates and Guides were developed by the Security Architecture Workgroup under a project funded by the Chief Information Officer and the Nebraska Information Technology Commission.

Additional information about these documents can be found at: http://www.nitc.state.ne.us/tp/workgroups/security/index.htm

IS Technical Staff Handbook

Version 1.0
August 24, 2001

Prepared by:

Table of Contents:

Chapter 1

About Information Systems Security (ISS)

About Information Systems Security (ISS)

Information Systems Security (ISS) is becoming more and more necessary as technology changes.

The Role of the IS Department

The IS department, also called IT, MIS is the technical core of the organization. The department is typically made up of programmers, systems analysts, network administrators, and support groups like Help desk and system administrators. The department is responsible for the implementation and maintenance of the computer systems that run the organizations business.

Because the technical staff of the IS department is involved every day with the internal workings of the systems technology, they are the front line to preventing, detecting, and responding to security violations.

The IS Department and the Security Officer

Depending on the size of your organization, there may be separate IS and Security departments. Since both departments make up the skills required to assemble a security team, it is probable that the two departments will work closely together.

ISS At-a-Glance

In order to fully understand the purpose of the Rules in this Guide, it is important to know more about ISS Security. This section gives you a brief overview of the key areas and reasons why we need to protect our organizations information.

Don't try to outsmart the intruder. Be unable to rid a system of a hacker or some other unauthorized user. As a result they may spend considerable time trying to outsmart the intruder, and in the process unduly jeopardize both information assets and systems availability.

Understanding ISS

One of the biggest concerns facing organizations today is to anticipate the type of security threats or intruders so they can safeguard against the attack.

Intruders

Intruders can come in from the outside or be an internal worker. There are amateur and professional intruders. Intruders can be very technical and persistent. Intruders are also adaptable. If you pick the top 10 risks to safeguard, they'll pick 11 or 26.

Types of Intruders

A hacker is an individual whose primary aim is to penetrate the security defenses of large, sophisticated computer systems. A truly skilled hacker can penetrate a system right to the core and withdraw again without leaving a trace of the activity. Hackers are a threat to all computer systems which allow access from outside your organization's premises. The worlds primary target, the pentagon, is attacked on an average of 1 every 3 minutes. A hacker is also called a black hat

A cracker is like a hacker only more deviant.

Kiddie scripts are …

Proto-hackers, can penetrate systems and leave messages to prove how smart they are. They aspire to be hackers, but have not yet acquired the necessary skills to get past serious security measures without setting off alarm systems.

Cyber crime is any criminal activity, which uses cyberspace (the internet network) as the communication vehicle to commit a criminal act. With the exponential growth of Internet connection, the opportunities for the exploitation of any weaknesses in ISS are multiplying. Cyber crime may be internal or external. Internal is easier to penetrate. The term has evolved over the past few years since the adoption of Internet connections on a global scale with hundreds of millions of users. Legal systems around the world are scrambling to introduce laws to combat cyber crime.

Techno-crime is a premeditated act against a system(s) with the express intent to copy, steal, prevent access, corrupt, or otherwise deface or damage parts of a computer system. This type of crime is a real possibility from anywhere in the world, leaving few, if any "finger prints". This term is also used to hacker or cracker that breaks into a computer system with the sole intent of defacing and or destroying its contents. They can deploy "sniffers" on the internet to locate soft (insecure) targets and then execute a range of commands using a variety of protocols. The best weapon against such attacks is a firewall which hide and disguise your agency's presence on the internet.

A virus is a …

A worm is a …

A Trojan horse is a

A time-bombs is …

A stealth-bombs (e.g. malicious code that is disguised as something else. It may be received as a "normal" e-mail, or perhaps as an amusing screen saver. Stealth-bombs deliver their "payload" surreptitiously and the results can be excessive.

A logic-bomb is a …

Social engineering is when

Types of Incidents/ Attacks

- Steal information
- Disclosure of information
- Defacement (e.g. mutilating a web site)
- Change environment (e.g. re-direct printers)
- Destroy and Ruin (e.g. change information, put garbage in information)
- Denial of Service (e.g. break the flow of information, cause excess information "traffic" to tie up all further processing)
- Buffer Overflow (e.g. information is sent to the server at a rate and volume that exceeds the capacity of the systems, causing errors)
- SYN Attack (e.g. connection requests to the server are not properly responded to, causing a delay in connections. These failed connections will eventually time out (true?) but if they occur in volumes, they can deny access to other legitimate requests for access.)

- Teardrop Attack (Large packets of data are spilt into "bite size chunks" with each fragment being identified to the next by an offset marker. Later the fragments are supposed to be reassembled by the receiving system. In the teardrop attack, the attacker enters a confusing offset value in the second (or later) fragment, which can crash the recipients system. (Is this too technical for this guide?)
- Smurf or Ping Attack (e.g. An illegitimate 'attention request' is sent to a system with the return address being that of the target host (to be attacked). The intermediate system responds to the Ping request but responds to the unsuspecting victim system. If the receipt of such responses becomes excessive, the target system will be unable to distinguish between legitimate and illegitimate traffic.
- Physical Attack (e.g. Cutting the power supply, removing a network cable, and damaging a computer.)

Understanding System Risks and Vulnerabilities

Vulnerabilities are …

Risks are …

Using this Guide

This **{IS Technical Staff Handbook}** is a reference tool for IS departments for the organizations of the State of Nebraska. It is written to all levels, that is management, staff, programmers, and such other technical personnel. It is to be followed by all employees, contractors, etc. of the IS department. It defines the general security areas, accompanying policies, and "how to" steps for any security tasks they may need to perform.). It can be used as a training tool or for reference support. This could also be used for an IS Awareness" part of their ISS program.)

About Rules

The majority of the chapters in this guide focus on specific Rules that target the key areas that you can protect. They are grouped by category to help you locate any specific rule.

Special Features of this Guide

(Introduce glossary, troubleshooting, …)

Guide Structure - How Its Organized

To understand the layout of this guide and to help you find a Rule by chapter:

Chapter 1	General ISS Information
Chapter 2	Security Incidents and Reporting
Chapter 3	Access Control Rules (system administrator)
Chapter 4	Network Security Rules (network administrator)
Chapter 5	Internet, E-mail, and E-commerce Rules (network administrator)
Chapter 6	IS Workstation and Equipment Rules (general IS)
Chapter 7	Software Development Rules (developers)
Chapter 8	Disaster Recovery Rules (team?)
Chapter 9	Physical Security / Premises Rules (operations?)
Chapter 10	Getting ISS Help
Appendix	Appendix A - List of Rules
Index	

Chapter 2
Security Incidents and Reporting

About Security Incidents

Security Incidents or security breaches can occur at anytime. Your organizations incident program will usually involve a security team, but the IS department will probably be a big part of the response team to provide the technical knowledge and evidence preservation.

Suspicions and Incidents

A Suspicion, an unconfirmed assumption of attack, is not yet an Incident. For this reason, it is even more critical to report a suspicion so as to avoid the incident from even happening or greatly decrease any negative results.

It is the responsibility of every employee to do their part in detecting and reporting any possible incidents or suspicions.

Witnessing / Causing an Incident

You could encounter a potential incident, one in process, or one to be carried out, at any time. You could also (intentionally or accidentally) cause an incident.

You, the witness, should react immediately. Do not try to handle it yourself.

Your Incident Response Team

Where no agreed response plan is in place, the reactions of users, management and IS are likely to be ad hoc and inadequate, thus possibly turning a containable incident into a serious problem.

Incident Participation

As part of the response team – you may need to get involved / called to help preserve evidence, or set up barriers, and other protective measures.

Your organization has assembled a security response team to handle all suspicions and incidents. You should be aware of who is on the response team and how to contact them. They are:

____

____

____

Responding to ISS Incidents

If an incident is reported, you must follow these steps:

1. Verify that it is indeed an incident
2. Analyze the intrusion
3. Communicate with all appropriate parties
4. Set up barriers to block the intrusion (if possible)
5. Collect and protect evidence
6. Investigate all issues
7. Document the incident
8. Recover from the incident
9. Follow up on the incident
10. Handle media inquiries (if necessary)

Suspicion and Incident Reporting

If you are not sure if something unusual is going on, and it still a suspicion, it is best to report it and have the experts check it out.

IMPORTANT: Reporting a suspicion, can prevent an incident.

Virus Reporting

Most of us have encountered a computer virus directly or indirectly already. The greatest danger with computer viruses, is that if they go unreported and uncontained, it will continue to spread. Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. You must report a computer virus infestation immediately after it is noticed.

Hardware Faults

All systems hardware faults are to be reported promptly and recorded in a hardware fault log. This will help you detect patterns in equipment problems.

Electronic Intrusion

For cases involving electronic intrusion, the goals of data integrity, data recovery, method of breach and intruder identification apply. Notification procedures could include the State Patrol (if deemed serious enough), the potentially affected business area manager, software application support manager, and data center manager. Any activity monitor data, collected as a normal part of doing business, should be kept until the incident has been cleared.

Unauthorized Access Intrusion

Whenever unauthorized system access is suspected or known to be occurring, you must take immediate action to terminate the access. If these actions do not completely suppress the unauthorized activity, assistance from the Corporate Information Systems Help Desk (?) must immediately be sought. You must inform both technical staff (and perhaps users) that they must take immediate action to suppress unauthorized system access.

Incident Reporting At-a-Glance

To Report …	Comments	Call … Do …
… an incident in process.		1. Call …
… sensitive information is disclosed, lost, or damaged.		1. Call …
… software/ system malfunction	Do not attempt a recovery yourself.	1. Note (if time) any error messages, unusual system behavior (how is it behaving different than before?) 2. Stop using the computer. 3. Disconnect from any attached networks. 4. Call …
… a virus	Because viruses have become very complex, users must not attempt to eradicate them without expert assistance. If users suspect infection by a virus, they must immediately:	1. Shut-down the involved computer. 2. Disconnect from all networks. 3. Call … ??? (help desk, security, manager?)
… an offensive E-mail, call, etc.		Respond directly to the originator. If the originator does not promptly stop sending offensive messages, report it to ??? (HR?)
… suspicious behavior.		1. Call …
… known systems security vulnerabilities, risks, alerts, and warnings		1. Call …
… equipment fault, damage or loss		1. Call …
… physical access violation		1. Call …

Evidence

When an incident occurs, you must gather the facts of what happened, how it happened, and note any indictors or trails that can help in the investigation. Lack of a clear trail of evidence when investigating any ISS crime is critical. Without proper evidence, you may be prevented from taking legal action.

Collecting Evidence

If possible, do whatever you can to quickly gather evidence of what you are witnessing or detecting. Do not let this task interfere or slow down the reporting process. For example, you may want to write down peculiar system performances, error messages to help the investigation.

Preserving Evidence

The most important task of the IS department in the event of an incident is to preserve the evidence.

IMPORTANT: Do not try to restore the system until all evidence has been gathered.

Recording Evidence

(…)

Tracking Intrusions

You organization shall implement procedures for logging information on intrusion attempts and storing that information in a manner for later analysis or use by law enforcement.

Incident Patterns

In order to see patterns develop that may detect in incident, you should implement a good log reporting process. For example, a log that lists equipment faults, software errors, and such could make you aware of an incident before it happens.

Chapter 3
Access Control Rules

About Access Control

Access Control is the one of the key concerns in any ISS program. Gaining access to any systems and applications should be carefully controlled and maintained by the IS department. It is through unauthorized access that extreme security violations can occur.

The Role of the IS Department

One of the key tasks performed in the IS department is to set up users to access systems. This is typically done by a System or Network Administrator. The IS department is responsible for assigning a unique User ID, and a default password to all users requiring system access. The information that each user can access must be carefully considered and these privileges should be consistent with the job performed by each user.

Access Control – Logging On

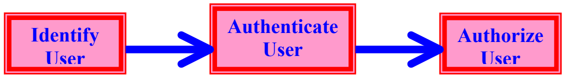
It is through a series of steps that the computer users can access, or log on to your organizations information.

Logon Types

There are many ways to identify the computer user. They are:

- Single signon where the user has only one User ID set up with user profiles
- Biometric
- Thumb print
- "Hamster"
- retina, iris, facial

The logon Process



Access Control Rules

Technical Specialists Rules

The IS department is staffed with technical specialists that have access to the internal system operations. For this reason, it is important to carefully select and monitor IS activity as it relates to ISS.

Information technology specialists include those individuals such as application developers and LAN administrators who have specific types of responsibilities and access to organization and enterprise information.

Rule - Access by Technical Specialists

The roles and responsibilities of technical personnel with higher access authorities should be defined.

Explanation/ Key Points

Application developers should have limited ongoing access to production databases. Organizations that allow application developers access to production databases because of business needs should do so limiting such access to only those tasks that are essential to ensure that the application runs smoothly once applications are in a production environment.

Rule - Technical Specialists Security Check

Technical specialists with broad access to data are in sensitive positions and may be required to undergo a security check as a condition of employment.

Rule - Security Administration Activities

Security administration activity regarding access should be recorded and reviewed and security violations or incidents should be detected and reported.

Application Requirements Rules

Rule - Application Controls

Applications shall incorporate controls for managing access to selected information and functions. Applications must include auditing capabilities to track access to sensitive information.

Logging On Rules

<u>Logon/ logoff</u> The processes by which users start and stop using a computer system.

Rule - Unique User ID and Password

Every user must have a unique User ID and a confidential password. This User ID and Password combination will be required for access to your organizations information systems.

Rule - Unsuccessful Logon Attempts

The user should be allowed {3} failed attempts to try to logon. If they fail all attempts, IS should revoke the User ID. This prevents trial-and-error or brute-force attempts to guessing passwords.

Rule - Single Sign On (Log On) Rule

Many organizations are going to a single sign-on (log on) which facilitates the set up process in IS. It also holds the user responsible to remember only one User ID and Password. The use of the same User ID on all computers and networks across an organization is additionally desirable because it makes analysis of activity logs considerably easier. There is also a risk involved when it comes to security, since it only takes one break through to get to all access points.

Rule - Disclosure of Incorrect Logon Information

When logging on, if any part of the logon sequence is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the entire log on process was incorrect.

Rule - Encrypted Logon Files

The logon file that contains User IDs and passwords should be stored encrypted. This is a high risk data classification and must be closely managed.

Rule - Logon Scripts

Logon scripts should not contain passwords. They should not be built into the logon script for auto-signon.

Rule - Third Party Logons

Before any third party is given access to your organizations systems, the proper approvals must met.

Rule - Giving Logon Information to the User

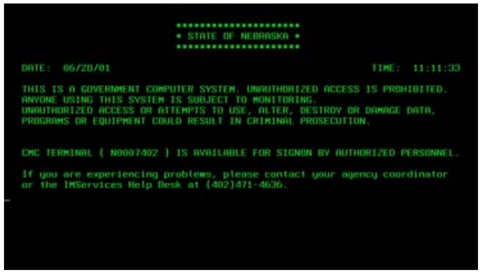
User IDs and passwords should not be distributed to the user in the same communication.

Warning Banner Rules

A warning banner is a security notice that displays on the screen when the user has successfully accessed the system or application requested. This system message is displayed each time the user logs on to an environment such as Lotus Notes, AS400, CICS, TSO and such. It can be considered the electronic equivalent of a no trespassing sign.

The warning banner should display:

- that the user has accessed a government system or system that may contain government information
- that use is restricted for authorized purposes
- that the users activities are subject to monitoring
- that misuse can be reported to security and/ or law enforcement personnel and subject the user to criminal and/ or civil penalties (laws, fines, penalties)



```
                    **********************
                    * STATE OF NEBRASKA *
                    **********************

DATE:  06/28/01                                        TIME:  11:11:33

THIS IS A GOVERNMENT COMPUTER SYSTEM. UNAUTHORIZED ACCESS IS PROHIBITED.
ANYONE USING THIS SYSTEM IS SUBJECT TO MONITORING.
UNAUTHORIZED ACCESS OR ATTEMPTS TO USE, ALTER, DESTROY OR DAMAGE DATA,
PROGRAMS OR EQUIPMENT COULD RESULT IN CRIMINAL PROSECUTION.


CMC TERMINAL ( N0007402 ) IS AVAILABLE FOR SIGNON BY AUTHORIZED PERSONNEL.

If you are experiencing problems, please contact your agency coordinator
or the IMServices Help Desk at (402)471-4636.
```

Sample Warning Banner

Rule - Display a Warning Banner

The user MUST receive a warning banner for each environment they access each time they log on..

Explanation/ Key Points

In the event of a prosecution against those who entered a system unlawfully, one of the most successful defending claims is that there was no notice saying they could not enter. As a result, a warning banner, displayed each time a user logs on.

Rule - Warning Banner Keystroke Monitoring

If your organization requires keystroke monitoring, it must be noted in the warning banner that activity logging is being done.

Rule - Warning Banner Last Logon

The warning banner should display the date, time and device of the last successful and unsuccessful logon you performed.

Explanation/ Key Points

This will allow unauthorized system usage to be easily detected. It puts the responsibility on the user and provides the user with the information needed to determine whether their User ID has been used by an unauthorized party.

Rule - Warning Banner Information Disclosure

The warning banner should not identify information about the organization, operating system, system configuration, or other internal matters.

Explanation/ Key Points

The lack of specific information will keep unauthorized persons in the dark as to the system that they have reached. This may make the system less interesting to them and gives them less information on which to base a password guessing attack. Lack of information about the computer operating system will also prevent the users from employing knowledge of specialized weaknesses in these operating systems.

Logging Off Rules

Rule - Automatic Log Off

All users should be automatically logged off if there has been no activity on their workstation for **{10}** minutes}, the system must automatically blank the screen and suspend the session.

Explanation/ Key Points

Re-establishment of the session must take place only after the user has provided the proper password. This is to prevent unauthorized system usage resulting from authorized users walking away from their desks without logging out.

Although most effective when it applies to all workstations, this policy could be restricted to systems containing or accessing sensitive, critical, or valuable information. In many instances, because automatic log off functionality is not a part of the operating system, for microcomputers and workstations a software security package will be needed to implement this Rule.

The user should never lose their work in progress as a result of the suspended session.

Identification/ User ID Rules

All users will be identified by a unique identifier, the User ID. This User ID is used for positive identification in order to access any systems. The User ID is not only used to distinguish each user, but also to assign privileges. *See Authorization Rules*.

Positive identification ordinarily involves User IDs, but may also include biometrics, call-back systems, dynamic password tokens, smart cards, digital certificates, and many others.

Rule - Unique User ID

All users MUST have a unique User ID making them responsible for all activities performed under that User ID.

Rule - Prohibit Group User IDs

Never setup a User ID for group(s) access. It must be tied to an individual. They should never be generic.

Rule - Dormant User IDs

User IDs should automatically have the assigned privileges revoked after **{30}** days of inactivity. Temporary employees. contractors, and consultants should be revoked in **{15}** days.

Rule - Internet User ID Expiration

User IDs on internet accessible computer should be set to expire **{3}** months from the time it is established.

Rule - Granting Multiple User IDs

A user may have multiple User IDs for access to different systems, however, each one should still is issued uniquely to that user. This may be necessary to grant different privileges to a user that requires using different applications on different necessary to perform their job.

Explanation/ Key Points

The use of the same User ID on all computers and networks across an organization is desirable because it makes analysis of activity logs considerably easier. With multiple User IDs, logs may be more difficult to analyze.

Rule - Granting User IDs to Outsiders

Outsiders or users who are not employees, contractors, or consultants must not be granted a User ID or otherwise be given privileges to use your organizations computers or communications systems without proper approvals.

Rule - Re-use of User IDs

Each User ID must be unique and forever connected solely with the user to whom it has been assigned. After a user leaves your organization, there must be no re-use of that User ID.

Rule - Customer Privacy and User IDs

To help preserve the privacy of customer information, IS should provide mechanisms for customers to remain anonymous when using your organizations systems.

Rule - Distribution of User IDs

When IS informs the user of their User ID, it should be delivered in a secured method.

Rule - User ID Format

The User ID should be difficult to guess.

Explanation/ Key Points

User ID suggested format: {xxxx.xxx.x.x.x.xx.} (?)

Rule - User ID Logs

IS is responsible for the monitoring of user activities and this is done by User ID.

Explanation/ Key Points

Suggested logs by User ID:

1. logon attempts failed
2. actions performed
3. high profile actions
4. wide scale deletions
5. who edited web site
6. activities of computer operations
7. activities of system administrators
8. activities of security officers

9. who accessed highly sensitive data

Most logs should report time, date, User ID, type of event, success or failure, origin of request (i.e. terminal address) and others.

Rule - Anonymous User IDs

(?) User IDs must be assigned in a sequential numeric fashion so that there is no obvious correlation between a User ID and the actual name of the involved user.

Authentication / Passwords Rules

After the user has been identified by the system, they will then be required to enter a Password to Authenticate that it is indeed them. Here, "Password" could be replaced by other authentication methods like smart cards, PIN (personal identification numbers) numbers, dynamic password tokens, biometrics, fingerprints, voice recognition, retinal scans, and other technologies.

Guessing passwords remains a popular and often successful attack method by which unauthorized persons gain system access.

Password Management

Although the password is chosen by the user, it is up to IS to provide the guidelines to which they must comply.

Rule - Assign a Default Password

A default password should be assigned to all new users, users requiring a reissue, or for users that forget their password. IS should stress to the user the importance of changing their default password. Even the IS security administrator should not know user passwords.

Explanation/ Key Points

Sometimes this type of Password is called an "expired" or "temporary" Password in that it is valid for only one log on session. Some vendors are now extending this idea to the default passwords that come with their computer or communications products.

Rule - Minimum/ Maximum Password Length

The length of a users password should be checked automatically at the time that they construct or select it. IS should control user password selection by placing system restrictions on the length of the password. Passwords must have at least eight **{5}** characters, but no more than **{n}**. Passwords with only a few characters are much easier to guess.

Explanation/ Key Points

Rule - Cyclical Previous Passwords

IS should control user password selection to not allow the changed password to be a derivative of a users previous one.

Explanation/ Key Points

A user should not just partially change their Password just to satisfy an automated process which compares the old and new passwords to make sure that previous passwords are not reused. This security eroding approach is particularly prevalent among users who must log on to many different machines.

Rule - Password Allowable Characters

IS should control user password selection to allow characters that are: {alpha, numeric, special, combination}. Ideally, the Password must contain at least one alphabetic and one non-alphabetic character.

Explanation/ Key Points

Non-alphabetic characters include numbers (0-9) and punctuation. This will help the user to choose a password that is difficult for unauthorized parties and system penetration software to guess.

Rule - Passwords Lower and Upper Case

IS should control user password selection so it must contain at least one lower case and one upper case alphabetic character.

Explanation/ Key Points

From a mathematical standpoint, the idea behind the use of both upper and lower case characters is to increase the total possible choices, thereby making password guessing more difficult.

For example: “a” is not the same as “A”

A password of 6 characters offers over 2 million possible combinations. In case-sensitive password applications, where “a” is not the same as “A” and doubles the number of available characters. Thus, making the same 6 character password case-sensitive, and allowing the shifted version of the numerical keys increases the number of combinations to about 140 million. Each additional character increases the number of combinations exponentially and so a 7-digit character, case-sensitive password would offer over a billion combinations. A human user has virtually no chance of ever identifying a 6 character password which has been randomly generated and less chance of cracking a password of 8 or more characters.

Rule - Reusing Passwords / History

System restrictions should be put in place so that a user cannot reuse their Password for **{15}** changes. OR They must not use the same password more than once in a **{12}** month period.

Explanation/ Key Points

Reuse of Passwords increases the chances that it will be divulged to unauthorized parties and increases the chances that it will be guessed since it is in use for a longer period of time. The security provided by forced password changes is much less effective if you repeat the same Passwords.

IMPORTANT: If a user utilizes sensitive data and has a high access authority, they must NEVER use the same Password twice.

Rule - Forced Expiration of Passwords

IS should force users to change their Password every **{90}** days. If they access sensitive data, they should be forced to change their Password every **{30}** days.

Explanation/ Key Points

When a password expires, the users should be restricted from continuing to work. This forces them to change it. If a password has fallen into the hands of an unauthorized party, then unauthorized system use could continue for some time in the absence of a forced password change process. The security provided by forced password changes is much less effective if users repeat the same passwords.

This Rule limits the time period in which any unauthorized use could continue. If combined with a dormant User ID privilege revocation process, it acts as a safety net if IS systems administrators forgets to disable privileges when users change jobs or leave an organization.

Some organizations have a tiered approach where different time intervals are used for different user populations, based on the nature of the privileges available to these users. For example, systems programmers may be forced to change their password every two weeks, while regular users may be forced to change their password once every month.

Rule - Unsuccessful Passwords Attempts

Users should be allowed **{3}** failed attempts to successfully enter their Password.

Explanation/ Key Points

To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. If a user fails the number of attempts, their User ID must be either:

(a) suspended until reset by the IS system administrator
(b) temporarily disabled for no less than three minutes

(c) if dial-up or other external network connections are involved, disconnected.

Rule - Proof Of Identify to Obtain a Password

IS should never give out a password over the phone. The user must appear in person to the IS department to obtain a new or changed Password to positively identify themself.

Explanation/ Key Points

If a user is in a remote location, IS must devise a method of obtaining a positive identification. For example, IS could use a user code that only the user knows, like employee number. The Help desk could create a questionnaire that covers both organization and employee information to positively identify them as an employee.

Rule - Distributing Passwords to Users

IS must never display or print a users Password. Instead it must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

Explanation/ Key Points

The moment a Password is committed to a paper or document, discovery of that paper will invalidate other security measures.

HINT: You could use the "black night" method. With this method, passwords may be shown in a conspicuous spot because they have been altered using some standard approach, such as bump the first letter up the alphabet one letter, bump the second letter down one letter, etc.

Rule - Typing Passwords

When a password is typed into a system, it should not be displayed on a monitor or printed on a printer.

Explanation/ Key Points

If a password were to be displayed, persons nearby could shoulder-surf or look over a users shoulder to obtain their password. If a password were to be printed and discarded, persons doing "dumpster-diving" (going through the trash) could recover your password.

Rule - Resetting Passwords

If a user forgets their password, IS should reset it to the default password.

Explanation/ Key Points

Some organizations require that the user re-register like a new user and receive both a new password and User ID.

IMPORTANT: IS must positively identify the user before re-setting is done. Some previously agreed upon mechanism and information is needed to accomplish this. Too often this is done over the phone without positive ID of the caller.

Rule - Dynamic Password Tokens

Dynamic password tokens must not be stored in the same briefcase or suitcase as portable computers used to remotely access your organizations networks.

Rule - Seed for System Generated Passwords

If system generated passwords are used, they must be generated using the low order bits of system clock time or some other frequently-changing unpredictable source.

Rule - Immediate Issue of System Generated Passwords

If passwords or Personal Identification Numbers (PINs) are generated by a computer system, they must always be issued immediately after they are generated. Unissued passwords and PINs must never be stored on the involved computer systems.

Rule - Storage of Passwords

Passwords must not be stored in readable form in batch files, automatic log on scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover or use them.

Rule - Zeroization of Password Materials

If passwords or Personal Identification Numbers (PINs) are generated by a computer system, special care must be taken to erase all residual data used in the process. All computer storage media (magnetic tapes, floppy disks, etc.) used in the construction, assignment, distribution, or encryption of passwords or PINs must be "zeroized" immediately after use.

Explanation/ Key Points

Zeroization means that the media must be repeatedly overwritten with a series of ones and zeros. Additionally, computer memory areas used in the derivation of passwords or PINs must be zeroized immediately after use.

Rule - Password Based Boot Protection (?)

All workstations used for your organizations business activity, no matter where they are located, must be using an access control system approved by the appropriate authorities. In most cases this will involve screen-savers with fixed-password-based boot protection along with a time-out-after-no-activity feature.

Rule - Sending Passwords through the Mail

If passwords must be sent by regular mail or similar physical distribution, they must be sent separately from User IDs. These mailings must have no markings indicating the nature of the enclosure. Passwords must also be concealed inside an opaque envelope that will readily reveal tampering.

Rule - Password Encryption

Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over networks. This will prevent them from being disclosed to wiretappers, technical staff who are reading systems logs, and other unauthorized parties. IS shall protect authentication data so that it cannot be accessed by any unauthorized user.

Rule - Use of Duress Passwords (?)

When system access to particularly valuable or sensitive data is given to a user, duress passwords must be employed to covertly signal the system that this user is being pressured to log on. Duress passwords are special passwords used only in those circumstances where an alarm should be triggered, but where the user's safety may be jeopardized if people accompanying the user know the alarm has been triggered.

Rule - Changing Vendor Default Passwords

All vendor supplied default passwords must be changed before any computer or communications system is used for your organizations business. One of the oldest ways to break into a system is to try the vendor-supplied default passwords.

Rule - Passwords of Key Role Holders

Passwords of key role holders -such as system and network administrators should be copied and held under dual control in a fire-resistant, secure location, to enable access to the system by an authorized person in the unavoidable absence of the password holder.

Rule -Review Digital Certificates

IS must review digital certificates for individuals every **{1}** years and for server side every **{2}** years.

Rule - Unauthorized Access to Passwords

IS systems developers must not construct separate mechanisms to collect passwords or User IDs. Also, they must not construct or install other mechanisms to identify or authenticate the identity of users without proper approvals.

Authorization (Privileges) Rules

Without unique User IDs, a user cannot have privileges assigned just for them. If privileges cannot be restricted by user, then it will be very difficult to implement separation of duties, dual control, and other generally accepted security measures.

Authorization, or privilege control is given at the User ID level and determines what you can access. Once you have successfully logged on, you will have access to all the authorities, or privileges you have been granted.

Authorization privileges are set up by IS according to the specific task requirements of the user and what information or programs they need to access to perform their job.

In order to define the user privileges, their roles need to be identified based on business functions. Then IS can determine what authorities are needed to perform these functions.

The authorities to read, write, modify, update, or delete information from automated files or databases should be established by the owner(s) of the information. Users may be granted a specific combination of authorities. Users should not be given any authority beyond their needs. Access rules or profiles should be established in a manner that restricts users from performing incompatible functions or functions beyond their responsibility and enforces a separation of duties.

Rule - Privileges Granted on a Need-to-Know Basis

IS will give only those authorities to users that they need to do their job. They will be presented with only the system capabilities and commands that they have privileges to perform. The user should have no more privileges than is required to perform their job and for the time period that it will be performed.

Explanation/ Key Points

TIP: Menus should show only the options which that user can select.

Rule – Dual Access Controls

Procedures should be implemented which ensure that access to data or information is not dependent on any individual. There should be more than one person with authorized access.

Rule - Privileges Granted by Groups

Group authorities can facilitate this task, but caution must be taken to be sure each user in the group is equal.

Rule - Users that Leave the Organization

Privileges should be deactivated by User ID when a user leaves the organization.

Rule - Systems Privileges

Access to systems and utilities must be restricted to a small number of trusted and authorized users. Whenever these utilities are executed, the resulting activity must be securely logged, and promptly thereafter reviewed by IS.

Rule - Limited Number of Privileges Users

Rule - Third Party Privileges

Restriction Of Third Party Dial-Up Privileges …

Rule - Time Dependent Privileges

Rule - IS Technical Staff Privileges

Rule - Periodic Review and Reauthorization of User Privileges

Rule - Changes in User Duties

Rule - Separation of Duties

User privileges must be carefully defined so that users cannot gain access to, or otherwise interfere with, either the individual activities or the private data of other users.

Applications with Sensitive Information Rules

Computer Operations which support sensitive information shall operate in accordance with procedures approved by the information custodians of participating organizations.

Rule -

Operating programs prohibit unauthorized inquiry, changes, or destruction of records.

Rule -

Operating programs are used to detect and store all unauthorized attempts to penetrate the system.

Rule -

… Special requirements are met, such as those for criminal justice records

Sanctions Rules

Rule – Revoking Access

The operator of a secure network may revoke access to the network to insure the security, integrity, and availability of the network to other users.

Employment Status Change Rules

IS must be promptly informed of any changes to the status of a user. This includes:

- new hires
- resignations
- terminations
- transfers
- promotions/ demotions

Title: *Setting up a New User*

> Suggested Rule Statement
>
> *"Each new user will need to be set up according to your organizations new hire procedures."*

Policy Category Access Control	**Policy Standard** Employment Change	**Rule Number** xx.xx.xx
Rule Date mm/dd/yy	**Rule Revision Date** mm/dd/yy	**Date Adopted ?** mm/dd/yy
Approval Name/ Code ? (signature?) (?)	**Rule Source** acdefg	**Audit Number/ Code (?)** xx.xx.xx

Explanation

Procedure(s)

To set up a new employee:

1. Assign a User ID.
2. Set the password to the default password.
3. Inform the new user to change the password immediately.
4. …
5. Orientation …

Title: *Handling Terminations*

Suggested Rule Statement

“Prompt attention should be given to revoking and denying access to any employee that has been terminated.”

Policy Category Access Control	**Policy Standard** Employment Change	**Rule Number** xx.xx.xx
Rule Date mm/dd/yy	**Rule Revision Date** mm/dd/yy	**Date Adopted ?** mm/dd/yy
Approval Name/ Code ? (signature?) (?)	**Rule Source** acdefg	**Audit Number/ Code (?)** xx.xx.xx

Explanation

IS should be notified immediately of any employee terminations by the employees manager or HR.

Procedure(s)

To handle employee terminations:

1. Be sure to
2. Delete the …
3. Remove the …

To handle employee resignations:

1. Be sure to
2. Delete the …
3. Remove the …

Chapter 4
Network Security Rules

About Network Security

Networks are common is all organizations to process and run the information necessary. This network is also an access point to other systems, internet and other networks. Networks allow sharing of information, applications, and other computer resources. Dependence on networks requires availability 24 hours per day, every day of the year. Integrity and confidentiality are paramount.

Networks also represent major points of vulnerability to a large range of security problems. Public networks such as the Internet compound the security threat. Remote access, connections between networks, Internet access by workstations on the network, Internet access to information and services, and other configurations make network security a complex problem.

Networks can also enable a quicker spreading of problems, including computer viruses due to its accessibility of external and internal resources.

State agencies and institutions shall manage networks in a manner that insures their proper use, prevents unauthorized access or use, maintains availability and protects the security of information resources. State agencies and institutions shall establish controls that are commensurate to the security needs of the information and computer resources on the network. Controls shall also reflect the security needs of other agencies or institutions connected to the network.

Internet and Intranet sites must be protected from intrusion so that an unauthorized individual cannot alter data and information or compromise the integrity of state controlled networks. Intranet sites must be further protected by user-Ids and passwords or other unique identifier so that access by unauthorized individuals is not allowed. The policy and standards set forth in the Individual Use and Access Policies will apply.

Internet or Intranet connections pose a risk of unauthorized access to state maintained data by compromising the integrity and privacy (where appropriate) of data. Potential consequences of unauthorized access include altering, erasing, or otherwise rendering the information invalid or unavailable by manipulating the data or the underlying programs.

The Role of the IS Department

Is it the role of the IS department to maintain networks and grant access to computers users to the areas of the network they need to do their job.

The IS department can reduce exposure to security problems by controlling remote access to computer networks, connections to the Internet, and using the Internet or an Intranet to deliver information or services, and connecting networks.

The main IS network tasks are:

- To protect the integrity of networks operated by state agencies and institutions from unauthorized access and fraudulent use and /or abuse.
- To reduce exposure to security risks associated with remote access, Internet use, and connecting networks;
- To monitor network use.

Network Security Rules

Network/ Perimeter Security Rules
Firewalls Rules
Remote User Access Rules

Network / Perimeter Security Rules

Identify network entry points (?) or back doors (?).

Rule - Configuring Networks

Your network must be designed and configured to deliver high performance and reliability to the users.

Explanation/ Key Points

Slow or inadequate response time can impede your systems processing.

Rule - Managing the Network

Only qualified IS technical staff should maintain the network.

Rule - Defending against Virus Attacks

Anti-Virus software is to be deployed across all PCs with regular virus definition updates and scanning across all servers, PCs, and laptops.

Explanation/ Key Points

Virus infection can be minimized be deploying proven anti-virus software and regularly updating the associated vaccine files. Many anit-virus companies supple such updates from their web sites.

Lack of an agreed standard or inconsistent deployment of anti-virus software can seriously increase the risk of infection, spread, and damage.

Failing to update the virus definition files on a regular basis increases the risk of infection from a variant for which you do not have the necessary vaccine.

A failure to run regular virus scans across all data files on your server(s) reduces the ability to detect and cure a virus before its “footprint” is identified by a user trying to open the file in question.

Rule - Handling Hoax Virus Warnings

IS should have procedures to handle hoax virus warnings, including someone designated as the virus handler.

Explanation/ Key Points

Threats from viruses are well known today. Hoax threats are the spreading of rumors of a fictitious virus or other malicious code. Good virus intelligence warnings are the key to minimizing the impact of hoaxes. Hoax threats can minimize reactions to a genuine threat increasing your susceptibility.

Rule - Installing Virus Scanning Software

Anti-virus software must be installed on all workstations and portable computers. Select your virus scanning software carefully and be sure you have adequate protection.

Explanation/ Key Points

Because anti-virus definitions (vaccine) are always changing, you should upgrade your virus software every {2} weeks.

Rule - Electronic Eavesdropping

Rule - Modem Pool

With the exception of portable computers and telecommuting computers, the use of local modems to establish direct dial connections is prohibited. All dial-up connections with your organizations systems and networks must be routed through a modem pool which includes an approved extended user authentication security system.

Rule - Dividing Large Networks

All large networks crossing national or organizational boundaries must have separately-defined logical domains, each protected with suitable security perimeters and access control mechanisms.

Rule - Network Connections with other Organizations

The establishment of a direct connection between your organizations systems and computers at external organizations, via the Internet or any other public network, is prohibited without the proper authorization.

Rule - State-owned Resources

Each organization using the State Data Communications Network (SDCN) is responsible for the activity of its users. (Put in IS Guide)

Rule - Network Controls

Network resources participating in the access of sensitive information or critical systems shall assume the security level of that information for the

duration of the session. Controls shall be implemented commensurate with the highest risk. All network components must be identifiable and restricted to their intended use. Specific standards and guidelines include:

Rule – Unattended Terminals

Password protected screen savers, terminal lock and key, or terminal software locking options will be enabled on each terminal so that access can be controlled by locking the terminal while it is unattended.

Rule – Securing Line Junctions Points

All line junction points (cable and line facilities) should be located in secure areas or under lock and key).

Rule – Controlling Network Analyzers

Some types of network protocol analyzers and test equipment are capable of monitoring (and some, altering) data passed over the network. Use of such equipment will be tightly controlled, since it can emulate terminals, monitor and modify sensitive information, or contaminate both encrypted and unencrypted data.

Rule – Network Diagrams

The IS network manager must maintain up-to-date diagrams showing all major network components, to maintain an inventory of all network connections, and ensure that all unneeded connections are disabled.

Rule – Default Passwords on Network Hardware

Default passwords on network hardware, such as routers, should be changed immediately after the hardware is installed. Security updates and patches for software should be kept current.

Rule – Keeping Track of Modems

The IS network manager must maintain a list of all approved dial access modems and establish a procedure that periodically checks for any unapproved modems that have been added to the network.

The network manager must periodically monitor sharing and trusting relationships for connecting with other networks to ensure they are still valid.

Rule - Network Audit

An audit of network security should be conducted annually.

Rule – Perimeter Security

Perimeter security protects a network by controlling access to all entry and exit points. Perimeter security must be managed as a mission critical infrastructure.

Explanation/ Key Points

Organizations shall manage the security for all points of entry to and from the state's network. Customers with all WAN connections provided and managed by a central network manager are considered "internal networks" located within the secure network perimeter boundary. Additional WAN connections that are not provided by the central network manager may be considered "internal networks" if they are authorized and approved by the central network manager. Customers with connections that are not managed by the central network manager must comply with perimeter security procedures established by the central network manager in order to connect to the network.

Rule – Accessing Network Vulnerability

The IS central network manager shall develop and use an on-going process to assess vulnerability of the network and risk in order to maintain adequate perimeter security controls. The IS central network manger and customer representatives must work together to address ways to meet customer business needs within a secured environment.

Rule – Network Entry Controls

Appropriate access controls such as identification, authentication, certification, and authorization must be implemented to control entry to the network.

Rule – Monitoring Network Entry

A program of continuous tracking, detection, and monitoring with audit trail and reporting is required for all network entry and exit points. This program must contain procedures for adequate and timely response to intruders.

Rule - Perimeter security 24/ 7

Perimeter security is required 24 hours per day, every day of the year in order to support continuous business operations.

Rule – Implementing Perimeter Protection

The IS central network manager shall work with users to develop operating procedures and business rules needed to implement perimeter protection.

Rule – Managing Risk

Security for a connected network should reflect the security requirements of the highest risk elements on the network.

Firewalls Rules

Rule – Firewalls Required for all Dial Up Connections

All inbound dial-up lines connected to your organizations internal networks and/or computer systems must pass through an additional access control point (such as a firewall), which has been approved by the proper authorities before users reach a log on warning banner.

Rule -

Firewall Detection

Rule – Firewalls Must Run on Dedicated Computers

All firewalls used to protect your organizations internal network must run on separate dedicated computers. These computers may not serve other purposes such as act as web servers.

Rule – Changing Firewall Configurations

Firewall configuration standards must not be changed unless the permission of the proper authorities has first been obtained.

Rule – Internet Connections Need Firewalls

All connections between your organizations internal networks and the Internet (or any other publicly-accessible computer network) must include an approved firewall and related access controls.

Remote User Access Rules

Rule - Unsuccessful Logon Attempts

The maximum permissible Password attempts for dial-up access is {3}. If the user has not provided a correct password after three consecutive attempts, the connection must be immediately terminated.

Remote Systems Connecting to Production Rule

All computers which have remote real-time dialogs with your organizations production systems must run an access control package approved by the Information Security Department.

Rule - Issuing Laptops/ Portable Computers

All users must be made aware of the rules surrounding remote equipment, in particular laptops and other portable computers that connect to the network from an outside location and use your organizations information.

Rule -

(DAS uses a token to positively ID people dialing in. About the token: Has a 6 digit password code (pin number) that is constantly changing. It must be synchronized with the mainframe. Mainframe keeps track of access info, inactivity, … Also a 4 digit that the user enters. Also could use finger print (on mouse), eye retina scan, smart card, … When you dial in from a remote site, you access the network first. (Citrix). The network authenticates and gives you access to the pre-defined areas: Notes, LAN, or Mainframe. You can access your user files and directories on H:

Rule – Controlling Remote Access

Remote access to State of Nebraska computer resources and information shall be controlled to insure the integrity, availability and confidentiality (according to the sensitivity and criticality) of the information stored within, processed by or transmitted by a system.

Rule – Dial Up access needs Protection

Other than public access to general information, access by dial-up or Internet will require user authentication and encryption services to protect the confidentiality of the session.

Rule – Highest Risk Elements on the Network

Security for a connected network should reflect the security requirements of the highest risk elements on the network.

Rule – Isolating Sensitive Systems from Network

Your organizations computer systems containing secret information must not be connected to any network or any other computer.

Rule - Using Modems/ ISDN, DSL Connections

Sensitive information may only be sent via public telephone lines where more secure methods of transmission are not feasible. Both the owner and the recipient of the information must be informed prior to the tranmission.

Explanation/ Key Points

This rule relates to the dangers of using modems, ISDN links, and DSL connections to access public telephone networks to link diverse parts of your system.

These services provide an extension of your network, but use insecure public lines and increase the risk of attack.

Rule – Connecting Networks to Third Party Networks

Your organizations computers or networks may ONLY be connected to third party computers or networks after the proper approvals has determined that the combined system will be in compliance with your organizations security requirements.

Explanation/ Key Points

As a condition of gaining access to your organizations computer network, every third party must secure its own connected systems in a manner consistent with your organizations requirements. Your organization reserves the right to audit the security measures in effect on these connected systems without prior warning. Your organization also reserves the right to immediately terminate network connections with all third party systems not meeting such requirements.

Rule – Inventory of Connections to External Networks

IS should maintain a current inventory of all connections to external networks including telephone networks, EDI networks, intranets, extranets, and the internet.

Rule – Contact Numbers in Directories

Information regarding access to your organizations computer and communication systems, such as dial-up modem phone numbers, is considered confidential. This information must NOT be posted on the Internet, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the advance proper approvals. Telephone numbers, fax numbers, and internet electronic mail addresses are permissible exceptions.

Rule – Extended User Authentication Systems for Dial Up

To positively identify the calling party, all dial-up connections to your organizations internal computer data network must employ extended user authentication. These systems include call-back devices, dynamic password software, identity tokens (smart cards), biometrics (thumb-print readers, eye blood vessel readers, voice print readers, etc.), and other approved technologies which provide more security than traditional fixed password systems.

Rule – Use of Cable Modems

Cable modems must not be used for any of your organizations business communications unless a firewall and a virtual private network (VPN) is employed on the involved computers.

Rule - Using Encryption Techniques

Where appropriate, sensitive information should always be transmitted in encrypted form, especially prior to transmission.

Rule – Connecting Modems to Network Prohibited

The IS technical staff are prohibited from connecting dial-up modems to workstations which are simultaneously connected to a local area network (LAN) or another internal communication network.

Rule – Modem Pools

With the exception of portable computers and telecommuting computers, the use of local modems to establish direct dial connections is prohibited. All dial-up connections with your organizations systems and networks must be routed through a modem pool which includes an approved extended user authentication security system.

Rule – Answer on Fourth Ring

All of your organizations dial-up modems must not answer in-coming calls until the {4th} ring. This will thwart people who seek to gain unauthorized access to your organizations computers with programs that identify computer-connected telephone lines. Because the modems don't pick up right away, these programs will erroneously conclude that these modem lines are voice lines.

Cyber Crime Rules

Rule - Defending against Cyber Crime

Plans are to be prepared, maintained and regularly tested to ensure that damage done by possible external cyber crime attacks can be minimized and that restoration takes place as quickly as possible.

Explanation/ Key Points

Even the most ISS conscious organizations can be attacked: this may be to 'prove a point' or for other malicious reasons.

Successful cyber attacks are likely to result in either a loss or corruption/ theft of data, and possibly the disabling of services.

Cyber crime can have a severe and immediate impact on your systems. Without proper planning for such events, your business may not be able to recover within an acceptable timeframe.

Rule - Defending against Premeditated Internal Attacks

In order to reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed and maintained at all times.

Explanation/ Key Points

Identifying staff actions as criminal is beset with difficulties. Access to confidential data may be legitimized in employee job descriptions. The act of copying sensitive data may not necessarily leave a "footprint" on the system and such copies can then be exported from your organization by e-mail or by removable media without leaving a trace. The effects of outright malicious data destruction are obvious, but the computer entry process of so doing may have seemed routine.

A member of your staff (?) may target confidential information, or deface the organizations web site, which could result in both financial loss and embarrassment and possibly legal proceedings.

The principle means of building defenses against internal malicious attacks includes strong access control, high levels of staff awareness and vigilance.

Rule – Defending Against Opportunistic Cyber Crime Attacks

It is a priority to minimize the opportunities for cyber crime attacks on the organizations systems and information through a combination of technical access controls and robust procedures .

Explanation/ Key Points

Opportunistic criminal attacks usually arise from chance discovery of a loophole in the system, which permits access to unauthorized information.

Your web site or data processing systems may be penetrated, allowing both the disclosure of sensitive information and also possibly the modification or corruption of the data. All such events can lead to public embarrassment and financial loss.

Without an effective risk management process, it may be impossible to identify weak security defenses before they are breached.

Rule - Defending against Denial of Service Attack

Contingency plans for a denial of service attack are to be maintained and periodically tested to ensure adequacy .

Explanation/ Key Points

A denial of service attack (DoS) is an attack against a system whereby a client is denied the level of service expected. This is sometimes thought of as overloading the system not allowing any transactions or requests to take place.

In a mild attack, the impact can be unexpectedly poor performance. In a worse case attack, the server can become so overloaded as to cause the system be crash.

DoS attacks do not usually have theft or corruption of data as their primary motive and will often be executed by persons who have a grudge against the organization.

Denial of Service (DoS) attacks have gained notoriety as being an effective way to disable web-based services. Your web server(s) may be subjected to a DoS attack, which could result in damage to your organizations reputation and also financial loss.

It is important that the responsible IS technical staff designated to handle DoS attacks are properly trained so normal service can be restored within an acceptable period.

Rule - Defending against Hackers

Risks to the organizations systems and information are to be minimized by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices .

Explanation/ Key Points

Unlike other forms of cyber crime, these attacks take a “scatter gun” approach in that they do not target a specific organization. If you happen to be “in the firing line” and your information Security safeguards are poor, you are likely to be hit.

Malicious code which can replicate itself may be downloaded unwittingly and executed. Having damages your system, it can continue to wreak havoc with the systems of other organizations and individuals.

E-mail may contain malicious code which may replicate itself to all addresses within your organizations e-mail system, and then corrupt the system of each recipient, without attachment even having been opened.

Rule - Defending against Premeditated External Attacks

Security on the network is to be maintained at the highest level. Those responsible for the network and external communications are to receive proper training in risk assessment and how to build secure systems which minimize the threats to cyber crime.

Explanation/ Key Points

There is a very high risk of external security breaches where network security is inadequate.

The best safeguard is to be sure to keep up with the latest software and patches to your virus checking software.

Rule – Testing for Viruses on a Stand-alone Computer

Whenever software and/or files are received from any external entity, this material must be tested for unauthorized software on a stand-alone non-production machine before it is used on your organizations information systems. If a virus, worm, or Trojan horse is present, the damage will be restricted to the involved machine.

Rule – Virus Checking at Firewalls, Servers, and Desktops

Virus screening software must be installed and enabled on all firewalls, FTP servers, mail servers, intranet servers, and desktop machines.

Rule – Two Virus Screening Software Packages

To assure that incoming viruses are immediately detected and eradicated, at least two virus screening software packages must be used at each point where electronic mail and other files enter your organizations network.

Rule - Floppy Virus Checking Decal

Externally supplied floppy disks may not be used on any PCs or local area networks (LAN) server unless these disks have first been checked for viruses and received a decal indicating that no viruses were found.

Rule – Integrity Checking Programs

To promptly detect and prevent the spread of computer viruses, all of your organizations personal computers (PCs) and servers must run integrity checking software. This software detects changes in configuration files, system software files, application software files, and other system resources. Integrity checking software must be continuously enabled or run daily.

Rule – Virus Checking Programs on PCs and LAN Servers

Virus checking programs approved by your security department must be continuously enabled on all local area network (LAN) servers and networked personal computers (PCs).

Rule – Decrypting Before Checking for Virus

All externally supplied computer-readable files (software programs, databases, word processing documents, spreadsheets, etc.) must be decrypted prior to being subjected to an approved virus checking process.

IMPORTANT: Many virus checking programs cannot detect viruses in encrypted files.

Rule - Write Protection and Virus

All software running on micros and workstations must be write-protected such that an error will be generated if a computer virus tries to modify the software. An exception to this policy will be made in those cases where the software must modify itself in order to execute.

Chapter 5
E-mail, Internet, and E-commerce Rules

About E-mail, Internet, and E-commerce

The internet is used for business purposes throughout most organizations. E-mail is the main way employees communicate within organizations today. Setting up internet and e-mail access, controls, and on-going monitoring can be a very large task.

The Role of the IS Department

The IS technical staff set up user access to the internet and e-mail. Only those users that have been given the proper authority can have access. IS must carefully consider access points, vulnerabilities, and safeguards for controlling access.

E-mail, Internet, and E-commerce Rules

E-mail Rules

E-mail Point of Entry Rule

The IS manager of the state's central address directory will provide the single point of entry for all state e-mail post offices other than the SMTP mail servers.

Rule -

In organizations that use central e-mail systems, managers of mail servers shall employ virus protection software to prevent transmission of viruses in e-mail attachments.

Rule – Intrusion Detection Systems

To allow your organization to promptly respond to attacks, all Internet-connected computers must be running an intrusion detection system approved by the security department.

Rule -

621. Internet Commerce Servers Must Be In Demilitarized Zone (DMZ) Rule: All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls in a demilitarized zone.

Rule -

622. Public Servers On Internet Must Be Placed On Separate Subnets Rule: Public Internet servers must be placed on subnets separate from internal networks. Routers or firewalls must be employed to restrict traffic from the public servers to internal networks.

Rule -

623. Internet Commerce Servers Must Use Digital Certificates & Encryption Rule: To prevent intruders from interfering with Internet commerce activities, all Internet commerce servers (web servers, database servers, payment servers, security servers, etc.) must employ unique digital certificates and must use encryption to transfer information in and out of these servers. An exception is made for web servers, FTP servers, and any other servers supporting communications with customers, prospects, or other members of the public.

Deleting and Destructing E-mail Rule

Internal correspondence must be disposed of when no longer needed.

Explanation/ Key Points

Multi-user electronic mail logs must be destroyed one year after being archived. Electronic mail messages relevant to current activities, or that are expected to become relevant to current activities, should be saved as separate files and retained as long as needed.

Rule - Contact Information on Web Site

Inclusion Of Information Security Contact Information On Web Site. The opening pages of all your organizations web sites must include contact information (email address, phone number, etc.) for the Information Security Department..

Rule - Using E-mail as a Database

You must regularly move important information from E-mail message files to word processing documents, databases, and other files. E-mail systems are not intended for the archival storage of important information. Stored electronic mail messages may be periodically expunged by IS systems administrators, mistakenly erased by users, and otherwise lost when system problems occur.

Rule – Recording and Retaining E-mail

725. Recording And Retention Of Electronic Mail. Rule: Your organizations systems administrators must establish and maintain a systematic process for the recording, retention, and destruction of electronic mail messages and accompanying logs. The destruction of both logs and the referenced electronic mail messages must be postponed whenever a subpoena, discovery motion, or other legal notice is received. Such destruction should also be postponed if the material might be needed for an imminent legal action.

Accepting Unsolicited Ideas via the Internet Rule

If a mechanism to receive comments or suggestions is provided on your organizations web sites, it must be accompanied by the following words: "The receipt of unsolicited ideas by your organization (Company ABC) does not obligate the company to keep these ideas confidential, nor does it obligate the company to pay the person who submits them."

Rule -

628. Internet Connections Require Approved Firewalls Rule: All connections between your organizations internal networks and the Internet (or any other publicly-accessible computer network) must include an approved firewall and related access controls.

Rule -

629. Trusted Host Relationships Prohibited For Internet Connected Machines Rule: Unless the Information Security Department Manager has approved, all your organizations computers that are Internet-connected or directly reachable through the Internet are prohibited from using shared directory systems, sometimes called shared file systems. These systems allow a user to obtain access to more than one computer's file system with only a single log-in process. Exceptions are made for Internet commerce and other systems where a multiple machine architecture involves automatically passing users with severely restricted privileges from one computer to another.

Rule -

702. Down-Loading Sensitive Information Prohibited Without Permission. Sensitive information may be down-loaded from a multi-user system to a microcomputer (PC) or a workstation ONLY after two conditions have been fulfilled. For this data transfer to take place, a clear business need must exist AND advance permission from the information owner must be obtained. This policy is not intended to cover electronic mail or memos, but does apply to databases, master files, and other information stored on mainframes, minicomputers, servers, and other multi-user machines. Any information that a user of a mainframe, minicomputer, or departmental server can display at the same time can often be captured on a hard drive or floppy disk at a microcomputer (PC) or a workstation. In the absence of viable generally-available technical controls to take care of this problem, this policy defines acceptable behavior. The policy thus relies on people rather than technological controls.

Rule -

Internet and E-mail Management

Rule - Setting up Intranet Access

Setting up your organizations intranet access must consider any access restrictions and security issues as you would the network.

Explanation/ Key Points

An intranet is a web based information service that is available only within your organization and its internal network. The use of an intranet raises the sameissues of security as the internet in that your intranet could permit unauthorized access to information.

Rule - Setting up Extranet Access

Setting up extranet access must consider any access restrictions and security issues as you would the network.

Explanation/ Key Points

An extranet is a semi-private web site and extends beyond an organizations internal network. It can provide access to outsiders like customers, suppliers, or third parties via a User ID password, or such other means.

Rule - Setting up Internet Access

Setting up internet access should only be given to those that have been authorized to have access.

Explanation/ Key Points

All users with internet access should be made aware of the rules around acceptable internet behavior. Accessing the internet raises many security issues. The dangers from downloading are potential threats and should be safeguarded against intruders.

Full time connection to the internet should be avoided as it offers unlimited opportunity for intruders.

Rule - Developing a Web Site

The IS technical staff that develop your organizations web site(s) should be aware of accessibility to/ from the web site. Each web site should always display contact information.

Rule - Web Browsers

Web browsers are to be used in a secure manner with the appropriate setting.

Explanation/ Key Points

Web browser software can be paths through an organizations security shield. The security issues are in the areas of cookies, java scripts, and controls.

Rule -

Using External Service Providers for E-commerce

Rule - Downloading Internet Files and Information

When you download software and files from the internet, they must be screened with virus detection software. This screening must take place prior to being run or examined via another program such as a word processing package.

E-Commerce Rules

📖 **Rule -**

Structuring E-commerce Systems including Web Sites

📖 **Rule -**

Structuring E-commerce Systems including Web Sites

📖 **Rule -**

Securing E-commerce Networks

📖 **Rule -**

Securing E-commerce Networks

📖 **Rule -**

Configuring E-commerce Web Sites

📖 **Rule -**

Using External Service Providers for E-commerce

Chapter 6
Workstation and Equipment Rules

About Workstation and Equipment

Users workstations and other equipment are the responsibility of the IS department to install, maintain, and test.

The Role of the IS Department

The IS technical staff support the users workstation and equipment. If the equipment is old, they are required to dispose of the equipment in the proper fashion.

Workstation and Equipment Rules

Media Security Rules

You will find general usage regarding diskette and CD media security in the Computer Users Security Handbook. This section is for the IS department and covers larger media, and those that are more critical and / or used less often.

Rule - Using Removable Storage Media

Only those IS technical staff that are authorized should remove data from the network. When using removable storage media, there are security risks associated with the portability of the media. The media itself needs to be protected, as well as the information it contains.

Disposal Rules

IS has to be very careful is disposing of software and hardware. Disposing of small media like diskettes and CDs is covered in the *Computer Users' Security Handbook*.

When data space in reused with new information, it is called object reuse. Disposal of any equipment that has been used and reused involves erasing the remaining data that has not been removed or overwritten.

Rule - Zeroization of Password Materials

If passwords or Personal Identification Numbers (PINs) are generated by a computer system, special care must be taken to erase all residual data used in the process. All computer storage media (magnetic tapes, floppy disks, etc.) used in the construction, assignment, distribution, or encryption of passwords or PINs must be "zeroized" immediately after use.

Explanation/ Key Points

Zeroization means that the media must be repeatedly overwritten with a series of ones and zeros. Additionally, computer memory areas used in the derivation of passwords or PINs must be zeroized immediately after use.

Rule - Disposal of Obsolete Equipment

Equipment owned by your organization may only be disposed of by authorized technical staff who understand the information security risks. This applies for disposal to scrap or to others to use.

Explanation/ Key Points

Legacy data can still remain on old PC hard rive, storage media, tapes, or other IS media devices.

Rule – Information Destruction

IS is responsible for the prompt and proper disposal of surplus property no longer needed for business activities. Disposal of information systems equipment must proceed in accordance with procedures established by the security department, including the irreversible removal of information and software.

Rule – Destruction of Records

IS technical staff should not destroy or dispose of potentially important records or information without specific advance management approval. Unauthorized destruction or disposal of your organizations records or information will

subject the perpetrator to disciplinary action. Records and information must be retained if: (1) they are likely to be needed in the future, (2) regulation or statute requires their retention, or (3) they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts.

Destruction is defined as any action which prevents the recovery of information from the storage medium on which it is recorded (including encryption, erasure, and disposal of the hardware needed to recover the information).

Rule – Object Reuse

Reusing data space is a common practice as long as your are aware of the contents prior to disposal.

Rule - Using External Disposal Firms

Any third party used for external disposal of the organizations obsolete equipment must meet the IS standards and disclose their method of disposal.

Rule - Disposing of Software

The disposal of software should be carefully planned. Be sure it is no longer needed and the associated data files which may be archived will not require restoration in the future.

Rule – Sensitive Information Destruction Before Servicing

Before computer magnetic storage media is sent to a vendor for trade-in, servicing, or disposal, all your organizations sensitive information must be destroyed or concealed according to approved methods.

The intention of this rule is to ensure that sensitive information is not unwittingly disclosed to unauthorized persons working for vendors, charities, and other third parties. For example, if a hard disk drive were to crash, the drive might be sent to a computer repair service. The service company could examine the data on the drive, perhaps leading to unauthorized disclosure of sensitive information. To counter this risk, the drive could be degaussed prior to being sent to the service vendor. Of course, then the data held on the drive, that has not yet been backed-up, will be lost (this is a major disadvantage of the rule). Such sensitive information destruction makes sense only if the information has been properly backed-up or if the consequences of disclosure are very severe. A more practical alternative would be to require that all hard drives storing sensitive data employ encryption, in which case there is no problem about sending the drive to an outside vendor. This is why the word "concealed" is included in the rule in addition to the word "destroyed."

Another approach is to require confidentiality agreements (NDAs) from all third parties.

Rule – Sensitive Information Disposal

Computer storage media which has been used to record sensitive information must not leave controlled channels until it has been degaussed (demagnitized) or zeroized according to the standards published by the security department.

This rule establishes the notion of a controlled channel for the custody of sensitive information. Degaussing involves subjecting magnetic storage media such as floppy disks to a strong magnetic field which will then erase the information stored thereon. Zeroization involves overwriting the storage media with repeated sequences of zeros and ones, thereby obliterating the data.

Rule – Zeroization for Erasure of Sensitive Information

When sensitive information is erased from a disk, tape, or other magnetic storage media, it must be followed by a repeated overwrite operation which prevents the data from later being scavenged.

With most operating systems, standard disk file "delete" and "erase" commands simply delete the entry in a file allocation table (FAT) or directory; the information in the file is still resident on the computer media. A notable aspect of using this overwriting process (known as "zeroization") to obliterate sensitive information is that it can be programmed to happen automatically. A command file can be written to automatically scrub data storage media, using zeroization, each time that a sensitive file or other object (database, program, etc.) is erased. Some operating systems do this automatically; for example, IBM's RACF for MVS will "erase-on-scratch" those files which have been designated as in need of this protection. The user need not be aware of this process. Alternatively, in the absence of an automated approach, users can invoke an approved zeroization software utility to handle this "scrubbing" process whenever sensitive data is involved. The intention of this rule is thus to prevent unauthorized disclosure of sensitive information from computer media scavenging, whether the process is handled automatically or by the end-users.

Rule – Erasing before Giving to a Third Party

Before information systems equipment or storage media which has been used for your organizations business is provided to any third party, the equipment or media must first be physically inspected by IS to determine that all sensitive information has been removed. This rule does not apply when a non-disclosure agreement (NDA) has been signed by the third party.

Rule – Hardcopy Sensitive Information Disposal

When disposed of, all sensitive information in hardcopy form (paper, microfilm, microfiche, etc.) must be either shredded or incinerated.

The intention of this rule is to prevent "dumpster diving" (the popular going-through-the-trash scavenging approach to recovering passwords, user-IDs, and other sensitive information). Scavenging information from the trash is a favorite tactic of hackers, private investigators, industrial spies, military spies, and the police. In many jurisdictions it is both legal and a successful method for gaining important information. In a related standard, many organizations specify the type of shredding required (for example, the pieces produced must be a certain size or smaller).

Rule – Person Authorized to Destroy Sensitive Information

To ensure that it is in fact performed, the destruction of sensitive information must be carried out by your organization designated IS technical staff or a bonded destruction service.

Explanation/ Key Points

The intention of this rule is to make sure that a trusted individual or organization is used for all sensitive information destruction efforts. There have been cases where destruction services did not shred sensitive data, instead simply dumping it in landfill. Others then discovered this sensitive information much to the dismay of the originating organization. To prevent such problems, this rule requires an employee or a destruction service that has gone through a background check and has received insurance (the bonding process).

Chapter 7
Systems Development Rules

About Systems Development

Systems development is the main function of the IS department. This involves programming software for business use. It also includes software packages that have been purchased for use with your organizations data. Many times these software packages require additional system development for customization purposes.

The Role of the IS Department

One of the main roles of the IS department is to create new software systems for the business processing. Programming, debugging code, and testing the software functionality are all common tasks in the life of the IS technical staff.

Systems Development Rules

Software Development Rules

Rule – Software Development

Software developed must always follow a formalized development process. The integrity of the organizations operational software code must be safeguarded.

Explanation/ Key Points

Sometimes a minor modification can become a large programming effort. When programmers work independently from each others, controls are even more required.

Rule – Development Security Requirements

Before a new system is developed or acquired, management of the user department(s) must have clearly specified the relevant security requirements. Alternatives must be reviewed with the developers and/or vendors so that an appropriate balance is struck between security and other objectives (ease-of-use, operational simplicity, ability to upgrade, acceptable cost, etc.).

Rule – Compliance with Internal Conventions

Management must ensure that all software development and software maintenance activities performed by in-house staff subscribe to your organization policies, standards, rules, and other systems development conventions.

Rule - In-house Developed Software Notice of Failure

Whenever software developed in-house fails to produce the expected results, it must always provide either an error message or some other indication of failure, one or both of which must be presented to the user.

Rule - In-house Developed Software Feedback

Whenever software developed in-house receives input from a user, some sort of feedback must be provided. If input from a user indicates a request, the user must always receive feedback indicating whether the request was performed.

Rule - In-house Developed Software Formal Specs

All software developed by in-house staff, and intended to process sensitive, valuable, or critical information, must have a written formal specification. This specification must be part of an agreement between the involved information owner(s) and the system developer(s). A first draft of the agreement must be completed and approved prior to the time when programming efforts begin.

Rule – Remove Unauthorized Access Paths to Production

Prior to moving software which has been developed in-house to production status, programmers and other technical staff must remove all special access paths so that access may only be obtained via normal secured channels. This means that all trap doors and other short-cuts that could be used to compromise security must be removed. Likewise, all system privileges needed for development efforts -- but not required for normal production activities -- must be removed.

Rule – Use of High Level Programming Languages

The use of higher level computer programming languages reduces the volume of code that must be developed, the difficulty of software maintenance, the time required to develop an application, and the number of bugs. (?)

Rule – Production Files Naming Conventions

A file naming convention must be employed to clearly distinguish between those files used for production purposes and those files used for testing and/or training purposes.

Rule – Special Labeling for Non-production Business

Transactions used for auditing, testing, training or other non-production purposes must be labeled and/or otherwise separated from transactions used for production processing. This will help ensure that your organizations records are not improperly updated by non-production transactions.

Rule – System Interruption

Robots and other computerized machinery must be programmed so that the current activity immediately stops if the activity is harming or is likely to harm someone or something.

Rule – Restricted Use of Diagnostics

Diagnostic tests of hardware and software, such as communications line monitors, must be used only by authorized personnel for testing and development purposes. Access to such hardware and software must be strictly controlled.

Rule – Systems Utilities Prohibited from Production Storage

Disks and other on-line storage facilities used on production computer systems must NOT contain compilers, assemblers, text editors, word processors, or other general purpose utilities which may be used to compromise the security of the system.

Rule - Separation of Programming and Development Environments

Business application software in development must be kept strictly separate from production application software. If existing facilities permit it, this separation must be achieved via physically separate computer systems. When computing facilities do not allow this, separate directories or libraries with strictly enforced access controls must to be employed.

Rule - Separation of Programming and Testing Environments

Production business application software in development must be kept strictly separate from this type of software in testing. If facilities permit it, this separation must be achieved via physically separate computer systems. When computing facilities do not allow this, separate directories or libraries with strictly enforced access controls must be employed.

Rule - System Developers and Production

IS technical staff that develop business application software must not be permitted to access production information, with the exception of the production information relevant to the particular application software on which they are currently working.

Rule - System Developers and Testing

IS technical staff who have been involved in the development of specific business application software must not be involved in the formal testing or day-to-day production operation of such software.

Data Management Rules

🕮 Rule - Managing Databases

The integrity of the organizations databases must be maintained at all times.

🕮 Rule - Amending Directory Structures

Data directories and folders may only be changed by the appropriate technical staff.

Explanation/ Key Points

The directory structure is a roadmap to the storage and access to files and data. Any unauthorized changes to data paths can cause access rights to be circumvented.

🕮 Rule - Setting up New Databases

Databases must be carefully stored, housed and tested when they are initially set up. Databases are set up for data storage, retrieval and reorganization so should consider the sensitivity of the data and its usage.

IS Software Rules

🕮 Rule – Risk Analysis of New Technology

(…)

🕮 Rule – Purchasing and Installing Software

(…)

🕮 Rule - Selecting Business Software Packages

All business software packages should meet your organizations security, technical, and business operating requirements.

🕮 Rule - Using Licensed Software

To comply with legislation and to receive continued vendor support, the terms and conditions of all vendor licensed software are to be strictly adhered to.

Explanation/ Key Points

Using unlicensed software can be a criminal offense.

IS Hardware Rules

Rule - Purchasing and Installing New Hardware

The purchase of new computers and peripherals requires careful consideration to your organizations business needs and the security required to protect it.

Explanation/ Key Points

New systems must have adequate capacity, performance reliability, maintenance and safeguards. All new equipment should follow technical standards set forth by IS. All major purchases should be evaluated by IS, including a detailed technical requirements document.

Rule - Maintaining Hardware

All equipment owned, leased, or licensed by your organization must be supported by appropriate technical staff.

Explanation/ Key Points

Rule - Moving / Relocating Hardware

Any moving of equipment between your organizations locations must be strictly controlled by the appropriate technical staff to ensure proper handling and re-installation.

Rule – Specifying ISS Requirement for New Hardware

(…)

Rule – Specifying Functional Needs for New Hardware

(…)

Software Maintenance / Upgrades Rules

Rule - Applying Patches to Software

Patches to resolve software bugs may only be applied with careful planning, testing and coordinating into the production system.

Rule - Implementing New/ Upgraded Software

The implementation of new or upgraded software must be carefully planned, managed and retested.

Explanation/ Key Points

All software, from operating system to applications needs to be upgraded. Adequate training should be incorporated for both technical and user staff. Software companies are always releasing software fixes or introducing new versions of functionality.

Rule - Change Control Process

(…)

Rule – Specifying ISS Requirement for New Software

(…)

Rule - Responding to Vendor Recommended Software Upgrades

The decision to upgrade software is only to be taken after weighing the risks to the anticipated benefits and necessity for such a change.

Rule - Interfacing Applications Software/ Systems

Developing interfacing software systems is a highly technical task and should only be done be authorized staff.

Explanation/ Key Points

Many software packages can exchange data and link with a variety of popular systems. Such interfaces may require data to be exported from one system, then massaged, and finally imported into the target system. This can put data at great risk.

Rule - Operating System Software Upgrades

Necessary upgrades to the operating system must have the associated risks identified and and be carefully planned, incorporating tested fall back procedures.

Explanation/ Key Points

This is a critical rule as it effects all applications running in that environment.

Rule - Managing Program Libraries

Only designated technical staff may access operational program libraries within your system where you keep the source code of your live systems. Live and development libraries should always be kept separate.

If your program libraries are poorly protected, your information could be modified in error.

Rule - Controlling Software Codes

During software development, formal change control procedures must be authorized and tested. Software coding standards should always be adhered to.

Rule - Controlling Program Listings

Program listings must be kept current at all times. Controlling the printouts or reports of the application source code should be kept in a secured area.

Rule - Controlling old Versions of Programs

Formal change control procedures with comprehensive audit trails are to be used to control versions of old programs. Beware of old versions of programs that may be obsolete.

Rule - Managing Change Control Procedures

Formal change control procedures must be used for all changes to systems. Change control assumes that all changes are analyzed and authorized.

Explanation/ Key Points

Seemingly harmless changes to software code can introduce weaknesses that could go unnoticed. If formal change control procedures are not implemented, it can be very difficult to manage change and accompanying safeguards.

Rule - Separating Duties - Systems Development

IS must have separation of duties dealing with systems development, systems operations, and systems administration. It is important to separate these functions.

Explanation/ Key Points

IS technical staff often have high privileges, so could potentially be high risk to other areas.

Rule – Complying with Copyright and Software Licensing

(…)

Rule – Other Business Activities

Information about the nature and location of your organizations information, such as that found in a data dictionary, is confidential and must only be disclosed to those who have a demonstrable need-to-know.

System Testing Rules

All new systems development needs extensive testing to debug errors and test for reliability and completeness.

Rule - Testing Third Party Software

Prior to distributing any software or information in computerized form to third parties, IS must first have completely tested the information, including comprehensive scanning to identify the presence of computer viruses.

Rule – Software Testing with Sensitive Data

All software testing for systems designed to handle Highly Restricted or Confidential information must be accomplished exclusively with sanitized production information. Sanitized information is production information which no longer contains specific details that might be valuable, critical, sensitive, or private.

Rule - Testing System Controls Prohibited

IS must not test, or attempt to compromise internal controls unless specifically approved in advance.

Rule - Controlling Test Environments

The IS testing environment must be a controlled, simulated environment to the live environment into which it will be implemented. System testing should be kept separate from live production.

Rule - Using Live Data for Testing

You should never use the live, production system for testing purposes. A copy should be made and used in the test system.

Explanation/ Key Points

IS should use data for testing purposes that is an exact replica of the live data. The only way to properly test applications is with simulated live data.

The acquisition of data for testing may breach the security safeguards of your live system. Be careful to never merge test data into the live database.

Rule - Testing Systems and Equipment

All equipment must be tested and accepted by the user before it is transferred to the live environment.

Explanation/ Key Points

New hardware should be tested thoroughly to be sure it is working properly. On-going testing and diagnostics should be run to keep the equipment in good running order.

Inadequate testing can threaten the integrity of your data.

Rule - Capacity Planning / Testing of New Systems

New systems must be tested for capacity, peak loading, and stress testing. They must demonstrate a level of performance that meets the technical and business needs.

Rule - Parallel Running

Normal system testing procedures will incorporate a period of parallel running prior to transferring to the live system. The results of parallel running should not reveal problems or difficulties.

Explanation/ Key Points

Parallel running is the process of running the new system simultaneously with the old system to confirm and validate it is working correctly before going into live production.

Systems Documentation Rules

Rule - Systems Documentation Security

Documentation that discloses systems processes and usage must be secured in a locked cabinet or other protected area.

Explanation/ Key Points

Although documentation for system operations and technical requirements should be made available and current, it must also be secured.

Rule - Maintaining a Hardware / Software Inventory

A register should exist that lists all software, hardware, communications, and database assets.

Explanation/ Key Points

This inventory list will greatly facilitate the Business Impact Analysis task of your ISS program. If there has been a theft of any hardware or software, you will have this inventory to use as a replacement list. This list will allow you to make better decisions, like amount of insurance coverage. An inventory list also helps IS plan for future technology changes/ upgrades.

Rule – Hardware Documentation

Hardware documentation must be kept current and readily available to the technical staff that are authorized to use it, yet in a secured area

Explanation/ Key Points

Hardware documentation includes all operating and technical manuals provided by the hardware vendor and any internal documentation written to customize the vendor manuals for your organizations use.

Keeping hardware maintenance is important to your organizations infrastructure.

Rule - Documentation Version Control

Version control should be an integral part of the documentation process. This provides a status of the documents and control over its distribution.

Rule – Required Documentation for Production

Every IS technical staff that develops or implements software and/or hardware to be used for your organizations business activities must document the system in advance of its deployment. The documentation must be written so that the system may be run by persons unacquainted with it. Such documentation must be prepared even when standard software--such as a spreadsheet program--is employed.

Chapter 8
Disaster Recovery Rules

About Disaster Recovery

All businesses are subject to disasters of all types. Disasters come in many forms - natural, terrorist, accidental, and intentional. In order to preserve the organizations information, it is critical to have a disaster recovery plan to get the operations of the business up and running as soon as possible.

The Role of the IS Department

The IS technical staff and the security department will probably make up the team that plans, designs, and implements your contingency and disaster recovery program.

Continency Planning

All IS departments need to have a contingency plan. This contingency plan not only temporarily takes over the processing of the business, but also handles the tasks for business resumption to get the main systems fully functional as quickly as possible.

Disaster Recovery Plan

The reason for a Disaster Recovery Plan is to rapidly recover your operations from a disaster. This will almost always involve restoring information from backups.

Each organization must have a disaster recovery plan that at least identifies and militates against risks to critical systems and sensitive information in the event of a disaster. The plan shall provide for contingencies to restore information and systems if a disaster occurs. The disaster recovery plan for information technology may be a subset of an organizations comprehensive disaster recovery plan. The concept of a disaster recovery includes business resumption.

The Security Officers usually pParticipate in preparing a disaster recovery plan. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan.

Disaster recovery plans must serve several core principles. These include:

- Information is an asset. It has value to the organization and needs to be suitably protected.

- Information resources must be available when needed. Continuity of information resources supporting critical services must be ensured in the event of a disruption to business or a disaster, which makes critical systems unavailable.
- Risks to information resources must be managed. The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected.

Testing the Plans

Your organization contingency and disaster recovery plans must be constantly tested as technology and business practices change.

Responding to Disaster

The response team outlined in *Chapter 3 Incident Reporting* must be well trained and have sufficient practice to be able to react in an emergency.

Disaster Recovery Rules

Disaster Recovery Rules
Back up Rules
Off-Site Storage Rules

Disaster Recovery Rules

Rule - Human Factor

The human factor needs to be taken into account when planning a disaster recovery plan. Redundancy is needed in people as well as systems. There must be multiple people to do a specific task.

Rule - Managing Data Storage

IS must store and backup daily business work and transactions.

Rule - Doing a Business Impact Analysis

IS should do a business impact analysis, including risk assessment, asset classification, and potential disruption to stakeholders.

Rule - Classification System

IS should do a classification of data system to identify critical systems and essential records.

Rule - Safeguards

Safeguards should include protective measures such as redundancy, fire suppression, uninterruptable power supply (UPS), surge protection, and environmental measures to protect sensitive equipment from dust, temperature or humidity.

Rule - Business Resumption

(…)

Rule - Contingency Plans for Different Types of Disruption

(…)

Rule - Implementing a Disaster Recovery Plan

(…)

Rule - Escalating Responses

Procedures should be put in place for implementing the disaster recovery plan and escalating your organizations response to a disaster.

Rule - Multiple Site Storage of Backup Documents

(…)

Rule - Disaster Recovery Plan – Training, Testing, Practice

A disaster recovery plan needs to be written, tested with different types of disasters, and practiced with multiple disasters and unexpected complications.

Rule - Disaster Recovery Plan Annual Review and Revision

(…)

Rule - Identifying Sensitive Information

User department managers must identify and maintain a current list of the vital records that their department needs to restore operations following a disaster.

Off-Site Storage Rules

Offsite storage of information is a basic rule of disaster survival. All the information, systems, infrastructure, configuration of systems necessary to rebuild the information system should be kept off-site. It is necessary to be able to conduct your business from an alternate location.

Rule - Physical Separation of Sites

Physical separation between the primary site and the recovery site is critical to the quality of the disaster recovery plan. There must be enough separation that both sites won't be hit by the same disaster. The minimal amount of off-site storage should be backups and a standby system.

Rule - Off Site Storage

Backups of essential business information and software must be stored in an environmentally-protected and access-controlled site which is a sufficient distance away from the originating facility to escape a local disaster.

Backup, Recovery and Archived Data Rules

Your organization should never lose more information than that which has changed since your last backup. Backups are fundamental to the installation of new systems and after the destruction of your existing systems.

The amount of backup methods depends on the value of your information (the cost to re-create it):

How often to do a backup depends on your organizations needs. It is usually done daily, and monthly. The storage process of the backup, number of generations and location are all factors in the backup process.

The scope of backups can be full, incremental, or differential (?) backups. What information is being backed up can change from organization to organization.

Rule - Backup all New Software

All software must be copied prior to its initial usage, and such copies must be stored in a safe and secure location. These master copies must not be used for ordinary business activities, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.

Rule - Frequency of Backing up Data

(…)

Rule - Backing Up on Portable Computers

It is the responsibility of the user to be sure that information on their portable computer is backed up. IS should advise the user when the laptop or other such equipment is issued.

Rule - Managing Backup and Recovery Procedures

Backup of the organizations data files and the ability to recover such data is important. A structured backup and recovery process should be put in place.

Rule - Backup and Recovery of your Systems

Information owners must ensure that backup and recovery procedures are in place. The proper safeguards must be incorporated to protect the integrity of the data after recovery and restoration of the files, especially where these files may replace more recent files.

Rule - Archiving Information

The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered.

This refers to information that is not required day to day, but needs to be available for a certain period of time. To move this information to archives, reduces the overhead of daily information processing.

Rule - Archival Storage

The computer data media used for storing sensitive, critical, or valuable information must be high quality and must be periodically tested to ensure that it can properly record the information in question. Used data media that can no longer reliably retain information must not be used for archival storage.

Rule - Preserving Data in Archival Storage

Computer media storage procedures must assure that sensitive, critical, or valuable information stored for prolonged periods of time is not lost due to deterioration. For instance, management must copy data to different storage media if the original backup media is showing signs of undue deterioration.

Rule – Users Restoring Data

If users are given the ability to restore their own files, they must not be given privileges to restore other users' files or to see which files other users have backed-up.

Rule – Backup Frequency

All critical business information and critical software resident on your organizations computer systems must be periodically backed-up. These backup processes must be performed at least every {1} day, and with sufficient frequency to support documented contingency plans.

Rule – Two Backup Copies

At least two recent and complete backups (not incremental backups) made on different dates containing critical records must always be stored off-site.

Rule – Users Backing Up

IS should review all user backups to make sure that proper backups of sensitive, critical and valuable data are being made if such data is resident on microcomputers (PC), workstations, or other small systems.

Rule – Automatic Backup to Network

All users with access to a local area network (LAN) connections must leave their work on the network so that an automatic backup can be performed.

Rule – Users Notified of Backups

To prevent accidental loss, all files and messages stored on your organizations systems are routinely copied to tape, disk, and other storage media. All users need to be made aware of this backup process. This means that information stored on your organizations systems, even if a user has specifically deleted it, is recoverable and may be examined at a later date by systems administrators and others designated by management.

Rule – Archive Retention

Critical business information and critical software must be backed-up onto archival storage media and kept for at least {1} year. These backups must be made every calendar quarter or more frequently if required by a relevant written contingency plan.

Rule – Fire Zones and Backups

Computer and network backup storage media must be stored in a separate fire zones from the machine producing the backup. Fire zones vary from building to building.

Rule – Information Retention

Information must be retained for as long as necessary but for no longer. Information must be destroyed when no longer needed--generally within {2} years.

Rule – Regular Purging of Information

All information must be destroyed or disposed of when no longer needed. IS must review the value and usefulness of the information on a periodic and scheduled basis and follow purging requirement when it is no longer needed.

Chapter 9

Physical Security/ Premises Rules

About Physical Security/ Premises

Security is required not only for software and information, but also for the physical security of equipment. All organizations must develop and implement rules which include at least the following:

- Restrict physical access to computer facilities where continued operation is essential or where sensitive or confidential data are stored online.
- Restrict access to computer facilities to agency employees or agents who need such access to perform assigned work duties.
- Restrict access to software documentation and data storage to state employees or agents who need such access to perform assigned work duties.)

The Role of the IS Department

The IS department requires extensive physical security to protect the systems and equipment. Typically, the IS computer operations area is highly restricted due to the important and costly equipment that is used. These physically secured room usually contain large data storage devices, high speed printers, tape drives, and complicated cabling and networking devices.

Physical Security/ Premises Policy Statements

Building/ Room Access
Environmental Rules
Working with (external) Security Organizations
Working with Security Equipment

Building/ Room Access Rules

Rule – Propped Open Doors to Computer Room

Whenever doors to the computer center are propped-open (perhaps for moving computer equipment, furniture, supplies, or similar items), the entrance must be continuously monitored by an employee or a contract guard from the IS and security department.

Rule – Network Components Protection

Control units, concentrators, multiplexers switches, hubs, and front-end processors will be protected from unauthorized physical access.

Rule - Supplying Continuous Power to Critical Equipment

An uninterrupted power supply (UPS) should be installed, in particular for sensitive data, to ensure continuity of services during power outages.

Rule – Environment Controls

Access to every office, computer room, and work area containing sensitive information must be physically restricted. Management responsible for the staff working in these areas must consult the proper authorities to determine the appropriate access control method (receptionists, metal key locks, magnetic card door locks, etc.).

Rule - Managing and Maintaining Backup Power Generators

Where necessary, secondary and backup power generators (standby) are to be employed to ensure continuity of services during power outages and in the event the UPS fails.

Explanation/ Key Points

If the main power supply fails, and the UPS fails, your system will crash without a backup power supply.

Environment Rules

Rule – Environment Controls

All equipment must reside in an environmentally security area with regards to conditions, proper air ventilation, temperature, and such.

Rule - Sensitive Information Prohibited from Network Printer

Sensitive information should never be sent to a network printer. The only safeguard is to have someone present at the printer to retrieve the document immediately after it has printed.

Rule - Installing and Maintaining Network Cabling

Network cabling should be installed and maintained by qualified engineers to ensure the integrity of the cabling and the connection points.

Explanation/ Key Points

Network cabling remains a vulnerable target as it is usually exposed and unprotected. Sometimes the damage is accidental and it can threaten data processing .

Rule – Scanning for Modems

You can scan to find modems per PC workstation and servers to check for standards, inventory of modems, and such.

Rule – Hard Drive Security

All information storage media (such as hard disk drives, floppy disks, magnetic tapes, and CD-ROMs) containing sensitive information must be physically secured when not in use. An exception will be made if this information is protected via an encryption system approved by the security department.

Working with (external) Security Organizations – ex. Guards

Rule -

959. Reporting Lost/Stolen Identification Badges And System Access Tokens Rule: Identification badges and physical access cards that have been lost or stolen--or are suspected of being lost or stolen--must be reported to the Security Department immediately. Likewise, all computer or communication system access tokens (smart cards with dynamic passwords, telephone credit cards, etc.) that have been lost or stolen--or are suspected of being lost or stolen--must be reported to the Security Department immediately.

Security Equipment Rules

(cameras, video surveillance, motion detectors, remote web viewing, …)

(General discussion about Misc. Equipment and IS. Miscellaneous equipment refers to cabling, UPS, Printers, and Modems, …)

Chapter 10
Getting ISS Help

Getting ISS Help

You will probably receive this Guide in a training class or seminar. You can also use it on-going for a reference guide as you need it. This chapter is written to answer any questions you may have on your ISS program.

Call for ISS Support

☎ If you need to ask ISS questions, call (xxx) xxx-xxxx.

☎ If you need to report an incident, IMMEDIATELY call (xxx) xxx-xxxx.

Troubleshooting Chart

Problem/ Question	Explanation	See Chapter …
What should I do if … I see something suspicious or an actual incident in action?	Do not handle it yourself. IMMEDIATELY Call xxx xxx-xxxx or your manager.	2

Appendix

Appendix A – List of Rules

The following list is a summary of all the Rules in this Guide.

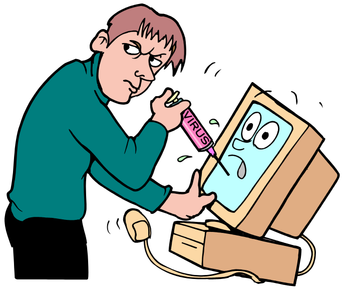
Access Control Rules

- 📖 Rule –
- 📖

Index

State of Nebraska

Information Security Systems (ISS)



Security Officer Instruction Guide

"A complete, easy-to-use instruction guide on how to use templates to develop and implement a successful ISS program."

Final Draft
August 24, 2001

This page is intentionally left blank for pagination of double-sided printing. 🗎

State of Nebraska
Information Security Guidelines

These Information Security Templates and Guides were developed by the Security Architecture Workgroup under a project funded by the Chief Information Officer and the Nebraska Information Technology Commission.

Additional information about these documents can be found at:
http://www.nitc.state.ne.us/tp/workgroups/security/index.htm

Computer User's Security Handbook

Version 1.0
August 24, 2001

Prepared by:

Table of Contents

This page is intentionally left blank for pagination of double-sided printing.

Chapter 1
Getting Started

The Importance of an ISS Program

Information Systems Security (ISS) has become more and more important to organizations. ISS is more than computer system security. It is the process of protecting all intellectual property of an organization. Dependence on information systems is integral in all business operations and it must be protected.

Securing Information in the Digital Age

The business environment is constantly changing. Relationships with other companies, outside affiliates, and worldwide access has made technology very complex to meet current and future needs.

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. Information and information technology systems are assets of vital importance to the institutions and government agencies and may impact each legislator, administrator, faculty, student, or patron that provides or relies on their services.

What makes up a good ISS Program?

What do you need to put the right security practices into your organizations business operations? Consider incorporating the following into your ISS program:

- Employee Awareness Program
- Incident Reporting
- Risk Assessment
- Response Team
- Security Tools and Materials
- Security Policies and Procedures

About your ISS Project

It is important that the security officer/ team get policy/management level support. This should include building and documenting a business case (justify the project) and preparing a project charter (RFP), budget, and organizational structure. See sample Charter in Appendix A - Attachments.

About the ISS Template Package

The ISS template package provides you with a comprehensive set of tools from which to develop and implement ISS practices into your business environment. This package provides a foundation upon which to build and protect the life blood of any organization – its information.

What are Information Security Templates?

The template package is an integrated suite of MS Word documents that guide you through the process of developing and implementing your ISS program. It helps you to integrate security best practices with your day-to-day operations by giving you a complete set of rules from which you can pick and choose those you wish to incorporate. The template package provides a solid foundation for the development and implementation of all areas of ISS – an awareness program, incident reporting program, policies and procedures, asset valuation and risk assessment.

What makes up the Template Package?

There are 3 guides make up the template package. They are:

- {*Security Officer Instruction Guide*}
- {*Computer User's Security Handbook template*}
- {*IS Technical Staff Handbook template*}

The {*Security Officer Instruction Guide*} is the main tool of the template package that gives instruction to the security officer on how to develop and implement the ISS program. Many sections provide checklists and work sheets to assist in the information gathering process.

The {*Computer User's Security Handbook template*} is the manual that will be given to all employees and contractors as part of the awareness program. This template needs to be reviewed and edited to meet the requirements of your organization. Any Rules you do not want to publish should be deleted. This guide can be handed out in awareness training, as part of the new hire package, and also as an ISS reference support tool.

The {*IS Technical Staff template*} is the manual that will be given to the IS department. It is assumed all IS employees will also be receiving the {*Computer User's Security Handbook template)* guide. This template also needs to be reviewed and edited to meet the requirements of your organization. Any Rules you do not want to publish should be deleted. This guide can be handed out in awareness training, as part of the new hire package, and also as an ISS reference support tool.

Technology Dependent

Many sections of the templates are left blank for you to complete with your organizations technology-specific instructions. The template structure was

developed to be independent of any technology you have implemented into your security systems.

Information Security Template Characteristics

- Do it yourself kit/ self-teaching
- Used as a starting point to tailor your own ISS program
- Not technology / person/ organization dependent
- Fill in the blank/ select and delete concept
- Example structure and category lists
- Suggested contents and examples
- Consistency with one template for all organizations
- Documentation standardization
- HIPAA compliance
- NITC approved
- Suggested implementation and training
- Written in MS Word and Visio
- Choice of formats and styles
- References and Glossary
- Working papers and checklists

Assumptions

- Knowledge of basic security practices
- Knowledge of MS Word

Benefits

- Standardization
- Others?

Information Security Template Requirements

- Office 2000 (could be earlier?) If you do not use Office 2000, you may experience problems.

Initial vs. Existing Guides

Using the Template for Initial Setup

(Notes: Describe first time user of the template package. Installation procedures?)

Using the Template to Update existing Manual

If you already have your policies and procedures written and in use, the template package can be used to incorporate them into this format.

Keeping the Template current

(Notes: Describe how we are going to keep the template current and re-distribute. Versions and releases, …)

(From NITC: Agency policy should establish a change control system for managing modifications to applications. The change control system should define the process for review and approval of code changes.)

ISS Policies and Procedures

ISS policies and procedures have been built into the template package. The contents of the template package reflect the NITC policies and standards outlined in the Security Architecture document.

Policies, Standards, and Rules

This section defines how we use the terms policy, standard, and rule throughout the templates.

Policy The 7 policies described in the NITC Security Architecture document provide the highest level structure and the basis from which all rules are organized and defined. *See NITC Security Architecture in Appendix.*

Standard The 7 policies in the NITC Security Architecture document are broken down into standards providing the middle level structure. *See NITC Security Architecture in Appendix*.

Rule Rules are the lowest level structure and a direct result of the policies and standards. They are organized by policy and are the most numerous.

Procedures

Procedures, or "how tos" are incorporated throughout the template package. Procedures are step-by-step instructions to perform a certain security task. Procedures can be followed with or without Rules. Rules can be dictated with or without Procedures.

Most of the procedures in this package are in the *Security Officer Instruction Guide*, complete with checklists and working papers. In the *Computer User's Security Handbook* and the *IS Technical Staff Handbook*, you can design the Rules with procedures in the full format, but initially they are "empty" since they are

technology-dependent. You can add your organizations procedures in the full format for any Rule.

The following procedures are incorporated into the template package:

- how to develop and implement an ISS program (See the *Quick Start Card*)
- how to do a risk assessment
- how to assemble a security team
- how to value asset inventories
- how to create an awareness program
- how to produce policies, standards, and rules
- how to develop awareness training
- how to implement an incident response / reporting program
- how to create ISS support materials
- how to keep your ISS program maintained (on-going)

About the Security Officer Instruction Guide

About this Guide

This guide provides the structure and the content for you to develop and implement your ISS program. This guide is designed for the Security Officer, regardless of the size of the organization, or any person responsible for the implementation and on-going maintenance of the ISS program. This is an extremely demanding role and requires a lot of planning and constant monitoring. The job is made easier with the right supporting tools.

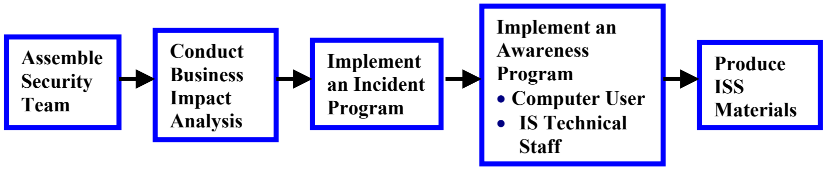
This guide provides the necessary working papers and checklists to help you to gather and analyze information.

The Template Process

There is a process that you should follow to develop and implement your ISS program.

> ***"Security isn't a product; it's a process. It is possible to have best-of-breed products and still have lousy security if your processes are flawed."***

The following flowchart shows the process you should go through to incorporate all components of the ISS program.


Assemble Security Team
Conduct Business Impact Analysis
Implement an Incident Program
Implement an Awareness Program
• Computer User
• IS Technical Staff
Produce ISS Materials

ISS Program Process

Assemble a Security T.E.A.M.

Having the key players in place is the first step in building your ISS program. *See Chapter 2 for complete details.*

Conduct Business Impact Analysis

Knowing your information inventory and how to protect it is the most critical of all steps in the process. *See Chapter 3 for complete details.*

Implement an Incident Program

Having an organized and well-tested incident reporting program in place can save your organization unnecessary damage. *See Chapter 5 for complete details.*

Implement an Awareness Program

Making every employee aware of good security practices is required. *See Chapter 6 for complete details.*

Prepare all ISS Materials (Use the templates)

It is important that you publish ISS rules and procedures. Keeping ISS visible and alive requires materials and guides for on-going support. *See Chapter 4 for complete details.*

Chapter 2

Assemble a Security TEAM

The Security TEAM

Responsibility for ISS on a day-to-day basis is everyone's duty. Information security effects every department and every person in an organization. Every worker must do their part in order to achieve appropriate levels of security. Information appears everywhere in an organization, and almost every workers uses information to do their job.

There may be several security teams:

- security day-to-day
- security advisory committee(s)
- security response team

Security Day-to-Day

There …

Security Advisory Committee(s)

Each organization should assemble a Security Advisory committee. This advisory group / steering committee should be made up of key technical and management personnel within the organization to coordinate security efforts and resolve security problems with overall authority over all aspects of security. The security guard coordinates this effort.

Each organization should also select a member for the CERT Team.

Incident Response Team

Each organization should assemble an Incident Response Team to handle all suspicions and incidents.

IMPORTANT: It is critical that someone on the response team be designated to produce the documentation that describes the events and outcomes.

The Security Officer

Appointing the Security Officer

One of the key appointments in any organization is to designate a Security Officer. In smaller organizations, the ISS Officer may not be a full-time security specialist, but may also have other technical or business related job functions. In the larger agencies, the ISS Officer may perform ISS tasks full time and may even require additional security staff to accomplish all security tasks. In both situations, someone needs to be appointed to take the overall responsibility of ensuring that the appropriate ISS safeguards are in place, the policies and procedures are agreed and rolled-out, and that all users of information understand their responsibilities and duties.

(Notes: Should we state that the security officer should be appointed by the Agency Head?)

The Tasks of the Security Officer

The Security Officer is responsible for overseeing the entire security process. The primary role is to ensure each organization's information is protected.

The following security officer tasks have been grouped by main function:

Rule Tasks

- recommend, develop and set up security Rules - the Rule Maker (use template)
- implement enterprise, organization-specific and application-specific security Rules and procedures (use template)
- enforce ISS Rules (use template)
- monitor compliance to security Rules
- periodically evaluate effectiveness of ISS Rules and procedures
- gather facts and analyze information security issues/ keep current
- develop recommendations for the agency on ISS matters

Systems Tasks

- act as liaison between security department and IS
- coordinate follow up procedures for ensuring proper adjustment of access privileges associated with changes in employee status and business arrangements.
- develop procedures and administer the information access control decisions made by information custodians within the organization.
- review changes to the configuration of security administration facilities and settings
- participate in preparing a disaster recovery plan to help prepare contingencies and be ready to implement the disaster recovery plan

- implement procedures for authentication of users and messages
- publish guidelines for creating and managing passwords
- approve/ disapprove access by users to systems/ set up access – passwords
- cooperate in the development and implementation of security technology
- perform security assurance reviews for new systems and changes to existing systems
- maintain up-to-date records for all systems accessed by employees and users
- maintain configuration profiles of all systems controlled by IS including but not limited to mainframes, distributed systems, microcomputers, and dial access ports.
- identify security technical resources and tools
- document the security support structure across platforms.
- participate in reviews and analysis of internal projects that may have impact on ISS.

Security Tasks

- investigate, coordinate, report, and follow-up on security incidents
- coordinate prosecution of offenders
- assign an owner to each asset
- provide interface with internal and external audit agencies
- conduct business impact analysis - risk assessments to identify threats and potential safeguards
- assemble a security team
- monitor unusual activities and report security breaches and incidents, including identifying resources to assist with tracking, analysis, and responding to incidents.
- establish and chair agency security committees.
- report risks and incidents to agency head - all areas
- furnish security awareness, training, and advisory programs for employees
- establish and maintain security teams with roles and responsibilities
- identify training requirements
- develop and implement strategies to make users aware of security Rules, procedures, and benefits.
- coordinate technical leads and public relations
- establish secure communication channels/ conduct regular training and readiness drills
- monitor, audit, and test systems for security vulnerabilities.

Security Officer Training

It is assumed in this template package that the security officer knows the basic principles of ISS. The intent of this manual is not to teach them everything about ISS, but to guide them through the tool, the template package, to implement a good ISS program.

Additional training may be required for the security officer to fully understand ISS. It is suggested that the security officer attend any of the following:

- MISTI
- SAN
- … (add new ones?)

Security Staff

The security Officer may perform ISS tasks full time and still may even require additional security staff to accomplish all security tasks.

Security and the IS Department

The security officer and the IS department work very closely together, especially the systems and network administrators who set up accesses and track usage. It is critical that the security officer have full cooperation from the IS department. Systems programmers, computer operators, managers, and IS clerical staff may also be critical to the security process.

RECOMMENDATION: When feasible, the security officer and staff should not report directly to the IS department. If it is not feasible, then the security officer should report to 2 areas – IS and other internal department for security.

Security Guards

Not all organizations will have the need for a guarded entry to a building or room. If they do, physical access becomes the responsibility of the security guards. Many companies support the physical entry process by providing equipment, software, tools, and even the guards. (mention the company ?)

Copyright Contact

Each employee must comply with copyright laws. Organizations should communicate this to all employees and should designate a single point of contact for inquiries about copyright violations, pursuant to federal law. There is an entire chapter in the *Computer User Security Handbook* dedicated to copyright rules.

Security Auditors

Some organization's are large and may have their own internal security auditor(s) who track daily traffic. Smaller organizations may not have anyone performing that role, however, there are many tools that can be put in place to assist with the auditing or tracking of ISS processes. Applications must include auditing capabilities to track access to sensitive information.

Security Audits

A security audit is performed to keep security tight and anticipate weak areas. An audit can also be thought of as an assessment or vulnerability test to review existing practices.

Day-to-day tracking and monitoring of logs and reports can also be thought of as an audit function. Therefore audits can be:

- ♦ Daily tracking and monitoring
- ♦ Formal Audit (re-assessment)

In a formal audit, you may enlist a third party company to regularly audit your security program. It is recommended that you perform an audit every 6 months, or at least once a year.

What should you audit?

- Audit new systems installations to ensure conformance to existing policy statements.
- Perform regular automated system checks to reveal possible intruder activity or illicit behavior by insiders.
- Random security checks
- Audit critical files (i.e. passwords) to assess their integrity and look for unauthorized changes.
- Audit user account activity on a regular basis to detect dormant, inactive, or misused accounts anomalies.
- View logs (i.e. # attempts to log on, …)
- You can audit from the inside out (on-site), or from the outside in (off-site).
- dormant User Ids for {} days
- ("User Logon Register" or some type of operator / admin logs show incorrect or unusual entries, it could indicate that data has been accessed and therefore possibly lost or stolen.)
- Applications must include auditing capabilities to track access to sensitive information.
- Monitoring reports (i.e. tokens) ex. remote access printouts, work with vendor to issue, replace, maintain, and deactivate tokens. Reports show inactivity. For example, you must log in once a month to keep token synchronized with the Citrix. Automatically expires battery – forced to replace it.

Daily Audit/ Tracking Logs

Logs, or reports should be used to manage and monitor activity on your system. The following logs are recommended: (need clean up?)

- 1. Logs Required On Application Systems Handling Sensitive Information
- 2.Keystroke Logs Required For All Production System Privileged User-Ids
- 3.inclusion Of Security Relevant Events In System Logs
- 4.Computer System Logs Must Support Audits
- 5.Accountability And Traceability For All Privileged System Command
- 6.Contents Of Logs For Systems Running Production Applications
- 7.Required Retention Period Of Logs
- 8.Daily Removal Of Logs From Internet-Accessible Computers
- 9.Logs Of User-Initiated Security Relevant Activities
- 10Retention Of Access Control Privilege Logs
- 11Reconstructibility Of Changes To Production Information
- 12Information To Capture When Computer Crime Or Abuse Is Suspected
- 13Logs Required For Rapid Resumption Of Production System Activities
- 14Systems Architecture For Logging Activities
- 15Clock Synchronization For Accurate Logging Of Events On Network
- 16Logs Of All Inbound And Outbound Faxes
- 17Resistance Of Logs Against Deactivation, Modification, Or Deletion
- 18Writing Logs To WORM Storage Media Prevents Alteration
- 19Persons Authorized To View Logs
- 20Regular And Prompt Review Of System Logs
- 21Notification Of Users About Logging Of Security Violations

Suggested logs by User ID:

1. logon attempts failed
2. actions performed
3. high profile actions
4. wide scale deletions
5. who edited web site
6. activities of computer operations
7. activities of system administrators
8. activities of security officers
9. who accessed highly sensitive data

Most logs should report time, date, User ID, type of event, success or failure, origin of request (i.e. terminal address) and others.

Working Paper #1
Assemble a Security TEAM
Tasks and Responsibilites

1. List all of the security tasks performed at your organization.

(See list above)

ISS Tasks	Agency	Department	Person Responsibile	Position	Member of Advisory Committee Y/N	Member of Response Team Y/N
Rule Tasks			John Doe	Network adminstrator	N	Y
SystemTasks						
Security Tasks						

2. For each task above, assign a name (position) to the task:

3. How many responsibilities / names do you have above in #2? _______

0 you need to identify your team.

1 you have 1 person doing all those tasks. This is not …

2-x you are probably from a large organization and require more people to run your ISS program.

You have now identified your ISS TEAM!

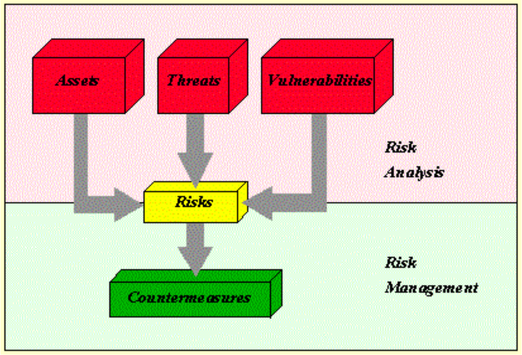
Chapter 3

Conduct Business Impact Analysis

About Business Impact Analysis

Now that you have assembled your security TEAM, you can begin the process of creating your ISS Program. This step performs an organization-wide Business Impact Analysis study.

This chapter will guide you through the process of conducting a Business Impact Analysis study for your Information Security. You have been provided with Working Papers and Checklists to capture and organize the necessary information.



Business Impact Analysis Procedure

The following steps outline the process you perform to conduct a business impact analysis.

Steps:

Assets

1. Identify Your Information Inventory – Asset and Assets Types
2. Assign an Owner to each Asset

Value

3. Assign a Value to each Asset

Threats

4. Identify Potential Threats and Types
5. Determine Likelihood of Threats
6. Measure Impact of Threats
7. Identify system Vulnerabilities to Threats and damage potential

Risk

8. Identify Risks (after Threats)
9. Measure Risk
10. Assign a Risk to each Asset

Classify

11. Classifying Assets (after Value and Risk)

Safeguards

12. Identify possible candidate Safeguards (after Risks)
13. Assign a Safeguard to each Asset (to reduce risk to acceptable level)
14. Implement and Test Safeguards
15. Accept Residual Risk

(Note:value > assets > risk > confidentiality (data) > classify
(build a threat database, vulnerability database)
("a vulnerability without a threat isn't worrisome." Focus on risk - where there are both vulnerabilities and people shooting.)

Identify your Information Technology Inventory

What are Information Assets?

In order to know what information you need to protect and how you are going to protect it, you must identify your Information Assets. A complete inventory is required to know what the organization requires for the ISS program. All information resources must be accounted for.

Information Assets are those resources that store, transport, create, use, or are information. These assets are those that add value to the organization or whose loss would reduce value to the organzation.

Assets Types

You may want to group your assets into Asset Types. Sometimes these Asset Types can be managed as a single asset.

Hint: You should have a log/ report that lists the following assets within their asset types.

(3 definitions (HIPAA will explain how to protect these?) system – hardware and operating system, software - applications, data?)

- hardware
  (owned and not owned)
  laptops, desktops, printers, …
- software
  application programs
  program libraries (in-house developed)
  software application - third party (i.e. MS Word)
- databases
  This includes backups, tape library ?
  Files, data elements, …
- communications
  This includes lines, switches, routers, bridges, networks
  What's connected to what? Who are we connected to? (ex. telephone company)

(Note: 164 outside firwall, 10. Inside firewall. Concern: PC attached internal modems)

Asset Ownership

Each Information Asset must be assigned an Owner. Accountability helps ensure that adequate security protection is maintained. The Owner is responsible for evaluating, classifying, and protecting the asset. The implementation of the safeguards may be delegated, but the owner of the asset is responsible for protecting it. The Owner can be a technical, business, or user resource.

The Owner can also be another agency or regulated data.

Location

You may want to organize your assets by location - either physical or logical locations. (Optional?)

Inventory Number

(Optional?)

Working Paper #2
Business Impact Analysis
Information Inventory

1. List your Asset Types:

(See list above)

ISS Asset Types

1 ______________________________

2 ______________________________

3 ______________________________

4 ______________________________

5 ______________________________

…

2. For each ISS Asset Types, list the Asset:

ISS Asset Type	Asset
Software Application	MS Word
	MS Excel
	…
Hardware	AS400
	…

3. For each ISS Asset, assign an Owner. You can also assign a Location or an Inventory Number (optional?). (Should we also add here - For each Asset - determine if you are IMS dependent or not? This will effect how to proceed?)

(By Asset Type)

ISS Asset	Owner	Location (physical or logical)	Inventory Number

Assign Values to Assets

What is the Value of an Asset?

Once you have identified your Information Assets, then you will give them each a Value or evaluation of the assets worth.

Different methods can be used to value assets. You can give the asset the value of simply replacement, but it can get more complicated than that. This is one of the most subjective of the ISS processes. You can make the value whatever you want it to be as long as you are consistent across all assets. The asset valuation is done with the goal of the process in mind, that is, to define assets in terms of a hierarchy of importance or criticality, the relativeness of the assets becomes more important than placing the "correct" Value on them.

Generally, assets can be valued based on the impact and consequence to the organization. Assigning value depends on its loss to the organization, and how much of the organization relies on it. Value can be based on loss.

IMPORTANT: The value of the asset did not change because of good backup and recovery procedures. All protection mechanisms are "removed" when calculating Values.

After you have given your assets a Value, you can then measure your Risks.

How do you Calculate the Value?

(There's many ways – here's a few suggestions - The Simple Asset Valuation?)

The value of the asset can be represented in terms of the potential loss. This loss can be based on the replacement value, the immediate impact of the loss, and the consequence. One of the simplest valuing techniques to indicate the loss of an asset is to use a qualitative ranking of high, medium, and low. Assigning values to these rankings (3=high, 2=medium, 1= low) can assist in the risk measuring process.

OR use this approach:

Value Sum of Invested and Loss Impact

Invested The cost already expended - purchase costs, man hours, other, … There are other intangible (hidden) values. The cost of creating or acquiring the asset.

Impact (A code/ plus values?)

Re-creation

The cost of re-creation or replacement. The cost of purchasing, building, or having a service provide the replacement of the asset. Time and $.

Value of re-create =
re-creating the asset +
man and machine hours

If the cost of re-creation is high - give it high protection/ safeguards (i.e. redundant storage of asset, backup and recovery).

Unavailability / Denial of Service

Cost of unavailability - Time and $. The inability to access information quickly can be devastating to many organizations. It depends on timing, duration, and the situation. (i.e. timing – may be need to know something until it happens and then you need it – how to shut down a nuclear power plant.)

This may require high level of redundancy to eliminate points of failure – not protect the information, but protect the access to it.

Disclosure

What is Disclosure? Revealing information to the wrong people or media can be disastrous to an organization. The intent of many attackers is to reveal confidential information or disclose information prior to its release. The more detailed the information, the more costly the disclosure. Information whose public disclosure could have drastic consequences should be given a high security level.

Propriety information – will business lose sales, market position? What will be the effect on the ability to conduct business in a profitable manner? Does it effect the bottom line.

Private information – individuals with which the company entrusted. This effects the individual that the information is about and the company who is the caretaker. The organization can suffer indirect damages through a loss of confidence and through legal actions taken by individuals who suffered from the disclosure.

Cost of Disclosure. Time and money. It is affected by the level of detail. The more detailed, the more costly the disclosure.

Information whose public disclosure could have drastic consequences should be given a high security level.

Disclosure life cycle. Most information has a life cycle. In planning, the longer into the future the information relates to, the higher the cost of disclosure. Plans that will become public tomorrow may not cause the same level of damage as plans covering the next 3 years.

Working Paper #2
Business Impact Analysis
ISS Asset Value

1. Each Owner of each ISS Asset should calculate the Value.

(By Asset Type)

ISS Asset	** Value **

Where Value is one of the following:
3=high, 2=medium, 1= low

OR

2. Use this method …

(See field descriptions above)

ISS Asset	Invested	Loss Impact			** Value **
		Re-creation	Unavailability	Disclosure	

OR ………..any other you wish to use.

Calculate the Risk Rating/ Measure (?)

What is Risk Analysis?

A risk analysis is required to understand the potential impact on operations and to justify the expenditures on security. An organization-wide risk analysis is required to collect all of this information. A risk analysis is a basic business process that should be performed on all major projects and new technologies before they are implemented to assure the feasibility of the projects. Since information systems technology is continually changing, risk analysis should be done periodically.

In this step of the ISS process, any potential risk shall be identified, whether already addressed or newly anticipated.

Security reduces risk. Although risks can be minimized, that cannot be eliminated. Security often focuses on worst cases scenarios – but typical scenarios are to also be considered. The "once in a million" scenario must be considered, but financial reasons may only implement the typical scenario.

How do I Measure Risk?

The Risk Measure can be considered the representation of the kinds of adverse actions that may happen to a system / organization and the degree of likelihood that these actions may occur. The outcome of this process should indicate the degree of risk associated with the defined assets. This outcome is important because it is the basis for making safeguard selection and risk mitigation decisions.

There are many ways to measure and represent risk. Depending on the particular methodology or approach, the measure could be defined in:

- qualitative terms
- quantitative terms
- one dimensional
- multidimensional
- some combination of these

Quantitative approaches are often associated with measuring risk in terms of dollar losses.

Qualitative approaches are often associated with measuring risk in term of quality as indicated through a scale or ranking.

One dimensional approaches consider only limited components (e.g. risk = magnitude of loss X frequency of loss).

Multidimensional approaches consider additional components in the risk measurement such as reliability, safety, or performance.

(Note: Risk can be dependent on timing (i.e. disclosing something before it should be known, whereas in a few weeks it wouldn't matter.)

(Note: Risks and Safeguards – First decide risks, then safeguards, then recalculate risks again? After implementation of the safeguards, is the remaining risk acceptable? The greater the risk value, the more important it is to implement better safeguards.)

Calculating Risk?

(Notes: Here's some ways to calculate Risk- these are confusing)

Risk Rating = Threat (+ or X) Vulnerability

Risk Rating = Threats + Impact + Likelihood

OR

Risk can have a minimum value of 0 - no risk and a maximum value of 25 (extremely dangerous risk).

OR

One Dimensional Approach to Calculate Risk (also confusing?)

The risk associated with a threat can be considered as a function of the relative likelihood that the threat can occur, and the expected loss incurred given that the threat occurred. The risk is calculated as follows:

risk = likelihood of threat occurring (given the specific vulnerability) x loss incurred

OR

The value estimated for loss is determined to be a value that ranges from 1 to 3. Therefore risk may be calculated as a number ranging from 1 to 9 meaning a risk of:

- 1 or 2 is considered a low risk
- 3 or 4 a moderate risk
- 6-9 high risk

Likelihood	Loss	Risk
1	1	1 - low
1	2	2 - low
1	3	3 - low
2	1	2 - low
2	2	4 - moderate
2	3	6 - high
3	1	3 - moderate
3	2	6 - high
3	3	9 - high

In this example, the levels are normalized (i.e. high, moderate, low) and can be used to compare risks associated with each threat. The comparison of risk measures should factor in the criticality of the components used to determine the risk measure. The simple methodologies that only look at loss and likelihood, a risk measure that was derived from a high loss and low likelihood may result in the same risk measure as one that resulted from a low loss and high likelihood. In these cases, you need to decide which risk measure derived from the high loss is more critical than the risk measure derived from the high likelihood.

OR

Risk Rating: Threat rating x visibility rating = a
a consequences rating x sensitivity rating = b
Rating = a + b (Add the two values together.)

2-10 Low Risk

11 – 29 Medium Risk

30-50 High Risk

Acceptable Risk Rating

All assets will have some risk attached to them. You must decide on the Acceptable Risk Rating for your organization. All risks having a value higher than this number are unacceptable risks which must be countered. (i.e. a good Acceptable Risk Rating is 15).

Working Paper #3
Business Impact Analysis
Risk Analysis

1. Make a list of all Risks.

…

2. For each Asset, calculate a Risk Rating.

ISS Asset	Threat (?)	Risk Rating

3. The Acceptable Risk Value for our organization is ________? {Acceptable Risk Rating}

Assess Threats and Vulnerabilities

What is an ISS Threat?

A Threat is any circumstance or event with the potential to cause harm. Threats are always present. As the world's dependence on information continues to increase, threats become more worldwide, more ambitious, and increasingly more sophisticated. Before deciding how to protect a system, it is necessary to know what the system is to be protected against. (i.e. what threats are to be countered.)

A threat assessment is a critical part of the risk analysis (?).The most important reason for identifying your threats is to know from what do the assets need protection and what is the likelihood that a threat will occur? Threats cannot be eliminated, but can be anticipated, and safeguards put in place to minimize their impact.

A Threat is not an Incident. With a Threat, no event occurred, nothing has happened.

TIP: Good employee relations help to minimize threats.

Identify Potential Threats

Threats can be:
deliberate or non-deliberate
internal or external

Threat Types:

- human error
  accident or lack of knowledge, the most common threat, reduce by education and reducing authorizations – least privileges

- system failures
  information systems: hardware (most solvable), software, infrastructure, power and communications.

- natural disasters

  (See Disaster Recovery in the IS Guide)

- malicious acts
  internal and external
  Ex. fraud, espionage, vandalism, theft, hackers,

- software virus

Threat Likelihood

One of the main components in calculating risk is to determine the likelihood of a threat.

Estimating the chance that the threat will cause a loss: can use: frequent, probable, occasional, remote, and improbable.

As specific threats and vulnerabilities are identified, a likelihood measure needs to be associated with the threat / vulnerability pair. (i.e. What is the likelihood that a threat will be realized, given that the vulnerability is exploited. Along with asset valuation, assigning likelihood measures can also be a subjective process.

(Notes: See simple likelihood measure. This likelihood measure coincides with the asset valuation measure defined in …)

Assigning Likelihood Measure - The likelihood of the threat occurring can be normalized as a value that ranges from 1 to 3. 1 will indicate a low likelihood, 2 will indicate a moderate likelihood, and 3 will indicate a high likelihood.

OR

What is the likelihood of a threat occurring (0-5?)

1 The threat is highly unlikely to occur.

2 The threat is likely to occur less than once per year.

3 The threat is likely to occur once per year.

4 The threat is likely to occur once per month.

5 The threat is likely to occur once per week.

6 The threat is likely to occur daily.

OR

Likelihood	
1	Very likely
2	Somewhat likely
3	50/50 chance
4	Highly likely
5	Nearly certain

Threat Impact/ Consequences

Threat Impacts

Impacts describe the effect of a threat.

What are the immediate damages of the threat being realized? Impacts are very specific. (i.e. change accounting data, falsify money transfers)

Impact Analysis - a number 0-6 as follows:

Impact Rating	Description
1	Impact is negligible.
2	Effect is minor, major business operations are not affected.
3	Business operations are available for a certain amount of time, revenue is lost, customer confidence is affected minimally (unlikely to lose customer).
4	Significant loss to business operations or customer confidence or market share. Customers may be lost.
5	The effect is disastrous, but the organization can survive, at a significant loss.
6	The effect is catastrophic, the company will not survive.

OR

Impact	
1	Minor impact on cost, schedule, performance, etc.
2	Moderate impact on cost, schedule, performance, etc.
3	Significant impact on project baselines
4	Very significant impact on project baselines
5	Disastrous impact, probable project failure

Threat Consequences

What are the long-term effects of the threat being realized (e.g. damage to reputation or organization, loss of business)?

Threat Calculations

Threats = the likelihood that they will occur x the damage they could cause.

Identifying Vulnerabilities

(Vulnerability is hard to understand?)

Vulnerabilities are comprised by a threat that causes a loss. They are difficult to define before there is a security incident. They are the cause of the incident. They exist in hardware, software, policies, procedures, and in people.

During risk analysis, you need to understand Vulnerabilities and where they exist. (What's the difference between a vulnerability and a risk?)

Vulnerability - common sources:

- Security design flaw
- Incorrect implementation
- Innovative misuses
- Social engineering

Working Paper #3
Business Impact Analysis
ISS Risk Measurement

1. Identify Potential Threats and Types.

Threat Type	Threat

2. For each Potential Threat, calculate the Likelihood and Impact.

3. For each Potential Threat, list its corresponding Vulnerabilities and Damage Potential.

Threat	Threat Likelihood (to that asset)	Impact	Vulnerability

4. For each …

Information Classification

What is classifying information?

Now you are ready to classify your assets according to how they ranked in the initial analysis. Your classification system puts the right controls on sensitive or other critical information. The Owner of the asset should be the one that determines the sensitivity or classification.

Assigning classifications determines day-to-day practices with information: how it is handled, who handles it, how it is transported, stored, who has access, where it can go, and such. You can use Classification labels if you wish to follow information in whatever form / media it is transported – printed, electronic, or on a display screen.

NOTE: Once a data classification system has been adopted, it is very expensive and difficult to change to another system.

(Link classifications > rules > safeguards > incidents?)

(Notes: Once standardization is achieved, then the applications can be ranked, and the most critical ones can receive special contingency planning attention. The number of criticality categories will vary from organization to organization, as will the meanings of the terms like "priority." Generally, each of these terms will have a time period during which the application must be recovered. For example, "highly critical" applications could be those which must be recovered within 15 minutes." Information itself could be rated according to criticality, but because information is so often processed by many different applications, it is frequently easier just to focus on applications when preparing a contingency plan and classifying information.)

Classifying Your Information

When doing a Classification with your information, consider:

- Sensitivity of the data

  This is the leading factor and should consider disclosure, damage, and loss of information and its impact on the business operations.

- Regulated/ legal and contractual obligations and penalties

  What is the minimum level of Classification required to which the law or contract applies? For example: Personally Identifiable Information (PII) or

Individually Identifiable Health Information (IIHI) as regulated by GLB, HIPAA, or FERPA.

- Standards and guidelines

  What has been defined by government, industry, locality, or the organization to be in compliance?

- Information lifecycle

  What are the effects of the Classification over time? In particular with disclosure, the importance can change over time. e.g. The closer to being made public the lower the Classification.

  (Note: Can break down confidentiality, integrity and availability into high, medium, and low.)

  Confidentiality – describes the impact from disclosure.
  Integrity – reflects the severity of the damage that could be caused
  Availability - urgency of the information and the systems that use it
  Non-repudiation – (See NITC?)

General vs. Critical Systems

A General support system can be defined as any system that provides processing or communications support across a wide array of applications. It consists of computers, networks, and programs.

Critical applications can be defined as all applications that require some level of security. General security should be provided by the security of the general support systems in which they operate. e.g. Personnel data, financial data.

What should you protect?

Typically, the high risk information areas are:

- ♦ Password and User IDs
- ♦ Tax / IRS
- ♦ Medical
- ♦ Social security numbers
- ♦ Payroll and salary

- Executive plans
- others ??

Security Classification Levels

State policy guidelines recognize four basic levels of security classifications that are associated with varying degrees of known risks. Once information technology assets definition are achieved, hardware, software, applications, databases and communication can be ranked. Those that are the most critical ones can receive special contingency planning attention.

☞ ***IMPORTANT***: Draft versions of information should be classified and handled in the same matter as final versions.

Classification Levels (4 Scale)

- **HIGHLY RESTRICTED** is for the most sensitive information intended strictly for use within your organization and controlled by special rules to specific personnel. It is highly critical and demands the highest possible security.

  Examples: pending mergers or acquisitions, investment strategies, executive plans and designs

- **CONFIDENTIAL** is for less sensitive information, but may include Personally Identifiable Information (PII) intended for use within your organization or by individuals, yet still requires a high level of security. It may be regulated for privacy considerations. (e.g. HIPAA)

  Examples: accounting data, business plans, sensitive customer information, patients medical records, procedures, operational work routines, project plans, designs and specifications that define the way in which your organization operates.

- **INTERNAL USE ONLY** (default category) is for non-sensitive information intended for use within your organization. The security is controlled, but not highly protected. This default category is to be used in the absence of any classification. This is the most prevalent category.

  Examples: internal memos, minutes of meetings, internal project reports.

- **UNCLASSIFIED/ PUBLIC** is for information that requires minimal security and can be handled in the public domain.

  Examples: annual reports, press statements approved for public use

Reclassification

Reclassification of information is on-going as a regular part of maintaining your ISS program. The periodic review of classifications in conjunction with risk assessment will lead to appropriate protection and safeguard expenditure, rather than unnecessary expense.

Classification Levels Quick Reference

Classification Level	Impact	Storage	Tracking/ Disposal	Labeling	Release to Third Parties/ Granting Access	Copying / Faxing / E-mail
HIGHLY RESTRICTED	High Impact. Loss or damage WILL seriously impede the organizations future. Public or internal disclosure will cause critical harm to on-going operations.	Encrypted and/ or physical access.	Track all recipients, copies made, locations sent, addresses, disposal method. Disposal - Shredding or Secure Disposal Boxes	Media – External and internal labels. Hard copy – each page should be labeled. Mail – address of specific person. No label on outside, only inside.	Owner approval and Non-Disclosure Agreement Highly restricted access or Owner only.	Distribution must be protected at all times. Owner approval for copying, faxing.
CONFIDENTIAL	Considerable Impact. Loss or damage COULD seriously impede the organizations future. Public or internal disclosure could cause harm to on-going operations.	Encrypted and /or Physical Access.	Tracking not required. Disposal – Shredding or Secure Disposal Boxes	Media – External and internal labels. Hard copy – each page should be labeled. Mail – address of specific person. No label on outside, only inside.	Owner approval and Non-Disclosure Agreement Highly restricted access or Owner only.	Distribution must be protected at all times. Owner approval for copying, faxing.
INTERNAL USE ONLY	Minor impact. Loss or damage could cause minor concerns to the organizations future. Public or internal disclosure could cause little or no harm to on-going operations.	Encryption Optional	Tracking not required. Disposal – no special process required.	No label required.	Non-Disclosure Agreement Local Manager (?) only	No restrictions.
UNCLASSIFIED/ PUBLIC	No impact.	Encryption not necessary	Tracking not required. Disposal – no special process required.	Release Date	No restrictions	No restrictions.

Working Paper #4
Business Impact Analysis
Asset Classification

1. Each Owner of each ISS Asset, assign a Classification.

ISS Asset	Risk Rating	Classification
Hardware		
Software		
Communications		
Databases		

Developing Safeguards

What are Safeguards?

Now that you have analyzed your information assets, their value, the risks confronting them, and the threats that could occur, it is time to determine what kind of protection or Safeguards you are going to implement. This is the most important and final step in the ISS process. Once you have assigned the appropriate Safeguard, you can then re-evaluate the Risk and bring its Rating to an acceptable level. (Risk Rating).

All assets do not have the same potential of loss and do not require the same expenditure of protection. Is it important to place the proper Safeguard on an Asset that justifies the cost and maintenance.

Ways to protect:

Disguise – change/ hide identification of devices and such, so hackers can't find it or get to it.

Have the system monitor the devices and check for their activity. Send a warning (?) if device doesn't respond.

Why safeguards?

Eliminate risk
Reduce risk
Limit the damage
Compensate the damage (insurance)

(Notes: What are the effective security measures (security services and mechanisms) needed to protect the assets? What is liability if it is not protected? How carefully should you protect information? How much should you invest in protecting information?)

(Note: Safeguards are also called: proper security measures, controls, protective means, counter measures.)

(Notes: In NITC document, Security Safeguards – procedures, responsibilities, incident reporting, security audits, physical security, compliance procedures.)

(Notes: The measures taken to protect assets should correspond to the value of the assets.)

(Notes: Safeguards assigned based on knowledge of the vulnerability, threats that are likely to exploit the vulnerability, potential loss that could occur, and the likelihood of its occurrence. Safeguards can be used in combination. You don't have to protect everything. Plan alternative configurations that will provide more secure profiles in an attack. High cost of re-creation - give it a high protection/ safeguards (i.e. redundant storage of asset, backup, and recovery,….)

Safeguard Types

- Policies and procedures
- Mechanisms
  - password generator
  - token based
  - biometrics
- Hardware
- Software
- Reporting
- Password protection
- Positive ID
- Encryption
- Physical Control

Safeguard Tools

Tools

(How much to put there? Computer Associates' CA-Unicenter, which provide a consistent platform-independent administrative interface for access control systems.)

Others?

Software that will trace the source of attacks.

(also Tools Overview - what is available? Outside Security Vendors – what is available? MSS (Managed Security Services) Make sure they can do a better job than you can. (i.e. handle all firewall configurations)

Assigning Safeguards to Risk and Assets

Threats cannot be eliminated, but can be anticipated, and safeguards put in place to minimize their impact.

With the list of potential threats, vulnerabilities, and risks done, … assessment of the current security situation can be determined. Areas that have adequate protection will not surface in contributing to the risk (since adequate protection leads to low likelihood) whereas those areas that have weaker protection do surface as needing attention.

(Risk – Before and after Safeguard assignment. After implementation of the security controls, is the remaining risk acceptable?)

An organization must protect its assets. Once there is an understanding of what resources need to be protected, their value, the size of the threat, the likelihood of vulnerabilities, then appropriate safeguards can be assigned. These prior steps help you define the appropriate type and size of the safeguard.

(Notes: Now that you have identified the information assets, their potential loss value, their importance, what do I do to address each one with a solution?)

What do I do to assign Safeguards?

Select Candidate / appropriate Safeguards
Implement and test safeguards
Accept Residual Value

Select appropriate safeguards

This task can be done using risk acceptance testing. Risk acceptance testing is described as an activity that compares the current risk measure with acceptance criteria and results in a determination of whether the current risk level is acceptable. While effective security and cost considerations are important factors, there may be other factors to consider such as: organizational policy, legislation and regulation, safety and reliability requirements, performance requirements, and technical requirements.

The relationship between risk acceptance testing and safeguard protection can be iterative. Initially, the organization needs to prioritize the different risk levels that were determined during the risk assessment. Along with this the organization needs to decide the amount of residual risk that it will be willing to accept after the selected safeguards are implemented. These initial risk acceptance decisions can be factored into the safeguard selection equation. When the properties of the candidate safeguards are known, the organization can reexamine the risk acceptance decisions to reflect the known properties of the safeguards. For example, there may be risks that are determined to be too high. However, after reviewing the available safeguards, it maybe realized that the currently offered solutions are very costly and cannot be easily implemented into the current environment. This may force the organization into either expending the resources to reduce the risk, or deciding through risk acceptance that the risk will have to be accepted because it is currently too costly to mitigate.

The methodology discussed here defines safeguards in terms of security services and mechanisms. A security service is the sum of mechanisms, procedures, etc., that are implemented to provide protection. The security services (and mechanisms) listed below … can be used as a starting point. The security services should be related to the threats defined in the risk assessment.

In most cases, the need for a specific service should be readily apparent. If the risk acceptance results indicate that a risk is acceptable, (i.e. existing mechanisms are adequate) then there is no need to apply additional mechanisms to the service that already exists.

After the needed security services are determined, consider the list of security mechanisms for each service. For each security service selected, determine the candidate mechanisms that would best provide that service. Using the threat/ vulnerability/ risk relationships developed (above), choose those mechanisms that could potentially reduce or eliminate the vulnerability and thus reduce the risk of the threat. In many cases, a threat/ vulnerability relationship will yield more than one candidate mechanism. For example, the vulnerability of using weak passwords could be reduced by using a password generator mechanism, token based mechanism, biometrics, … Choosing the candidate mechanisms is a subjective process that will vary from one organization to another. Not every mechanism is feasible to use in every system. Some filtering of the mechanisms needs to be done to make this step beneficial.

Selecting appropriate safeguards is a subjective process. When considering the cost measure of the mechanism, it is important that the cost of the safeguard be related to the risk measure to determine if the safeguard will be cost-effective. The methodology should provide a measure for representing costs that is consistent with the measures used for representing the other variables determined so far.

Calculating Cost Measure

In this example cost measure, the cost of the safeguard is the amount needed to purchase or develop and implement each of the mechanisms.

(Cost can be normalized same as loss value - 1 will indicate a mechanism with a low cost, 2 … moderate cost, 3 … high cost.)

When a measure (or cost) is assigned to the safeguard, it can be compared to the other measures in the process. The safeguard measure can be compared to the risk measure (if it consists of one value) or the components of the risk measure. There are different ways to compare the safeguard measure to the risk measure. The risk management methodology should provide a method to select those effective safeguards that will reduce the risk to an acceptable level.

Comparing Risk and Cost

To calculate risk/ cost relationships use the risk measure and the cost measure associated with each threat/ mechanism relationship and create a ratio of the risk to the cost (i.e. risk/ cost). A ratio that is < 1 will indicate that the cost of the mechanism is greater than the risk associated with the threat. This is generally not an acceptable situation (and may be hard to justify) but should not be automatically dismissed. Consider that the risk value is a function of both the loss measure and the likelihood measure. One or both of these may represent something so critical about the asset that the costly mechanism is justified. This situation may occur when using simple methodologies.

Implement and test safeguards

The implementation and testing of safeguards should be done in a structured manner. The goal of this process is to ensure that the safeguards are implemented correctly, are compatible with other safeguards, and provide expected protection.

This process begins by developing a plan to implement the safeguards. This plan should consider factors such as available funding, user' learning curve,… A testing schedule for each safeguard interacts of effects other safeguards. The expected results (or the assumption of no conflicts) of the interaction should be detailed. It should be recognized that not only is it important that the safeguard perform functionally as expected and provide the expected protections, but that the safeguard does not contribute to the risk through a conflict with another safeguard / functionality.

Each safeguard should first be tested independently of other safeguards to ensure that it provides the expected protection. This may not be relevant to do if the safeguard is designed to interwork with other safeguards. After testing the safeguard independently, the safeguard should be tested with other safeguards to ensure that is does not disrupt the normal functioning of those existing safeguards. The implementation plan should account for all these tests and should reflect any problems or special conditions as a result of the testing.

Accept Residual Value

After all safeguards are implemented, tested and found acceptable, the results of he risk acceptance test should be reexamined. The risk associated with the threat/ vulnerability relationships should now be reduced to an acceptable level or eliminated. If this is not the case, then the decision made in the previous steps should be reconsidered to determine what the proper protection should be.

Working Paper #5
Business Impact Analysis
Safeguards

1. Each Owner of each ISS Asset, assign a current and proposed Safeguard.

ISS Asset	Classification	Safeguard (current)	Safeguard (proposed)

Business Impact Analysis Checklist ✓

____ Assets

____ Identify Your Information Inventory – Assets

____ Assign an Owner to each Asset

____ Assign a Value to each Asset

____ Threats, Risks

____ Identifying vulnerabilities to threats and damage potential

____ Prioritizing impact of threats

____ Develop a Risk Profile

- Identify the Risks
- Assess the Risks
- Plan the Risk Response
- Monitor the Risks
- Analyzing risks with new technology

____ Assign a Risk to each Asset

____ Classification

____ Classifying Assets (after Value and Risk)

____ Safeguards

____ Selecting cost-effective safeguards
____ Risk Acceptable

Chapter 4

Using the Templates

About the Templates

You have been given two templates to assist in the implementation of your ISS program. These templates are for the general employee or computer user, and also for the IS technical staff. These two different audiences have specific differences in how they practice and respond to security issues.

The majority of the content of both of the templates are security Rules. You can use the entire template as it is and not change any of the Rules or you can add, change or remove any Rules or other content that does not apply to your organizations security issues.

These templates produce a manual that can be handed out to the audience for reference, used in ISS training awareness as a training manual, or incorporated into the new hire process.

It is assumed the IS Technical Staff will also be a Computer User. If you are conducting ISS training sessions, it is suggested that the IS department be trained as a Computer User first to gain the basic knowledge that all employees will receive. After the Computer User training, then the IS department should also receive the IS security training.

Using the Templates

Communication and Addressing your Audience

If you are going to make changes to the templates content, it is important that you understand the writing styles, so you can keep the information consistent with your audience.

In the *Computer User's Security Handbook*, it is written using the term "you" to refer to your audience.

In the IS Technical Staff Handbook, the audience is addressed as "IS department" since there are many technical positions within the IS department and this handbook is general to anyone in the IS department. The role of the IS department is to support the end user, so there is reference to the "user" as the main target for the IS activities.

Templates Design and Organization

Modular Documentation

The design of the contents of the ISS template package is modular, that is, keeping topics contained in small sections, clearly labeled and in the chapter to which they relate.

How are the Rules organized?

This guide organizes the rules into categories for easy access and access. (expand)

Template Mechanics

(…)

Technology Dependent Areas

The templates structure was developed to be independent of any technology you have implemented into your security systems. One of the challenges in the design is to give the SO as much info as is needed without getting into any particular technology. For example,

Getting Started

- ***IMPORTANT***: Copy the template before you use it. (expand and add to *Quick Start Card*.)

MS Word Features Used

It is assumed you know how to use MS Word features in order to update the templates. There are a few MS Word features, however, that require some explanation. For complete details on using MS Word features, refer to a MS Word Guide.

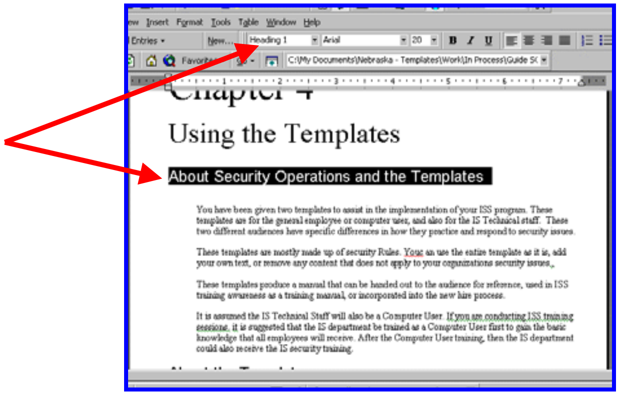
MS Word templates

The document files reside in the template area of MS Word. To see what templates you have available, …

When you install your template package, it will automatically …

MS Word styles

All of the chapter and section names have been chosen from the style guide. As you can see in the example below, the heading “About Security Operations and the Templates” is a Heading 1. This keeps your document consistent, automatically builds the Table of Contents, the allows for global updates.


ew Insert Format Tools Table Window Help
Entries
New...
Heading 1
Arial
20
B I U
Favorites
C:\My Documents\Nebraska - Templates\Work\In Process\Guide SC

Chapter 4

Using the Templates

About Security Operations and the Templates

You have been given two templates to assist in the implementation of your ISS program. These templates are for the general employee or computer user, and also for the IS Technical staff. These two different audiences have specific differences in how they practice and respond to security issues.

These templates are mostly made up of security Rules. Youc an use the entire template as it is, add your own text, or remove any content that does not apply to your organizations security issues.

These templates produce a manual that can be handed out to the audience for reference, used in ISS training awareness as a training manual, or incorporated into the new hire process.

It is assumed the IS Technical Staff will also be a Computer User. If you are conducting ISS training sessions, it is suggested that the IS department be trained as a Computer User first to gain the basic knowledge that all employees will receive. After the Computer User training, then the IS department could also receive the IS security training.

WARNING: Do not choose “ Update … style …” (get exact message …). This will change the style throughout the entire document!

MS Word Tables

Some of the content in the templates reside in tables. The table features are:

Table headings (expand on style)
Table text (expand on style)

MS Word Fields

MS Word allows you to enter parameters to globally be inserted into the document. For example, …

To add a field, …

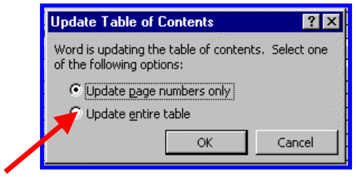
MS Word Linking

The list of Rules in the appendix of both templates have been automatically assembled from the Rules throughout all the chapters. So that you do not have to maintain the appendix list, a link has been set up for every rule. As you change a Rule in a chapter, it is also changed in the appendix list.

If you add a Rule, you will also have to add a link to keep the appendix list current. To do this, …

MS Word automatic Table of Contents

To update the Table of Contents, click on any text to highlight the entire Table of Contents, and then hit [F9]. This will update the page numbers and any headings you have changed. You may be asked:



Update Table of Contents

Word is updating the table of contents. Select one of the following options:

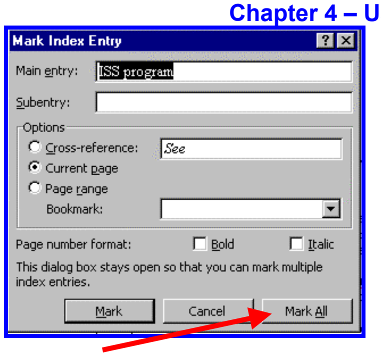
● Update page numbers only
○ Update entire table

It is suggested that you always select *Update entire table*. (Put better sample with it checked).

MS Word automatic Index

To update the Index, click on any text to highlight the entire Index and then hit [F9]. This will update the page numbers and any new entries you have marked.

To add an entry to the Index, highlight the text you want to appear in the Index, and hit [Shift] + [Alt] + [x]. You will receive:



Mark Index Entry

Main entry: ISS program
Subentry:
Options
○ Cross-reference: See
● Current page
○ Page range
Bookmark:
Page number format: □ Bold □ Italic

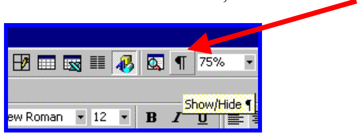
This dialog box stays open so that you can mark multiple index entries.

Click on the *Mark All* button to mark all occurrences of the selected text. It will appear on your screen as :

(show example) { …..}

and will put you into the Show/ Hide mode.

TIP: To exit the Show/ Hide mode, click on the Show/ Hide icon ¶.



Underlined Words

Many terms, phases, and acronyms are underlined throughout the template package to denote that there is more information about that topic elsewhere in the document. For example, all Glossary words are underlined implying that term is in the glossary.

The Rules are organized into meaningful security categories to facilitate locating a Rule. At the beginning of each Rule chapter (Chapters 3 -9 of the *Computer User's Security Handbook* and the *IS Technical Staff Handbook*.) For example,

Example: Physical Access Rules tells you there is more information about the topic.

If you decide to automate the template into an on-line system (e.g. Robo Help), you would use these underlined topics to build your links (go to) and pop-ups (glossary definitions).

Rule Statements

The Computer User's Security Handbook and the IS Technical Staff Handbook contain a comprehensive set of security Rules that you can tailor to meet your individual organizations needs. The content can be used "as is" or modified to reflect your security operations.

You can determine the size of your Rules guide. Important: If you have less rules, that does not mean they need to be written at a higher level.

Updating Rules

Initially you will need to review each Rule and determine:

1. … if you want to keep it, delete it, or modify it
2. … if you want to prioritize it – 1, 2, or 3
3. … if you want to use a full format or condensed format

On-going - what triggers a new Rule?

(Security changes, Technology changes, Business operations changes, NITC requirements change, HIPAA requirements change, …

Adding a Rule

(i.e. not listed in our template - their own) – copy and paste.

Adding a technology/ organization-dependant policy (i.e. not listed in our template - their own)

☝ *REMEMBER*: If you add a Rule, you must add a link for the appendix list. See *MS Word Features Used* on how to add a MS Word link.

Changing a Rule

Deleting a Rule

Use the standard MS Word deletion techniques. If you delete all the Rules in a category, then you will also need to delete the category.

Rule Formats

The templates provide 2 formats for a Rule. You can choose the Full or Condensed format..

Condensed Format

(Explain how to incorporate with full format).

Most of the Rules in the templates are in the condensed format which states the Rule Title and Rule Statement. as follows:

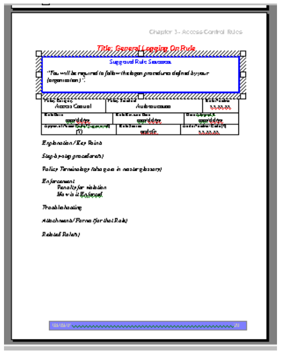
📖 **Rule - Unique User ID and Password**

You MUST have a unique User ID and a confidential Password to log on. This User ID and Password combination will be required for access to your organizations information systems. *See Password Rules in this chapter.*

Full Format

The templates also have a full format if you want to add additional information to your Rules. You can insert any Rule in the condensed format into the full format by putting the Rule Title and Rule Statement in the format as follows:

(Get new screen shot and use same rule as in condensed to show how it is actually done?)



Chapter 3 - Access Control Rules

Title: General Logging On Rule

Suggested Rule Statement

"You will be required to follow the logon procedures defined by your (organization)."

Access Control

Authentication

mm/dd/yy

Explanation / Key Points

Step-by-step procedure(s)

Policy Terminology (also goes in master glossary)

Enforcement
Penalty for violation
How is it Enforced

Troubleshooting

Attachments/Forms (for that Rule)

Related Rule(s)

Full Format Rule Fields

You can fill in the full format for each selected Rule. Below are the suggested fields you could use.

Identify the Rule	Rule Name/ Title Rule Description/ statement Rule Number - how is it assigned? Who? Rule Category(s)
Dates	Date of Rule (history) Revision Date(s)

	Date Adopted/ approved (?)
About the Rule	Timing Process (flowchart) Responsibility (who does it) Key Points Step-by-step procedure(s) Rule Terminology (goes in master glossary)
Enforcement	Penalty for violation How is it Enforced (What if..) Reporting requirements
Supporting Topics	Troubleshooting Attachments/ Forms (for that policy) Related Rules

Assigning Priorities to Rules

You may want to assign priorities to your Rules to know which ones to emphasize and which ones to enforce. It is suggested you use the following priority levels:

Priority 1	Critical Rules Use full format
Priority 2	Strongly Suggested Rules Use full format or condensed format.
Priority 3	Optional Rules No Format, just a list of Rule Title and Suggested Rule Statement. It will require less printing of pages and more cutting and pasting.

Template Parameters { }

You will need to decide certain values that are inserted into parameters. They are identified by the brackets { }. These parameters can appear in any of the 3 guides.

The following parameters have been incorporated into the templates:

# attempts to log on	You will be allowed {3} failed attempts to try to logon.
# daily log ons	You are not permitted to log on more than {10} times a day.
# days passwords expire	Your passwords will expire every {10} days.
auto log off	You will automatically be logged off if there has been no activity on your workstation for {10} minutes. This can different from platform to platform.
dormant User ID	Your User ID will automatically have the associated privileges revoked after {30} days of inactivity. If you are a temporary employee, contractor, or consultant, it will be revoked in {15} days.
#password attempts	You will be allowed {3} failed attempts to successfully enter your Password. OR You will be allowed 3 failed attempts within {5} minutes."
reusing passwords	You cannot reuse your Password for {15} changes. OR You must not use the same password more than once in a {12} month period.
inspection advance notice	Your organization maintains the right to conduct inspections of your telecommuter offices with {1} day advance notice.
# password attempts dial-in	The maximum permissible Password attempts for dial-up access is {3}. If you have not provided a correct password after three consecutive attempts, the connection must be immediately terminated.
# months expire Internet	Your User ID on Internet accessible computers must be set to expire {3} months from the time they are established.

Confirm e-offers	All contracts formed through electronic offer and acceptance messages (fax, Electronic Data Interchange, E-mail, etc.) must be formalized and confirmed via paper documents within {2} weeks of acceptance.
# minutes for unattended workstation	If you leave your workstation unattended for {10} minutes, your screen will lock up.
# days valid temporary badge	If you forgot your badge, you must obtain a temporary badge by providing positive proof of identity. A temporary badge is valid for {1} day only.
# weeks to respond privacy disclosure	A subject must be given advance notice that their personal data held by your organization has been requested by a third party. Unless compelled to release the data by clear and authoritative law or regulation, a reasonable period of {2} weeks must be provided for the subject to block this disclosure. No response from the subject can within that period can be considered to be acquiescence to the disclosure.
# years to keep records of disclosure	If you have the proper authority and disclose information to a third party, you must keep records of all such disclosures including specifically what information was disclosed, to whom it was disclosed, and the date of such disclosure. These records must be maintained for at least {5} years.
# weeks notice to customer to get info	If you must get customers information (i.e. via a subpoena), the customer will be given {2} weeks advance notice prior to the release to provide the information.
# months to see personnel records	You could allow each employee a copy of their own personnel records to review and to ensure that it contains no errors every {12} months.
# years data retention	You must retain all financial accounting, tax accounting, and legal records for a period of at least {7} years. All other records must be retained for a period of at least {5} years.
# day input	

retention	Business source documents containing input data must be retained for at least {90} days beyond the date when this information was entered into your organizations computer system(s).
phone numbers	If you need to ask ISS questions, call (xxx) xxx-xxxx. If you need to report an incident, IMMEDIATELY call (xxx) xxx-xxxx.
Remote # days backups	You must make periodic backups of all critical information and store it away from the portable device. These backups should be performed every {1} day. They should be stored elsewhere than the portable computer's carrying case.
Training	Employees should be have a formal security briefing within {3} days of their start date/ receiving their ISS packet.
Organization Name	Enter your **{Organization Name}**
Guide(s) name	Enter the title of your **{Guide name}**

Completing the Templates

About Completing the Templates

The majority of the templates are Rules …

Computer User’s Security Handbook template is … (About Employee/ User Awareness / Individual Use)

The IS Technical Staff Handbook template is used the same way as the Computer User’s Security Handbook Template.

The Sections of the Template(s)

The sections of the Computer User’s Security Handbook template and the IS Technical Staff Handbook template are:

- Title Page
- Table of Contents
- (front matter)
- Chapter 1 About Information Security
- Chapter 2 Security Incidents
- Chapter 3 – 9 Rules
- Chapter 10 Getting ISS Help
- Appendix
- Index

Updating each Section

Title Page

1. Enter your **{Organization Name}.**

2. Enter the title of the **{Computer User’s Security Handbook}** and **the {IS Technical Staff Handbook}**. Other possibilities are:

   General Employee ISS Booklet
   ISS User Reference Guide

   IS Department Security Handbook
   Technical Security Guide

Table of Contents

The templates Table of Contents has been designed with the structure and alignment automatically based on the chapter names, sections and sub-sections used throughout the documents.

It is recommend that you do not change the Table of Contents (TOC). You can change chapter names, headings and sub-headings, but not the Table of Contents format and structure.

REMEMBER: Hit F9 and the Table of Contents will automatically update chapters, sections, sub-sections, and page numbers. See *MS Word Features Used* in this chapter.

(front matter)

Insert any information you want to be separate from the page numbered guide, yet a part of the guide. For example: Proprietary Statement, Copyright / Trademark information, organization logo, and such.

Chapter 1 – About Information Security

In both templates, Chapter 1 covers all the general information about ISS. It is the introduction to ISS and to the guide itself. Here you can get an overview of what ISS is all about and learn some of the key areas of concern. You can use this chapter as it is or make changes. It is mostly boilerplate. You might want to add sections unique to your organization like: marketing ISS, your organizations support, and such.

Chapter 2 – Security Incidents

This chapter is slightly different between the templates due to the nature of the audience. The computer user needs to know the basic incident reporting requirements, while the IS technical staff may need to get more involved in the technical detection and evidence preservation.

A chart has been provided to summarize the reporting structures. You can update this chart to reflect your incident reporting structures.

Chapter 3 - 9 Rules

The templates contain a different set of Rules for each audience. The IS technical staff should be aware of the Rules in both templates.

Review each Rule and determine:

- if you want to keep it, delete it, or modify it
- if you want to prioritize it (1, 2, or 3)
- if you want a full format or condensed format

Computer User’s Security Handbook template

The Computer User's Rules are arranged in the following categories:

Chapter 3 - Access Control Rules
Chapter 4 - Network Rules
Chapter 5 - E-mail, Internet, and E-commerce Rules
Chapter 6 - Individual Use/ Copyright Rules
Chapter 7 - Acceptable Use Rules
Chapter 8 - Workstation Rules
Chapter 9 - Physical Security Rules

IS Technical Staff Handbook template

The IS Technical Staff Rules are arranged in the following categories:

Chapter 3 - Access Control Rules
Chapter 4 - Network Rules
Chapter 5 - E-mail, Internet, and E-commerce Rules
Chapter 6 - Workstation and Equipment Rules
Chapter 7 - Systems Development Rules
Chapter 8 - Disaster Recovery Rules
Chapter 9 - Physical Security Rules

Chapter 10 – Getting ISS Help

This chapter is dedicated to helping the reader to answer any questions or concerns about ISS.

Review the Troubleshooting Chart and …

Appendix

Insert any information you want to be used as reference for the guide. This is where you put lists, supporting documents, and such. They are usually part of the page numbered guide. (unlike front matter).

The templates both contain the following appendix items:

List of Rules   This is a consolidated list of all the Rules in the guide. This list or Rules-at-a-glance is automatically linked to the Rules in chapters 3-9. (not yet!!)

Glossary   An ISS glossary. It is the same in both templates.

Attachments   …

Index

To help your reader find the topic they want to read, an Index is critical. Using standard MS Word indexing, you can update your index to include any words, phases, or acronyms. See *MS Word Features Used* section in this chapter.

Working Paper #x
Templates Checklist / Procedures

Be sure to follow these steps to use the templates:

1. 💣 ***IMPORTANT***: Copy the templates.
2. Review each Rule and determine:
   -if you want to keep it, delete it, or modify it
   -if you want to prioritize it (1, 2, or 3)
   -if you want a full format or condensed format
3. …

Chapter 5
Implement an Incident Program

What is an Incident Program?

In your ISS plan, the most important program you can implement is one that handles suspicions and incidents quickly and thoroughly. You need to be in position react, detect, and resolve. The key to a good response is having your team established, trained, and ready to react to any and all occurrences.

Your Incident program will usually involve your security team, but you may want to include others in your response team. For example, making managers of user departments aware of how to respond may be critical especially if the incident is occurring in their area with their information. The IS department will probably be a big part of the response team to provide the technical knowledge and evidence preservation.

The three main components that make up the Incident Program are:

- Prevention
- Detection
- Response

Suspicions and Incidents

Security Incidents or security breaches can occur at anytime. Your prompt attention to reacting to reported incidents could greatly deter the amount of damage, loss, or disclosure that has taken place.

Suspicions and Incidents

A Suspicion, an unconfirmed assumption of attack, is not yet an Incident. For this reason, it is even more critical to report a suspicion so as to avoid the incident from even happening or greatly decrease any negative results.

It is the responsibility of every employee to do their part in detecting and reporting any possible incidents or suspicions.

Prevention

Prevention is the key to good security practices, however, even with all the proper protection methods in place, there are always ways to compromise it. In order to know how to prevent incidents, you need to know what your assets are, where the risks lay, and how to protect critical information from being targeted. For complete details, see *Chapter 3 Business Impact Analysis* section *Safeguards*.

Detection

Detection is the only way of knowing when a system is being compromised. Without proper detection, you may never know when an incident has occurred and therefore it may continue to happen. Even worse that having a security incident is having one and not knowing it.

To understand intrusion detection, you must be aware of the intruder, where attacks come from, what motivates them, how attacks occur, and who the attackers are. Not all organizations have the resources to conduct their own intrusion detection and analysis. In these situations, it may be necessary to identify other sources for assistance in tracking and responding to possible incidents.

IMPORTANT: The difference between an incident and a disaster is detection!

Intrusion Detection Methods

There are many methods used to detect suspicious system behavior. Some methods will keep the intruder busy, while he is tracked down. Others will lock the intruder out until he is discovered.

It is important that detection methods not only find known attacks scenarios, but also new scenarios. Detection methods should look for the unusual and unexpected.

Intrusion detection systems (IDS) exist to help you safeguard your assets. These systems can monitor configurations, compare user actions, and distinguish conflicts in activities. IDS runs constantly with your system in the background and only notifies you when it detects something suspicious or illegal.

Whatever method you choose, be sure it is used daily and incorporated into your Incident program.

Tracking Intrusions

You organization shall implement procedures for logging information on intrusion attempts and storing that information in a manner for later analysis or use by law enforcement.

Incident Patterns

Response/ Reaction

Now that you have all your safeguards in place and are actively practicing good detection techniques, you can only hope that you have thought of everything. As many ways as there are to prevent mishap, there are just as many to circumvent your safeguards.

The key to further protecting your information even in the event of an attack is to have a good response plan implemented. A quick reaction can greatly diminish the damage.

If you do not have a response team established, you are depending on the reactions of users, IT and management to react, thus possibly turning a containable incident into a serious problem.

Your Incident Response Team

The security team you assembled in Chapter 2 may or may not be the same group that is responsible for the reaction to an incident. Be sure your response team knows who they are and have been trained in ISS issues.

TIP: Periodic mock drills are recommended for each possible type of attack.

Incidents Response Centers

There are companies that can assist in the incident handling process, but your internal response is the key. These companies can help you after the fact, with collecting and processing evidence and furthering the reporting to law enforcement and such if required.

Responding to ISS Incidents

If an incident is reported, you must follow these steps:

1. Verify that it is indeed an incident
2. Analyze the intrusion
3. Communicate with all appropriate parties
4. Set up barriers to block the intrusion (if possible)
5. Collect and protect evidence
6. Investigate all issues
7. Document the incident
8. Recover from the incident
9. Follow up on the incident
10. Handle media inquiries (if necessary)

Catastrophic Event

For catastrophic disasters such as fire, bomb threats, hostage situations, floods or destructive storms, the goals of employee safety and damage containment apply. Notification procedures will include the appropriate public service departments (Fire Department or Police Department).

Secured Area Intrusion

For intrusion of secured areas, the goals of employee safety, intruder identification, and if warranted, the intruder's removal from the premises apply. Notification procedures will include building security or local police.

Virus Reporting

Most of us have encountered a computer virus directly or indirectly already. The greatest danger with computer viruses, is that if they go unreported and uncontained, it will continue to spread. Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. You must report a computer virus infestation immediately after it is noticed.

Electronic Intrusion

For cases involving electronic intrusion, the goals of data integrity, data recovery, method of breach and intruder identification apply. Notification procedures could include the State Patrol (if deemed serious enough), the potentially affected business area manager, software application support manager, and data center manager. Any activity monitor data, collected as a normal part of doing business, should be kept until the incident has been cleared.

Unauthorized Access Intrusion

Whenever unauthorized system access is suspected or known to be occurring, you must take immediate action to terminate the access. If these actions do not completely suppress the unauthorized activity, assistance from the Corporate Information Systems Help Desk (?) must immediately be sought. You must inform both technical staff (and perhaps users) that they must take immediate action to suppress unauthorized system access.

Notifying the Intruder – yes or no?

In some cases, a stern cease and desist message must be sent to the source of all attacks against your organizations computers whenever the source or intermediate relay points can be identified. The intention of this is to send a message to attackers that their activities have been noticed and that they should stop immediately. Such a message may, in some instances, be enough to discourage an intruder from further efforts. If an attacker is using a shield such as a relay site (need to define?), then the message can still be sent to the relay site's administrator. Even if the attacker doesn't get the cease and desist message, someone who manages that site can still take action, such as revoke the privileges of the offending User ID or otherwise tighten-up security.

Sometimes someone outside your organization can be valuable in helping to detect an incident. For example, if a web page were to be modified by hackers, and then noticed by a potential customer. In an indirect way, this solicits outsiders to assist with information security. Often customers and prospects are the first to notice there is a problem. The inclusion of contact information on web pages helps outsiders to report problems. You could even add to your web site along with the contact information: "Please report any suspected security violations or problems to **{contact name}**".

Notifying Employees of Incidents

When appropriate, notify your employees of known incidents.

Evidence

When an incident occurs, you must gather the facts of what happened, how it happened, and note any indictors or trails that can help in the investigation. Lack of a clear trail of evidence when investigating any ISS crime is critical. Without proper evidence, you may be prevented from taking legal action.

Collecting Evidence

If possible, do whatever you can to quickly gather evidence of what you are witnessing or detecting. Do not let this task interfere or slow down the reporting process. For example, you may want to write down peculiar system performances, error messages to help the investigation.

Preserving Evidence

(…)

Recording Evidence

(…)

Incident Reporting

Gather Evidence … Report it… and Be Prompt!

💣 ***IMPORTANT***: The most important thing to remember is to be PROMPT.

All information security suspicions and incidents must be reported as quickly as possible through your organizations proper internal channels. If problems and violations go unreported, they may lead to much greater losses for the organization than would have been incurred, had the problems been reported right away. Delays in reporting can mean massive additional losses for the organization.

Internal Reporting

This reporting structure is internal to your organization and includes the following (response team):

- security department
- Help desk
- your manager
- security guard
- information owners
- IS system administrator
- others… ?

Initially problems should be reported internally rather than externally, reducing any adverse publicity or loss announcements. External reporting should only be done an extreme emergency.

In many organizations, the help desk would then contact information security technical specialists (typically by pager).

Internal reporting could include violations of policies and other non-legal requirements.

Centralized Reporting

If is sometimes necessary to centralize the ISS department to better control ISS issues. This department may include those not on the response team.

The reporting process can be to a central group such as the Help desk as opposed to line management or a service provider. The reporting process should not always go through management, since this additional step takes longer and is likely to delay corrective actions.

Establish a centralized Information Security Department as the focal point for all reports of vulnerabilities and violations. In many organizations, these reports go only to lower level managers (such as department managers), and never find their way back to a centralized group. Unless there is centralized reporting, no loss history can be compiled, no loss analysis can be conducted, and no related decision-making can be performed. Centralized reporting is also useful for the mobilization of a computer emergency response team (CERT), an organization-wide contingency plan, and other important defensive resources. It also alleviates the reporting party's concerns about short-circuiting the chain of command.

External Reporting

Information describing information security problems is valuable, certain government regulations (such as those pertaining to commercial banks in the United States) now require the reporting of information security problems to government regulators.

(Note: You must report incident to state patrol and then they may accelerate it to the FBI. Most organization's will not go directly to the FBI.)

If criminal action is suspected, the organization must contact the appropriate law enforcement and investigative authorities as quickly as possible.

While internal reporting is to be encouraged and required, external reporting is sometimes necessary and includes the following:

- law enforcement, police
- fire department
- FBI
- external auditors
- outside authorities
- local and national organizations.

(From NITC Agencies and institutions shall report potential criminal violations to the Nebraska State Patrol and the Federal Bureau of Investigation.)

If required by law or regulation, management must promptly report information security violations to external authorities. If no such requirement exists, in conjunction with representatives from the Law Department, the Security Department, and the Internal Audit Department, management must weigh the pros and cons of external disclosure before reporting incidents. Many organizations still refrain from reporting computer crimes because the public embarrassment, cost, and diversion of staff resources appear to outweigh the benefits. Benefits include setting an example to discourage other violations, giving employees the impression that management believes in the criminal justice system, and obtaining restitution. It is often desirable that management be given the ability to choose to report violations on case-by-case basis. Some organizations may wish to establish a committee that will evaluate the merits of external reporting on a case-by-case basis. As it stands, a significant number of computer crimes go unreported, and a significant number go undetected.

Incident Reporting At-a-Glance

To Report …	Comments	Call … Do …
… an incident in process.		1. Call …
… sensitive information is disclosed, lost, or damaged.		1. Call …
… software/ system malfunction	Do not attempt a recovery yourself.	1. Note (if time) any error messages, unusual system behavior (how is it behaving different than before?) 2. Stop using the computer. 3. Disconnect from any attached networks. 4. Call …
… a virus	Because viruses have become very complex, users must not attempt to eradicate them without expert assistance. If users suspect infection by a virus, they must immediately:	1. Shut-down the involved computer. 2. Disconnect from all networks. 3. Call … ??? (help desk, security, manager?)
… an offensive E-mail, call, etc.		Respond directly to the originator. If the originator does not promptly stop sending offensive messages, report it to ??? (HR?)
… suspicious behavior.		1. Call …
… known systems security vulnerabilities, risks, alerts, and warnings		1. Call …
… equipment damage or loss		1. Call …
… physical access violation		1. Call …

Investigating Incidents

Investigating the Cause and Impact of IS Incidents

(…)

Ensuring the integrity of IS Incident Investigations

(…)

Conducting Internal Investigations

Until charges are pressed or disciplinary action taken, all investigations of alleged criminal or abusive conduct must be kept strictly confidential to preserve the reputation of the suspected party.

Whenever evidence clearly shows that your organization has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that: (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

Some organizations - instead of requiring investigations after an organization has been shown to have been victimized, investigations can be required if such acts are only suspected. Or you can require that an investigation be performed after an abuse has been noted, even if this abuse is not legally a crime; this approach of course requires that the term "abuse" be defined. An example of a computer abuse that is not a computer crime in many jurisdictions is privacy violation.

Documenting the Incident

Documenting the incident is critical for the investigation and also to track future similar attacks. Someone should be designated to the task of preparing and maintaining all incident reports.

You organization should require a written report following the initial oral report. The scope could be expanded to include "suspected problems," not just "problems and violations." The word "weaknesses" may also be used instead of "problems." While internal reporting is to be encouraged and required, external reporting is not encouraged unless necessary.

Incident Reporting Form

You employees should have an Incident Reporting Form to capture the events they witnessed. (See attachment for sample form?)

Incident Reporting Checklist

(…)

Incident Reporting Retention

Information describing all reported information security problems and violations must be retained for a period of {3} years.

Certain important information security related information must not be destroyed. It can be helpful when doing risk assessments, when planning information security projects, and when developing budgets. It may also be useful for prosecution or disciplinary actions. The applies to computer logs and internal correspondence, as well as notes from secret investigations, "unless approved in advance.

Incident Follow Up

You must follow up on all reported incidents or suspicions. Without a good follow up process in place, you will discourage your employees from future reporting.

Enforcement

Enforcement is sometimes difficult in a working environment, but without enforcement the policies and procedures you have put in place with your ISS program may not be taken seriously.

What if an employee violates a Rule?

It is up to your organization to determine how and when to take action onan employee that has violated a Rule. Even if the violation was an accident, you may still want to take action in the form of a warning or other corrective activity.

Legal Responsibility

Perpetrators of crime should be prosecuted by the organization to the full extent of the law. Suitable procedures are to be developed to ensure the appropriate collection and protection of evidence for these purposes.

In order to prosecute successfully, you need proof. This can be difficult to provide unless your organization's information systems have adequate controls and audit capabilities.

(For non-criminal attacks, your organization should …)

Chapter 6
Implement an Awareness Program

What is ISS Awareness?

Information Systems Security (ISS) awareness is an important part of any security plan or program. Employees at all levels need to understand that they play a large part in protecting their organizations information assets. Awareness teaches employees that they are a key piece of the total security environment. Through training and on-going reinforcement, everyone will begin to "Think Security" as a matter of daily practice. Only with full support and cooperation of all employees can a successful ISS program be established and maintained.

While training is sometimes one of the first items to feel the budget pinch, its importance is acknowledged and supported not only as one of the seven security principles adopted by the Nebraska Information Technology Commission, but it is also a requirement for HIPAA compliance. An awareness program process has two major parts:

- awareness briefing (initial rollout)
- continuous awareness materials

Awareness Briefings

Before granting access to systems, all employees should receive at least a Security Awareness information packet.

All employees should be taught the importance of information security, what the rules are that must be followed, and what to do if there is a violation. An ISS awareness program is critical to any ISS program design. Increased awareness increases the proper use of security principles and the likelihood that suspicious activities will be noticed and reported.

ISS policy and standards are ineffective if individuals at any level of the organization are unaware of the importance of security policy, do not understand established standards or fail to perform required practices for any reason. Good security is "a state of mind" that can best be achieved by a program or process that reinforces the concern and appropriate actions on a regular and ongoing basis.

Continuous Awareness Materials

Information Security is not a one-time event, nor is it a "volume of rules sitting on the shelf". Good security practices are not always obvious, intuitive or easily incorporated into established routines. To have maximized effectiveness information security standards must be known, understood, believed to have value, and appropriately and consistently practiced.

A program that offers continuous reinforcement of the organizations position with regard to handling the many aspects of ISS provides the tone and commitment to support greater sensitivity to the potential of an unwanted compromise or loss of assets.

On-going and positive reinforcement for the necessity for information security policy and standards provides awareness and a "mind set" that encourages the intended practice of the established procedures. Without such reinforcement, policies or standards may be perceived as not relevant, necessary, or valuable and may be "followed" but not be practiced in a manner that supports full effectiveness.

The following are suggestions for ways to keep your awareness program alive:

- Refresher classes
- Regular updates to materials
- Top management communications to staff
- Conduct regular readiness drills
- Poster reminders

As technology and business needs change, the program will need to be revamped accordingly. Awareness never ends.

What is an Awareness Program?

An ISS awareness program brings ISS to a personal level. Everyone is responsible for the security of the information they use. The purpose of an awareness program is to teach the audience how to incorporate the rules and procedures into their daily operations.

Two awareness programs have been included in this template package:

- Computer User Awareness – broad based awareness for all employees/ contractors
- IS Awareness – focused awareness on the technical security issues

Incorporating your Awareness Program

ISS awareness can be incorporated into the following workshops:

- Initial ISS program rollout
- Continuous awareness refresher courses
- New hire orientation
- New hire package

Security is Everyone's Business

ISS is every worker's duty on a day-to-day basis. Specific responsibility for information security is NOT solely vested in the Information Security Department. Information security is multi-departmental, multi-disciplinary, and multi-organizational in nature.

This means that information security cannot possibly be adequately addressed by a single department within your organization. Thus every worker must do their part in order to achieve appropriate levels of information security. After all, information can be found nearly everywhere in the organization and nearly every worker utilizes information in order to do their job. It is only natural that every worker should be specifically charged with responsibility for information security.

Security and Performance Reviews

Some organizations may want to go one step further and incorporate a question into performance review forms. The question could read something like this: "Does the employee observe information security policies in the course of his/her work?"

This must be supplemented with additional instructions, telling workers exactly what is expected of them.

Signed Agreements

Without confirmation that all new and existing employees are aware of security policy there is no assurance that the desired actions are understood or followed. Failure to follow policy or practice standards for any reason reduces the value of such statements to "documents of prosecution" and negates the positive reinforcement and protective intent for which the information policy and standards exist.

Some organizations require users to sign a statement that they agree to: (*See Appendix for samples.)*

- abide by information security policies and procedures. A signature on a form with this statement, and perhaps a summary of the policies and procedures, can be required before a user is given a user-ID and a password.

- their understanding of the code of conduct by annually signing a form acknowledging that they agree to subscribe to the code. The intention is to annually remind employees that they must abide by the organization's code of conduct. From a legal standpoint, it is desirable to have employees acknowledge in writing that they have read and understand that a code of conduct is a required part of their job. If they are subsequently terminated due to code of conduct related problems, there is no doubt that the employee understood what was required of him or her. This agreement therefore reduces the probability of a wrongful termination lawsuit.

- to provide evidence that every employee has attended ISS class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions. For existing employees, a modification of this agreement could state they must attend within **{6}** months of the date when such courses become available.

- Every worker must understand the ISS rules and procedures and must agree in writing to perform his or her work according to such rules and procedures.

- All employees with access to computer systems must be informed of security policies and procedures and their responsibilities in writing. All new employees with access to critical systems or sensitive information will sign a statement acknowledging they have received and read the policy and understand their responsibilities. This should include knowledge of the consequences of violations of security procedures.

- A signed statement indicating awareness, compliance and intent of continued compliance with information security policy and standards will be required upon annual review of each employee with access to critical systems or sensitive information.

- Contractors, agents acting on behalf of the state, auditors, and other non-employees in a position to impact the security or integrity of information

assets of the state will be made aware of the Information Security Policy. These individuals must sign a statement acknowledging they have received and read the policy and understand their responsibilities.

Mandatory Awareness Training

ISS training should be mandatory. Every worker must attend an information security awareness class within {3} months of the date of employment. To provide evidence that every employee has attended such a class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions.

Awareness Applies to Everyone

All workers (employees, consultants, contractors, temporaries, etc.) are required to receive the same level of ISS awareness and training. This training requirement should be included as appropriate in all contracts. Workers must be provided with sufficient training and supporting reference materials to allow them to properly protect your organizations information resources. Management must allocate sufficient on-the-job time for employees to acquaint themselves with the organizations security rules, procedures, and related ways of doing business.

What makes up an Awareness Program

Your awareness program can be delivered in many ways. Initially, when you rollout your ISS program, it is suggested that you offer awareness training in a classroom environment. A classroom environment with a standardized curriculum gives a consistent message to all attendees and encourages interaction and discussion.

An awareness program can consist of the following:

- Campaign
- Training
- Materials

Awareness Campaign

An awareness campaign is a good way to initially incorporate the ISS program. A campaign can “advertise” that the ISS program is coming soon and with good promotional items, you can gain employees attention, emphasize key points, and even educate them on key security issues.

Campaign Mottoes/ Themes

You may want to start a theme that identifies the ISS program or the awareness program itself. For example: call the training class “Security 101”, or “Think Security” .

The T.E.A.M. approach (<u>T</u>ogether <u>E</u>veryone <u>A</u>chieves <u>M</u>ore) is also effective to bring everyone together as one complete ISS program and the concept that we will have to all work together to make it a success. Everyone is responsible for the security of the information they use.

Campaign Ideas

- Stage vulnerability demonstrations.
- Give small prizes (i.e. free lunch) for exemplary staff (i.e. reported a violation)
- Give “traffic ticket” warnings reflecting policy statement violations. (due it when they are all out for a drill, ….)
- Initiate an unannounced “unauthorized software duplication” inventory where PCS are checked for illegal software.
- Adopt an annual ISS day on with special educational materials and events.
- Develop a “tagline” or theme that represents ISS at your organization.

Awareness Materials

The template package prepares your ISS program materials. You may need to develop additional training materials, checklists, and such for your organizations particular needs.

Suggested awareness materials:

Reference Rule Guide (results from templates)
Training Guide (results from templates)
E-mail messages
Articles in your organizations newsletter
Magazines, internet articles for circulation
Bulletins and alerts
Posters
FAQs
Web announcements
Labels for system (PC), diskettes, etc.

Awareness Training

The best way to educate your employees on ISS awareness is in a training classroom environment. The curriculum for the class can follow the same sequence as the guides you created from the templates.

Training Purpose

To teach the attendees how to recognize security issues, to be involved in the overall security of the organization, and to know what to do if they encounter an incident.

Training Specs

- Self-teaching or classroom
- Informal, workshop, seminar
- Role playing
- Stage mock incidents to see responses
- On-the-job training

Other Special Training Topics

There may be additional training classes needed for some specialty ISS areas. These are areas that require getting deeper into the topic content for certain computer users that have a special need. These specialty classes may be:

♦	Remote access	You must complete an approved remote systems access training course prior to being granted privileges to use dial-up, Internet, or any other remote access data communications system.
♦	Copyright	?

Training Materials

For classroom awareness training, you may want to create the following class materials:

- Training Guide (from templates)
- Handouts
- Overhead slides
- Exercise workbook
- Quiz (to measure results)
- Practice sessions (do mock security drills)
- Presentation tools
- Class Evaluation
- Classroom posters
- Giveaways – buttons, pens, certificates, t-shirt's, mouse pads, …

Training Audience

The training audiences can be very general or very specific to a certain job taks. The following lists the main audiences Guides that requires ISS awareness training.

Management

Management at any level many require a different view of ISS business practices. Upper level management may need simply an executive overview, while middle management and user department management may need to know more about prevention, detection, and incident reporting.

Although management is a separate audience, the materials and curriculum are a subset of the Permanent Staff course.

Permanent Staff

The largest of all audiences, the permanent staff audience requires a unique training class and can use the *Computer User's Security Handbook* template to produce the training manual.

Temporary Staff

The temporary staff audience may not need as much training as the permanent staff since HR issues and such do not apply. They are not necessarily a separate audience, but are a subset of the Permanent Staff course. They could also be combined/ incorporated with Permanent Staff.

Contractors, Agents, Auditors and non-Employees

See Temporary Staff (above).

Technical Staff/ Management

This is a highly specialized and separate audience from the Permanent Staff group. They require a unique training class and can use the *IS Technical Staff Handbook* template to produce the training manual.

Security Officer/ Staff

The security department consisting of a security officer and security staff is a separate audience and they require a unique training class and can use the *Security Officer Instruction Guide* to produce the training manual.

Working Papers and Checklists

1. Who do you want to make aware of ISS …

ISS Topic	Audience	Class

2. For each audience, define the curriculum agenda.

Computer User Agenda

- About ISS
- Rules
- Procedures
- Questions and Answers
- Quiz
- …

IS Technical Staff Agenda

- About ISS
- Rules
- Procedures
- Questions and Answers
- Quiz
- …

Chapter 7

Getting Help with the ISS Program

About Getting Help

(describe high level)

Call for Support (?)

(Notes. What do they do if they need help understanding the templates? Call xxx-xxx-xxxx for assistance …?)

Troubleshooting the Template

Problem/ Question	Explanation	Action
What should I do if …	You are not ..	1. 2. 3.

Appendix

Appendix A - Attachments

NITC Security Architecture Document

Policies from Other agencies (already developed by other agencies, refer to them in the details of the content))

IMS Charter – project level

Appendix B - Reference List

The following resources were used to gather the information contained in this template package:

"Information Security - Protecting the Global Enterprise" by Pipkin

"Inside Internet Security - What Hackers Don't Want You to Know" by Crume

…

Index

State of Nebraska

Information Systems Security (ISS)

Computer User's Security **Template**

This template provides the foundation from which to build your organizations ISS rules. You can use the template rules as they are, add your own rules, or delete those that do not apply.

Final Draft
August 24, 2001

This page is intentionally left blank for pagination of double-sided printing.

State of Nebraska

Information Security Systems (ISS)

{Your Organization Name}

Computer User's Security Handbook

"A complete ISS awareness guide for the State of Nebraska employee."

This page is intentionally left blank for pagination of double-sided printing.

State of Nebraska
Information Security Guidelines

These Information Security Templates and Guides were developed by the Security Architecture Workgroup under a project funded by the Chief Information Officer and the Nebraska Information Technology Commission.

Additional information about these documents can be found at:
http://www.nitc.state.ne.us/tp/workgroups/security/index.htm

Computer User's Security Handbook

Version 1.0
August 24, 2001

Prepared by:

This page is intentionally left blank for pagination of double-sided printing.

Table of Contents

Chapter 1
About Information Security

About Information System Security (ISS)

Welcome to the age of technology, where information is readily available and easy to access. Information and your computer systems are critical assets that support your organizations current and future business practices. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, and employees.

In general, security is smart business practices. You, the employee, therefore are a key factor in protecting information, as you use it in your daily job. The intent of this guide is to educate you on information security by making you aware of threats and risks, giving you a good set of Rules to incorporate into your own business practices, and to know what to do if you encounter a security violation.

ISS is multi-departmental, multi-disciplinary, and multi-organizational in nature. This means that information security cannot possibly be adequately addressed by a single department within your organization. You must do your part in order to achieve appropriate levels of information security. After all, information can be found nearly everywhere in the organization and nearly every worker utilizes information in order to do their job. It is only natural that every worker should be specifically charged with responsibility for information security.

Users may be employees, temporaries, contractors, consultants, or third parties with whom special arrangements have been made. If you have been permitted to use information, you must also have the understanding that you must properly protect it.

Your ISS Program

This Information Security System (ISS) Program has been designed with the employee in mind. It focuses on the tools you require to do your job, your work habits, and even your work area.

It Takes a T.E.A.M.

It takes a TEAM and you are an important part of it. All employees, consultants, contractors, and temporaries must be provided with sufficient training and supporting reference materials to allow you to properly protect your organizations information resources. You should be allowed sufficient on-the-job time to acquaint yourself with the ISS Rules and to know what to do in the event of an incident.

Together
Everyone
Achieves
More

Compliance

All employees, consultants, contractors, and temporaries must be subject to the same Rules and compliance of those Rules. If is your responsibility, as a State of Nebraska employee, to comply with all Rules of your organization.

Compliance Form

(See attachments in Appendix)

Consequences of Non-Compliance or Violation

(…)

Acknowledgements

Employee Signed Documents

You may be required by your organization to sign an agreement as part of the ISS program requirements. *See Appendix A – Attachments*.

Using this Guide

This *Computer User Security Handbook* is a reference tool for the employees of the State of Nebraska. It defines the general security areas, accompanying Rules, and the "how to" steps for any security tasks you may need to perform. It can be used as a training tool for an awareness program or for on-going reference support. This guide could be handed out as part of the new hire package.

About Rules

The majority of the chapters in this guide focus on specific Rules that target the key areas that you can protect. They are grouped by category to help you locate any specific rule.

Special Features of this Guide

(Introduce glossary, troubleshooting, …)

Guide Structure - How Its Organized

To understand the layout of this guide and to help you find a Rule by chapter:

Chapter 1	General ISS Information
Chapter 2	Security Incidents and Reporting
Chapter 3	Access Control Rules
Chapter 4	Network Security Rules
Chapter 5	Individual Use/ Internet/ E-mail Rules
Chapter 6	Individual Use/ Acceptable Use Rules
Chapter 7	Individual Use/ Copyright Rules
Chapter 8	Access Control/ Workstation Rules
Chapter 9	Physical/ People Security Rules
Chapter 10	Getting ISS Help
Appendix	Appendix A - Attachments Appendix B - List of Rules Appendix C – Glossary
Index	

ISS At-a-Glance

In order to fully understand the purpose of the Rules in this Guide, it is important to know more about ISS Security. This section gives you a brief overview of the key areas and reasons why you need to protect your organization's information.

Understanding ISS

One of the biggest concerns facing organizations today is to anticipate the type of security threats or intruders so they can safeguard against the attack.

Intruders

Intruders can come in from the outside or be an internal worker. There are amateur and professional intruders. Intruders can be very technical and persistent. Intruders are also adaptable. If you pick the top 10 risks to safeguard, they'll pick 11 or 26.

Types of Intruders

A hacker is an individual whose primary aim is to penetrate the security defenses of large, sophisticated computer systems. A truly skilled hacker can penetrate a system right to the core and withdraw again without leaving a trace of the activity. Hackers are a threat to all computer systems which allow access from outside your organization's premises. The worlds primary target, the pentagon, is attacked on an average of 1 every 3 minutes. A hacker is also called a black hat

A cracker is like a hacker only more deviant.

Kiddie scripts are …

Proto-hackers, can penetrate systems and leave messages to prove how smart they are. They aspire to be hackers, but have not yet acquired the necessary skills to get past serious security measures without setting off alarm systems.

Cyber crime is any criminal activity, which uses cyberspace (the internet network) as the communication vehicle to commit a criminal act. With the exponential growth of Internet connection, the opportunities for the exploitation of any weaknesses in ISS are multiplying. Cyber crime may be internal or external. Internal is easier to penetrate. The term has evolved over the past few years since the adoption of Internet connections on a global scale with hundreds of millions of users. Legal systems around the world are scrambling to introduce laws to combat cyber crime.

Techno-crime is a premeditated act against a system(s) with the express intent to copy, steal, prevent access, corrupt, or otherwise deface or damage parts of a computer system. This type of crime is a real possibility from anywhere in the world, leaving few, if any "finger prints". This term is also used to hacker or cracker that breaks into a computer system with the sole intent of defacing and or destroying its contents. They can deploy "sniffers" on the internet to locate soft (insecure) targets and then execute a

range of commands using a variety of protocols. The best weapon against such attacks is a firewall which hide and disguise your agency's presence on the internet.

A virus is a …

A worm is a …

A Trojan horse is a

A time-bombs is …

A stealth-bombs (e.g. malicious code that is disguised as something else. It may be received as a "normal" e-mail, or perhaps as an amusing screen saver. Stealth-bombs deliver their "payload" surreptitiously and the results can be excessive.

A logic-bomb is a …

Social engineering is when

Types of Incidents/ Attacks

- Steal information
- Disclosure of information
- Defacement (e.g. mutilating a web site)
- Change environment (e.g. re-direct printers)
- Destroy and Ruin (e.g. change information, put garbage in information)
- Denial of Service (e.g. break the flow of information, cause excess information "traffic" to tie up all further processing)
- Buffer Overflow (e.g. information is sent to the server at a rate and volume that exceeds the capacity of the systems, causing errors)
- SYN Attack (e.g. connection requests to the server are not properly responded to, causing a delay in connections. These failed connections will eventually time out (true?) but if they occur in volumes, they can deny access to other legitimate requests for access.)
- Teardrop Attack (Large packets of data are spilt into "bite size chunks" with each fragment being identified to the next by an offset marker. Later the fragments are supposed to be reassembled by the receiving system. In the teardrop attack, the

attacker enters a confusing offset value in the second (or later) fragment, which can crash the recipients system. (Is this too technical for this guide?)

- Smurf or Ping Attack (e.g. An illegitimate 'attention request' is sent to a system with the return address being that of the target host (to be attacked). The intermediate system responds to the Ping request but responds to the unsuspecting victim system. If the receipt of such responses becomes excessive, the target system will be unable to distinguish between legitimate and illegitimate traffic.
- Physical Attack (e.g. Cutting the power supply, removing a network cable, and damaging a computer.)

Understanding System Risks and Vulnerabilities

Vulnerabilities are …

Risks are …

What is Disclosure?

Revealing information to the public or media can be disastrous to an organization. The intent of many attackers is to reveal confidential information or disclose information prior to its release.

Disclosure life cycle: Most information has a life cycle. In planning, the longer into the future the information relates to, the higher the cost of disclosure. Plans that will become public tomorrow may not cause the same level of damage as plans covering the next 3 years.

Chapter 2

Security Incidents & Reporting

About Security Incidents

The biggest role you can play in the ISS program is to be in tune to your surroundings so you will notice when something seems unusual. You, the employee, use the system day after day, so are often the one to spot unusual behavior or even incidents in actions.

Security Incidents or security breaches can occur at anytime. Your prompt attention to discovering and reporting any incidents could greatly deter the amount of damage, loss, or disclosure that has taken place.

Suspicions and Incidents

A Suspicion, an unconfirmed assumption of attack, is not yet an Incident. For this reason, it is even more critical to report a suspicion so as to avoid the incident from even happening or greatly decrease any negative results.

It is the responsibility of every employee to do their part in detecting and reporting any possible incidents or suspicions.

> ✌ **Be Alert**
> **You can make a difference by being aware of your environment, noticing unusual activities, safeguarding vulnerabilities, and quickly reporting any incidents.**

Witnessing / Causing an Incident

You could encounter a potential incident, one in process, or one to be carried out, at any time. You could also (intentionally or accidentally) cause an incident.

You, the witness, should react immediately. Do not try to handle it yourself.

Preserving Evidence

If possible, do whatever you can to quickly gather evidence of what you are witnessing. Do not let this task interfere or slow down the reporting process. For example, you may want to write down peculiar system performances, error messages, or …

Gather Evidence … Report it… and Be Prompt!

IMPORTANT: The most important thing to remember is to be PROMPT.

All information security suspicions and incidents must be reported as quickly as possible through your organizations proper internal channels. If problems and violations go unreported, they may lead to much greater losses for the organization than would have been incurred, had the problems been reported right away. Delays in reporting can mean massive additional losses for the organization.

Don't Resolve it Yourself

Not under any circumstances should you, the employee, attempt to prove the existence of potential or current weaknesses, or try to solely resolve suspicions, or incidents, unless you have been specifically assigned this task.

Your Incident Response Team

Your organization has assembled a security response team to handle all suspicions and incidents. You should be aware of who is on the response team and how to contact them. They are:

____

____

____

____

____

Suspicion and Incident Reporting

If you are not sure if something unusual is going on, and it still a suspicion, it is best to report it and have the experts check it out.

IMPORTANT: Reporting a suspicion, can prevent an incident.

Anonymity and Protection

To encourage reporting, your organization may wish to publicize the fact that reports can be made anonymously. Using a voice messaging systems also encourages reporting if you know your will receive an answering machine instead of a person.

If you have reported security issues to your organization in good faith, your organization will protect you if you report what you believe to be a violation of laws or regulations, or conditions that could jeopardize the health or safety of other workers. You will not be terminated, threatened, or discriminated against because you report what you perceive to be a wrongdoing or dangerous situation.

Virus Reporting

Most of us have encountered a computer virus directly or indirectly already. The greatest danger with computer viruses, is that if they go unreported and uncontained, it will continue to spread. Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. You must report a computer virus infestation immediately after it is noticed.

Reporting Types

Internal Reporting

This reporting structure is internal to your organization and includes the following (response team):

- security department
- Help desk
- your manager
- security guard
- information owners
- IS system administrator
- others… ?

You should initially report problems internally rather than externally, reducing any adverse publicity or loss announcements. External reporting should only be done an extreme emergency.

Centralized Reporting

If is sometimes necessary to centralize the ISS department to better control ISS issues. This department may include those not on the response team.

The reporting process can be to a central group such as the Help desk as opposed to line management or a service provider. The reporting process should not always go through management, since this additional step takes longer and is likely to delay corrective actions.

External Reporting

While internal reporting is to be encouraged and required, external reporting is sometimes necessary and includes the following:

- law enforcement, police
- fire department
- FBI
- external auditors

Interfering with Incident Reporting

You should never attempt to interfere with, prevent, obstruct, or dissuade another employee from reporting a suspected information security problem or violation. Any form of retaliation against an individual reporting or investigating information security problems or violations is prohibited.

Not reporting an incident is prohibited. If a report of a known infestation is not promptly made, and if an investigation reveals that you were aware of the infestation, you will be subject to disciplinary action. (?) Some organizations add specific penalties for not reporting problems.

Incident Reporting At-a-Glance

To Report …	Comments	Call … Do …
… an incident in process.		1. Call …
… sensitive information is disclosed, lost, or damaged.		1. Call …
… software/ system malfunction	Do not attempt a recovery yourself.	1. Note (if time) any error messages, unusual system behavior (how is it behaving different than before?) 2. Stop using the computer. 3. Disconnect from any attached networks. 4. Call …
… a virus	Because viruses have become very complex, users must not attempt to eradicate them without expert assistance. If users suspect infection by a virus, they must immediately:	1. Shut-down the involved computer. 2. Disconnect from all networks. 3. Call … ??? (help desk, security, manager?)
… an offensive E-mail, call, etc.		Respond directly to the originator. If the originator does not promptly stop sending offensive messages, report it to ??? (HR?)
… suspicious behavior.		1. Call …
… known systems security vulnerabilities, risks, alerts, and warnings		1. Call …
… equipment damage or loss		1. Call …
… physical access violation		1. Call …

Chapter 3

Access Control Rules

About Access Control

As a user of information systems in your organization, you will be given access to the applications and information you need to do your job. Access Control is the set up and maintenance of system access data that determines who you are, what you can access, what restrictions you have been given, and what tasks you can perform.

Logging On and Off

Before you can access any information systems, you must first identify yourself to the computer via a logon process. Here you will enter your unique User ID that identifies you as the requesting user. You will always need to protect your access rights by supplying a confidential Password along with your User ID. Your Password is strictly confidential. Once you have successfully logged on, you will have access to all the authorities you have been granted in your Access Control authorization(s).

Depending on the configuration used by your organization, you may need to have several User IDs and Passwords to access various applications and data.

Sensitive Data

If your job requires that you use highly confidential or time sensitive information, you will be given a higher access level so you can get to the more sensitive applications and data. If this is the case, you must be even more aware of information security issues and should carefully review all the Rules in this chapter.

Identification

When you initially log on to the system, you will need to enter the User ID given to you. This User ID is a unique identifier that tells the systems that you are requesting access. Any work performed on the system under your User ID is directly traceable back to you. This makes you accountable for all activities performed under your User ID. For this reason, it is important that you do not allow others to perform tasks under your Identification.

Authentication

After you have entered your User ID, you will be required to enter your confidential Password. This allows the system to Authenticate, or prove that it is indeed you requesting access.

Authorization

When you have successfully logged on, that is, identified and authenticated yourself, you will be automatically given access to all the areas that apply to your job requirements. This Access Control procedure is set up when you are hired or change job status. The areas you can access, or privileges you are given are called your Authorization.

Access Control Rules

The ISS Rules pertaining to Access Control are critical to protect information systems by preventing unauthorized access. Since you are responsible for all activity under your Identification, you can play a big part in preventing unauthorized persons from taking access of your User ID or finding out your confidential Password.

The Access Control Rules are grouped accordingly:

- Logging On Rules
- Warning Banners Rules
- Logging Out Rules
- Identification Rules
- Authentication Rules
- Authorization Rules

Logging On Rules

Rule - Unique User ID and Password

You MUST have a unique User ID and a confidential Password to log on. This User ID and Password combination will be required for access to your organizations information systems. *See Password Rules in this chapter.*

Rule - Unsuccessful Logging On

You will be allowed **{3}** failed attempts to try to logon. If you fail all attempts, your User ID may be revoked.

Troubleshooting

Problem: What should I do if … I failed all attempts to log on?
Action: You must call IS to have them manually reset your User ID.

Rule - Limitation on Number of Daily Log Ons

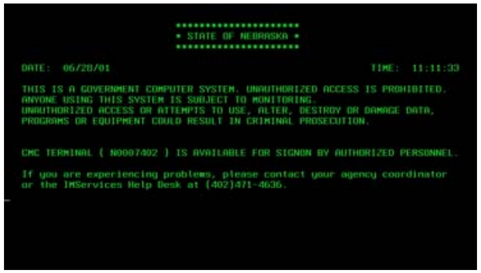
To prevent unauthorized system usage, you are not permitted to log on more than **{10}** times a day. Any User ID that reaches this threshold will be automatically blocked until the next day. If this high usage level continues, the User ID will be subject to immediate cancellation. (Does this apply? It states it is more for customers?)

Warning Banner Rules

A warning banner is a security notice that displays on the screen when you have successfully accessed the system or application requested. This system message is displayed each time you log on to an environment such as Lotus Notes, AS400, CICS, TSO, and such. It can be considered the electronic equivalent of a no trespassing sign.

The warning banner should display:

- that you have accessed a government system or system that may contain government information
- that use is restricted for authorized purposes
- that your activities are subject to monitoring
- that misuse can be reported to security and/ or law enforcement personnel and subject you to criminal and/ or civil penalties (laws, fines, penalties)



```
                    **********************
                    * STATE OF NEBRASKA *
                    **********************

DATE:  06/28/01                                          TIME:  11:11:33

THIS IS A GOVERNMENT COMPUTER SYSTEM. UNAUTHORIZED ACCESS IS PROHIBITED.
ANYONE USING THIS SYSTEM IS SUBJECT TO MONITORING.
UNAUTHORIZED ACCESS OR ATTEMPTS TO USE, ALTER, DESTROY OR DAMAGE DATA,
PROGRAMS OR EQUIPMENT COULD RESULT IN CRIMINAL PROSECUTION.

CMC TERMINAL ( N0007402 ) IS AVAILABLE FOR SIGNON BY AUTHORIZED PERSONNEL.

If you are experiencing problems, please contact your agency coordinator
or the IMServices Help Desk at (402)471-4636.
```

Sample Warning Banner

🕮 Rule - Display a Warning Banner

You must receive a warning banner for each environment you access.

🕮 Rule - Warning Banner Keystroke Monitoring

If your organization requires keystroke monitoring, it must be noted in the warning banner that activity logging is being done.

🕮 Rule - Warning Banner Last Logon

The warning banner should display the date, time and device of the last successful and unsuccessful logon you performed. You should always think back to the last time you used the system and check to see if the time and device are correct.

Logging Off Rules

At end of day, be sure you log out off all systems you accessed that day. If you leave your workstation for an extended amount of time, you should also log off.

🕮 Rule - Automatic Log Off

You will automatically be logged off if there has been no activity on your workstation for **{10}** minutes. Your screen will become blank and your session will be suspended.

Explanation/ Key Points

This Rule is most effective when it applies to all workstations. It could, however, be restricted to users accessing sensitive, critical, or valuable information.

Troubleshooting

Problem: What should I do if … I was automatically logged off?
Action: Re-establishment of the session must take place only after you have provided the proper Password. (Is this true?)

Problem: Will I loose the work I was doing, like a word processing file?
Action: No. After you have supplied the Password, work can resume at the exact place you left it.

🕮 Rule - Leaving Your Workstation - Logging Off / Locking

You must log off / lock when you leave your workstation for an extended amount of time (lunch, breaks, meetings), in the event of an emergency (time permitting), or other instance that would cause you to leave your workstation.

Explanation/ Key Points

Particularly in open offices and cubicles, it is critical that you do not leave your workstation available for others to access your information. Remember: You are responsible for the security of information in your possession.

IMPORTANT: There is no acceptable period during which systems with sensitive or valuable information may be unattended.

Title: General Logging On Rule

Suggested Rule Statement

"You will be required to follow the logon procedures defined by your {organization}".

Policy Category Access Control	**Policy Standard** Authentication	**Rule Number** xx.xx.xx
Rule Date mm/dd/yy	**Rule Revision Date** mm/dd/yy	**Date Adopted ?** mm/dd/yy
Approval Name/ Code ? (signature?) (?)	**Rule Source** acdefg	**Audit Number/ Code (?)** xx.xx.xx

Explanation / Key Points

Step-by-step procedure(s)

Policy Terminology (also goes in master glossary)

Enforcement

Penalty for violation

How is it Enforced

Troubleshooting

Attachments/ Forms (for that Rule)

Related Rule(s)

Identification (User ID) Rules

You will be given a User ID (or sometimes called a Logon ID) to identify who you are to the system. This unique identifier makes you accountable for your activities in the system(s).

With the ever-increasing number of computers and networks found in organizations today, use of several User IDs for the same person is common and getting very complex. You may have multiple User IDs for access to different systems, however, each one still is issued uniquely to you.

Without unique User IDs, you cannot have privileges assigned just for you. If privileges cannot be restricted by user, then it will be very difficult to implement separation of duties, dual control, and other generally accepted security measures.

Many organizations are going to a single sign-on approach giving you one User ID for all environments.

Rule - Unique User ID

You must have a unique User ID that makes you responsible for all activities involving your User ID.

Troubleshooting

Problem: What should I do if … I forgot my User ID?
Action: You must positively identify yourself to IS and they will give it to you.

Rule - Prohibit Group User IDs

You must never use one User ID for group(s) access. This prohibits Identification. Your User ID must be tied to an individual user and must never be generic.

Rule - Sharing your User ID is Prohibited

Your User IDs may not be utilized by anyone but you. You must not allow others to perform any activity with your User ID. Any IS logs will not reflect the true identity of the user.

Troubleshooting

Problem: What should I do if … I'm going on vacation and another user needs to do my job?

Action: As soon as you return from your vacation, change your Password.

Rule - Using another Users ID is Prohibited

You should never perform any activity with another users User IDs.

Troubleshooting

Problem: What should I do if … I have to do another users job?
Action: ??

Rule - Dormant User IDs

Your User ID will automatically have the associated privileges revoked after {30} days of inactivity. If you are a temporary employee, contractor, or consultant, it will be revoked in {15} days.

Troubleshooting

Problem: What should I do if … my User ID has been revoked?
Action: Your User ID will need to be re-activated when you return.

Rule - Forged Messages

You must not sending forged messages under someone else's User ID.

Rule - Internet User ID Expiration

Your User ID on Internet accessible computers must be set to expire {3} months from the time they are established.

Authentication (Password) Rules

After you have been identified by the system, you will then enter a Password to Authenticate that it is indeed you. Here, "Password" could be replaced by other authentication methods like smart cards, PIN (personal identification numbers) numbers, dynamic password tokens, biometrics and other technologies.

Your Password is a string of characters that only you know. Even the IS security administrator should not know your confidential code chosen for your password.

Upon being hired, you will be given a standard or "default" password to initially enter the system. It is important that you change it immediately to your confidential code.

Guessing passwords remains a popular and often successful attack method by which unauthorized persons gain system access. For this reason, we ask that you consider these Rules in choosing and maintaining your Password.

Rule - Changing Your Default Password

You must change your Password when you are initially given the IS default Password. The IS Password should be valid for only your first log on session.

Explanation/ Key Points

You should be forced to change your default Password issued to you by IS. Sometimes this type of Password is called an "expired" or "temporary" Password in that it is valid for only one log on session. Some vendors are now extending this idea to the default passwords that come with their computer or communications products.

Troubleshooting

Problem: What should I do if … I forget my Password?
Action: Call IS and identify yourself so they can to reset your Password.

Rule - Difficult to Guess Passwords

You should choose a Password that is difficult to guess, yet easy to remember.

Explanation/ Key Points

The most frequently encountered problem with security systems is human error, and choosing an easily guessed password is one of the most common security-related mistakes.

IMPORTANT: If a Single Sign-on Password is guessed, an intruder then gains access to many systems.

Rule - Minimum/ maximum Password Length

Your Password must have at least eight **{5}** characters, but no more than **{n}**. Passwords with only a few characters are much easier to guess.

Rule - Cyclical Previous Passwords

When you change your Password, you should make it different each time, not a derivative from your previous one.

Explanation/ Key Points

You should not just partially change your Password just to satisfy an automated process which compares the old and new passwords to make sure that previous passwords are not reused. This security eroding approach is particularly prevalent among users who must log on to many different machines.

Rule - Password Allowable Characters

Your Password allowable characters are {alpha, numeric, special, combination}. Your Password must contain at least one alphabetic and one non-alphabetic character.

Explanation/ Key Points

Non-alphabetic characters include numbers (0-9) and punctuation. This will help you to choose a password that is difficult for unauthorized parties and system penetration software to guess.

Rule - Passwords Lower and Upper Case

Your Password must contain at least one lower case and one upper case alphabetic character.

Explanation/ Key Points

From a mathematical standpoint, the idea behind the use of both upper and lower case characters is to increase the total possible choices, thereby making password guessing more difficult.

For example: “a” is not the same as “A”

Rule - Keeping Your Password Confidential

You should never give your Password to anyone without approval.

Explanation/ Key Points
Passwords should be treated as private and highly confidential. Passwords should never be written down, typed into the system as a reminder or sent via e-mail.

Non-compliance with this policy could result in disciplinary action.

Troubleshooting

Problem: What should I do if …I know someone else has my Password?
Action: Immediately change your Password.

Problem: What do I do if … I’m going to be gone for an extended time and want someone to have my password?
Action: Get the proper approvals and be sure to change your Password as soon as you return.

Problem: What do I do if … someone gives me their password to perform a task?
Action: Make sure they change their Password.

Rule - Reusing Passwords / History

You cannot reuse your Password for **{15}** changes. OR You must not use the same password more than once in a **{12}** month period.

Explanation/ Key Points

You must not construct your Password identically or substantially similar to Passwords that you used previously. You must not recycle your Passwords.

Reuse of Passwords increases the chances that it will be divulged to unauthorized parties and increases the chances that it will be guessed since it is in use for a longer period of time. The security provided by forced password changes is much less effective if you repeat the same Passwords.

IMPORTANT: If you use sensitive data and have a highly access authority, you must NEVER use the same Password twice.

Rule - Display and Printing Passwords

You must never display or print your Password.

Explanation/ Key Points

The display and printing of Passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. When you type your password into a system, it should not be displayed on a monitor or printed on a printer..

If a password were to be displayed, persons nearby could shoulder-surf or look over your shoulder to obtain your password. If a password were to be printed and discarded, persons doing "dumpster-diving" (going through the trash) could recover your password.

Rule - Forced Expiration of Passwords

You will be automatically forced to change your Password every **{90}** days. If you access sensitive data, you will be forced to change your Password every **{30}** days.

Explanation/ Key Points

You will need to change your Password regularly in order to continue working. If a password has fallen into the hands of an unauthorized party, then unauthorized system use could continue for some time in the absence of a forced password change process. The security provided by forced password changes is much less effective if users repeat the same passwords.

Rule - Unsuccessful Passwords Attempts

You will be allowed **{3}** failed attempts to successfully enter your Password.

Explanation/ Key Points

To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. If you fail the number if attempts, your User ID must be either:

(a) suspended until reset by a system administrator
(b) temporarily disabled for no less than three minutes
(c) if dial-up or other external network connections are involved, disconnected.

Troubleshooting

Problem: What should I do if … I failed all attempts to log on?
Action: You must call IS to have them manually reset your Password.

Rule - Same Password on Different Systems

Do not use the same Password on multiple systems if your job requires you to access multiple environments.

Rule - Disclosure Forces Password Change

You must change your Password if you know someone has discovered it or it has been disclosed.

Rule - Writing Passwords Down

Your Passwords should never be written down. Use a password that you are able to commit to memory, so you don't forget it or have to write it down.

Explanation/ Key Points

The moment your Password is committed to a paper or document, discovery of that paper will invalidate other security measures.

With multiple systems and regular changes to Passwords, you may have a lot of Passwords to remember. Therefore, sometimes it is necessary to write it down. Discovering passwords written down and left in the top drawer, taped to a computer monitor, or in some other conspicuous spot is a surprisingly common way for penetration attackers to break into computers. This does not mean that you should never write down your password, only that you must not leave it in a spot where others could see it.

HINT: You could use the "black night" method. With this method, passwords may be taped in a conspicuous spot because they have been altered using some standard approach, such as bump the first letter up the alphabet one letter, bump the second letter down one letter, etc.

Rule – Written Passwords Left Near Devices

You must never write down or otherwise record a readable Password and store it near the access device to which it pertains.

Explanation/ Key Points

For example, you should not leave Passwords and telephone access numbers inside portable computers. PINs needed to initialize dynamic password tokens or smart cards should not be recorded on the devices themselves.

Rule - Proof Of Identify to Obtain a Password

You must appear in person to the IS department to obtain a new or changed Password to positively identify yourself.

Troubleshooting

Problem: What should I do if … I'm working remote and forgot my Password?

Action: Your organization must devise a method of obtaining a positive remote identification. For example, you could use an employee code that only the employee knows, like employee number. The Help desk could create a questionnaire the covers both organization and employee information to positively identify you as an employee.

Title: Choosing Your Password

Suggested Rule Statement

"Passwords can provide reasonably good security, but only if you select them carefully."

Policy Category Access Control	**Policy Standard** Authentication	**Rule Number** xx.xx.xx
Rule Date mm/dd/yy	**Rule Revision Date** mm/dd/yy	**Date Adopted ?** mm/dd/yy
Approval Name/ Code ? (signature?) (?)	**Rule Source** acdefg	**Audit Number/ Code (?)** xx.xx.xx

Explanation / Key Points

Passwords - Good Choices

- Use a password with mixed-case alphabetic characters.
- Use a password with some non-alphabetic characters. i.e. digits or punctuation
- Use the standard English alphabet and numerals
- Join 2 small words with a special character.
- The longer the better. (no maximum limit)

Passwords - Bad Choices

- Do not use derivatives of your User ID (i.e. reversed, capitalized, doubled)
- Do not use common character sequences such as "123456"
- Do not use personal details such as your name, family member's name, pet's name, automobile license plate, social security number, address.
- Don't use a word (alone) contained in the dictionary (English or foreign language), spelling lists, or other lists of words.
- Do not use proper names, geographical locations, and common acronyms.
- Don't use important dates in your life - you and your family birthday , anniversary, hire date, etc.
- Do not use repeating characters or all digits or letters. This significantly reduces the amount of search time for a hacker.

Syntax Suggestions:

Good choice: A mix of alpha and numeric characters.

Ex: A3NY8T

Better choice: A mix of alpha and numeric characters – more characters.

Ex. Z9W34B2F

Best choice: A mix of case sensitive alpha and numeric characters - more characters.

Ex. Z9w34B2f

Do not use: Jackie1
KatherineS
123456

Step-by-step procedure(s)

Policy Terminology (also goes in master glossary)

Enforcement

Penalty for violation

How is it Enforced

Troubleshooting

Attachments/ Forms (for that Rule)

Related Rule(s)

Authorization (Privileges) Rules

Your Authorization privileges are set up by IS according to your specific task requirements and what information or programs you need to access.

Once you have successfully logged on, you will have access to all the Authorities to which you have been granted by your User ID.

Rule - Authorized Privileges

You can only view, modify, print, transport, and mail information you have been authorized to access.

Chapter 4
Network Security Rules

About Network Security

Most organizations today process their business applications on or via a network. This network system may be internal or connected to an external communication environment. Organizations may have several networks, several mainframes and other peripheral computer systems that require a sophisticated configuration to connect it all together.

It is important that you, the employee, understand the important of protecting the information on your network(s) in your organization. You play a large part in keeping the network safe from intruders, virus free and in good working order.

Remote Access

With the introduction of the laptop computers, E-mail messaging, fax machines, and the Internet, it became less necessary for employee to report to an office. Many employees and contractors today work via telecommuting, that is, from a remote location. This maybe due to logistics, business travel, having remote branches, or many other business purposes that best serve the function by having a portable office.

In addition to the precautions and safeguards we can all do to protect our network, we also need to be aware of connections with outside parties, over whose network environment you have no control. This openness of the Internet is making organizations more vulnerable than years ago.

Network Security Rules

The ISS Rules pertaining to Network Security are critical to protect information systems on your network(s).

The Network Security Rules are grouped accordingly:

Network Access Rules

Rule - Approval for Connections

You must not connect any devices to the state network, internal network, or any other equipment with a modem or communication system without prior approvals.

Explanation/ Key Points

You may be putting your organizations information in jeopardy if you create entry points in your own communication systems. You could create vulnerabilities that you are unaware of by bypassing the proper controls.

Rule - Gaining Unauthorized Access

You are not permitted to gain unauthorized access to any information systems on your network or connected to the network.

Explanation/ Key Points

You should not in any way damage, alter, or disrupt the operations of information systems with unauthorized access. You are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism, which could permit you to have unauthorized access.

Rule - LAN Backups

If you have a local area network (LAN) connection, you must leave your computers turned on at night so that an automatic backup can be performed. (?)

Rule - Network Browsing Prohibited

You must not browse through your computer systems or networks searching for interesting files and/or programs. Steps taken to legitimately locate information needed to perform one's job is not considered browsing

Rule - Backup Notification

To prevent accidental loss, all files and messages stored on your organizations systems are routinely copied to tape, disk, and other storage media. This means that information stored on your organizations systems -- even if you specifically deleted it -- is recoverable and may be examined at a later date by systems administrators and management.

Rule - Altering Computer Equipment

You cannot expand or alter computers supplied by your organization. This includes upgraded processors, expanded memory, extra circuit boards, and such, without proper approval and authorization.

Rule - Overwhelming the Network

You must not send an overwhelming number of files across the network to cause interruption of processing. This is called denial of service attack, spamming or E-mail bombing.

Rule - Malicious Intent and the Network

You are prohibited from any form of malicious or disruptive use, including use of the organizations own resources, or any attached network in a manner that precludes or significantly hampers its use. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses, and use of the organization owned resources to make unauthorized entry to any other machine accessible via the network facilities.

Modem Rules

Rule - Modems Connections to Internal Networks Prohibited

You are prohibited from connecting dial-up modems to workstations, which are simultaneously connected to a local area network (LAN) or another internal communication network unless approved.

Explanation/ Key Points

This could establish a weak link in a system of network access controls.

Rule - Prohibit Modems in AutoAnswer Mode

You must not leave your approved modem connected to personal computers in autoanswer mode, such that it is able to receive in-coming dial-up calls. Be sure to turn off your modem at end of day.

Remote Access Rules

Rule - Dial-up Password Attempts

The maximum permissible Password attempts for dial-up access is {3}. If you have not provided a correct password after three consecutive attempts, the connection must be immediately terminated.

Troubleshooting

Problem: What should I do if … I failed all attempts to dial in?
Action: You must call IS to have them manually reset your password. (even for dial -in?)

Rule - Remote Access Training

You must complete an approved remote systems access training course prior to being granted privileges to use dial-up, Internet, or any other remote access data communications system.

Remote Sites Rules

Rule - Telecommuting Permissible Equipment

If you are working on business at alternative work sites, you must use computer and network equipment provided by your organization. An exception will be made only if other equipment has been approved as compatible with your organization information systems and controls.

Rule - Protections of Off-Site Property

The security of your organizations property at an alternative work site is just as important as it is at the central office. At alternative work sites, reasonable precautions must be taken to protect hardware, software, and information from theft, damage, and misuse.

You must also not alter the configuration of hardware and software without prior approval.

Rule - Information to be Returned

You must return all property and information created in your portable computer provided by your organization. You may be given a portable computer so you can perform your job at remote locations including hotel rooms and personal residences.

Rule - Remote Working Environment

If you are a telecommuter, to retain the privilege of doing off-site work, you must structure your remote working environment so that it is in compliance with your organizations policies and standards.

Rule - Security at Home / Off-site

If you work at home (telecommuting) or any alternative work site (i.e. hotel), consideration should include physical and information security for your organizations property.

Explanation/ Key Points

When required, you must abide by all remote system security policies, rules and procedures. This includes compliance with software license agreements, performance of regular backups, and use of shredders to dispose of sensitive information.

Rule - Right to Conduct Inspections of Telecommute Office

Your organization maintains the right to conduct inspections of your telecommuter offices with {1} day advance notice. The information stored in your portable computer belongs to your organization and they can inspect or use the information in any manner, and at any time.

Rule - Sensitive Information on Portable Computers

If you are in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing sensitive information, you must not leave these computers unattended at any time unless the information has been encrypted.

Rule - Backing up Portables Computers

You must make periodic backups of all critical information and store it away from the portable device. These backups should be performed every {1} day. They should be stored elsewhere than the portable computer's carrying case.

Rule - Transportable Computers Hand Luggage on Airplanes

If you are in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing sensitive information, you must not check these computers in airline luggage systems. These computers must remain in your possession as hand luggage.

Explanation/ Key Points

The primary reason to not check your computer as baggage is to avoid theft or loss.

Rule - Portable Computer Security

You must keep your portable computers (i.e. laptop) in your possession at all times, or locked in a secure location (i.e. hotel safe). You must do your part to protect your equipment and information against theft, destruction, and loss.

This page is intentionally left blank for pagination of double-sided printing. ⌨

Chapter 5

Individual Use/ E-mail, Internet, and E-commerce Rules

About Internet and E-mail

The use of the Internet and E-mail has become an important critical function for many organizations. The key concern with ISS and the cyber world is the connections and communications required accessing it. This is a high-risk security area that without proper safeguards can leave the door open to intruders to access your organizations information.

In addition to security concerns, proper use of the Internet and E-mail is the responsibility of every employee. Improper use can detract from performance of duties and subject your organization to potential legal action. Careless use can subject you and other users to malicious software attacks.

Your IS department should implement a secure and managed environment for you to effectively and safely use the Internet and E-mail to accomplish your jobs tasks. It is your responsibility to uphold the Rules of proper usage.

Internet and E-mail Rules

The ISS Rules pertaining to Individual Use/ Internet and E-mail are critical to protect information systems by …

The Internet and E-mail Rules are grouped accordingly:

E-mail Rules
Internet Rules
E-Commerce Rules

E-mail Rules

All authorized employees will be provided with an appropriate E-mail system upon proper authentication to easily exchange business-related information in a secure and managed manner.

Rule - E-mail Virus Protection Software

Your organization will use virus protection software on your workstation to prevent transmission of viruses in e-mail attachments and diskettes.

Explanation/ Key Points

A lack of user awareness about the risks of opening unsolicited E-mails may result in a virus infection spreading throughout the organization.

IMPORTANT: It is critical that you keep your anti-virus software and definitions (library of virus profiles) current with frequently updates / downloads.

Rule - E-mail for Business Purposes Only

You should use E-mail for business purposes only.

Rule - E-mail and Confidential Information

E-mail that is not secure or encrypted (non-readable) should not be used to send Highly Restricted or Confidential information.

Explanation/ Key Points

Highly Restricted or Confidential information may not be sent over an E-mail system unless it is encrypted at the source and decrypted at the destination. (?)

Rule - Forwarding E-mail

You must not forward electronic mail to any address outside your organizations network unless the information owner/originator agrees in advance, or unless the information is clearly public in nature.

Rule - Blanket Forwarding E-mail

Blanket (global) forwarding of electronic mail messages to any outside address is prohibited without written permission from the appropriate security resource.

🕮 Rule - Forwarding External E-mails

You must not create your own, or forward externally provided electronic mail messages which may be considered to be harassment or which may contribute to a hostile work environment. Among other things, a hostile work environment is created when derogatory comments about a certain sex, race, religion, or sexual preference are circulated.

🕮 Rule - Forwarding E-mail to Archival Records

All official organizational E-mail messages, including those containing a formal management approval, authorization, delegation, or handing over of responsibility, or similar transaction, must be copied to the Records Management division or use a special archival account set up by your organization.

🕮 Rule - E-mail Retention

You can erase most E-mail messages after receipt. The only exception to this is if the E-mail message contains information required for future use.

🕮 Rule - Certainty of E-mail File Attachments Origin

You must be certain of the original of any file attachments you receive through E-mail. This is critical to protect your workstation and others against malicious software.

🕮 Rule - Using another Users E-mail Account

You must not use an E-mail account assigned to another individual to either send or receive messages.

Troubleshooting

Problem:	What should I do if … I need to read another users E-mail messages while they are away on vacation?
Action:	Use message forwarding or use your mail delegation features of your e-mail system ?

🕮 Rule - Using E-mail as a Database

You must regularly move important information from E-mail message files to word processing documents, databases, and other files. E-mail systems are not intended for the archival storage of important information. Stored electronic

mail messages may be periodically expunged by IS systems administrators, mistakenly erased by users, and otherwise lost when system problems occur.

🕮 Rule - Deleting and Destroying E-mail

Internal correspondence must be disposed of when no longer needed.

Explanation/ Key Points

E-mail messages relevant to current activities, or that are expected to become relevant to current activities, should be saved as separate files and retained as long as needed.

IMPORTANT: Be aware of local rules, regulations, or pending legal actions that may restrict the deleting of your E-mail messages.

🕮 Rule - Privacy and E-mail

You must treat E-mail messages and files as private information. E-mail must be handled as a private and direct communication between the sender and the recipient.

🕮 Rule - E-mail is Public Communication

You should treat E-mail as public communications. Consider E-mail to be the electronic equivalent of a postcard. Unless the material is encrypted, you must refrain from sending credit card numbers, passwords, research and development information, and other sensitive data via E-mail.

🕮 Rule - E-mail as a Public Record (government)

Be aware of and follow local rules and regulations that define some or all E-mails as public records. Also observe rules governing archiving and deleting as well.

🕮 Rule - E-mail Profanity

You must not use profane, obscene or derogatory remarks in E-mail messages.

Explanation/ Key Points

Such remarks, even when made in jest, may create legal problems such as trade libel and defamation of character. Special caution is warranted because backup and archival copies of electronic mail may actually be more permanent and more readily accessed than traditional paper communications.

Rule - Responding to Junk (SPAM) E-mail

When you receive unwanted and unsolicited E-mail (also known as SPAM), you must refrain from responding directly to the sender unless you can “unsubscribe” thus sending out a “do not send” mail message.

Troubleshooting

Problem: What should I do if … I need to read another users E-mail messages while they are away on vacation?

Action: You should forward the message to the IS E-mail administrator who will take steps to prevent further transmissions.

Rule - Ownership of E-mail Messages and Attachments

All messages sent by E-mail are owned by your organization. Your organization reserves the right to access and disclose all messages sent over its E- mail system, for any purpose.

Rule - Disclosure of E-mail Messages and Attachments

Your organization management may review your E-mail communications to determine whether they have breached security, violated company policy, or taken other unauthorized actions. Your organization management may also disclose the contents of E-mail messages to law enforcement officials without prior notice to the your or whoever may have sent or received the message.

Rule - Authorization to Issue Broadcasts in E-mail

You must get the proper authorization to issue broadcasts through E-mail.

Rule - Scanned Signatures in E-mail

You must not use scanned versions of hand-rendered signatures to give the impression that an E-mail message or other electronic communications were signed by the sender.

Rule - Misrepresentation of identity in E-mail

Misrepresenting, obscuring, suppressing, or replacing your identity on an E-mail communications system is forbidden. Your name, E-mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.

Internet Rules

All authorized state employees will be provided with an appropriate Internet system.

Rule - Downloading Internet Files and Information

When you download software and files from the Internet, they must be screened with virus detection software. This screening must take place prior to being run or examined via another program such as a word processing package. Internet access should only be permitted from stand-alone personal computers. (?) All files down-loaded from the Internet must be checked with an authorized virus detection package prior to being moved to any other computer.

Rule - Sending Sensitive Information Over the Internet

Your organizations Highly Restricted and Confidential information must never be sent over the Internet unless it has first been encrypted by approved methods. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

Rule - Reliability of Downloaded Information Over the Internet

All information taken off the Internet should be considered suspect until confirmed by another source. There is no quality control process on the Internet, and a considerable amount of Internet information is outdated, inaccurate, or deliberately misleading.

Rule - Uploading via the Internet

You must not upload software, which has been licensed from a third party, or software, which has been developed by your organization Company X, to any computer via the Internet unless authorization from the user's department manager has first been obtained.

Rule - Using the Internet for Personal Use

You should use the Internet for business purposes only. If you use the Internet for personal use, it must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not potentially embarrass or harm your organization.

IMPORTANT: Be aware that firewalls can create a detailed audit log reflecting transmissions, both in-bound and out-bound.

Rule - Using Internet Search Engines

You must …

Rule - Filtering Inappropriate Internet Information

You must …

Rule - Using the Internet in an Acceptable Way

You must …

Rule - Using Copyrighted Information from the Internet

You must …

Rule - Approval for Internet Connections

You must not establish Internet or any other external network connections, which could allow non-organization users to gain, access to your organizations information. These connections include the establishment of multi-computer file systems (like Sun's NIS), Internet home pages, Internet FTP servers, and such.

Rule - Training for Internet Use

You must complete an approved ISS Internet and E-mail training course prior to being granted privileges to use dial-up, Internet, or any other remote access data communications system.

Rule - Internet User ID Expiration

Your User ID on Internet accessible computers must be set to expire {3} months from the time they are established.

Rule - Personal Messages Disclaimer on Internet

If you post a message to an Internet discussion group, an electronic bulletin board, or another public information system, this message must be accompanied by words clearly indicating that the comments do not necessarily represent the position of your organization.

Explanation/ Key Points

Such statements are required even when your organizations name does not appear in the text of the message and/or when an affiliation with your organization has not been explicitly stated.

When engaged in discussion groups, chat rooms, and other Internet offerings, only those individuals authorized by management to provide official support for your organizations products and services may indicate their affiliation with your organization.

Example: If you disclose an affiliation with your organization, you must clearly indicate that "the opinions expressed are my own, and not necessarily those of my employer."

Rule - Internet Products and Services

You must not advertise, promote, present, or otherwise make statements about your organizations products and services in Internet forums such as mailing lists, news groups, or chat sessions.

Rule - Disclosure of Personal Information on the Internet

For your own personal protection, you should never disclose your real name, addresses, or telephone numbers on electronic bulletin boards, chat rooms, or other public forums reached by the Internet.

Rule - Public Area of Your Organizations Web Site

If you submit information to the public area on your organizations web site or electronic bulletin board system (BBS), you grant to you organization the right to edit, copy, republish, and distribute such information.

Rule - Unofficial Web Pages on the Internet

You cannot create or implement unofficial web pages dealing with your organizations products or services. If you notice a new Internet reference to your organizations products and/or services, you should promptly notify (? the Director of Public Relations, Marketing?)

Rule - Concealing your Identity on Internet is Prohibited

When using your organizations information systems, or when conducting your organizations (Company ABC) business, you must not deliberately conceal or misrepresent your identity. This includes participating in discussion groups and chat rooms, as well as establishing accounts on other computers.

Rule - Exchanges of Information on the Internet

Your organizations software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-organization party for any purposes other than the business purposes and only with the proper authorization.

Rule - Updating Organization Information on the Internet

If you are connected to your organizations systems via the Internet, you are not permitted to directly modify any organization information.

E-commerce Rules

Rule - Giving Information when Ordering Internet Products

Rule - E-transactions

If transactions are sent and processed automatically (via Electronic Data Interchange for instance), then a message must not be accepted or acted on unless: (a) the message has been shown to match a trading profile for the initiating organization, or (b) the message has been shown to deviate from a trading profile but additional steps have been taken to verify the accuracy and authenticity of the message.

Rule - Forming E-contracts

Unless specifically authorized to enter into contracts on behalf of your organization, or otherwise authorized to legally represent your organization, you must never respond to an E-mail message that binds your organization to any contract, position, or course of action.

Rule - Validating Identity of External Parties on Internet

It is relatively easy to spoof the identity of another user on public networks such as the Internet. Before you release any internal organization information, enter into any contracts, or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed.

Explanation/ Key Points

Identity confirmation is ideally performed via digital certificates, but in cases where these are not yet available, other means such as letters of credit, third party references, and telephone conversations may be used.

Rule - Electronic Offers

All contracts formed through electronic offer and acceptance messages (fax, Electronic Data Interchange, E-mail, etc.) must be formalized and confirmed via paper documents within **{2}** weeks of acceptance.

Rule - Internet Customers

All customers (?) using the Internet to place orders with your organization must be presented with a summary of your organization important terms & conditions, and in order to complete their orders, they must specifically indicate that they agree to be bound by these terms & conditions.

This page is intentionally left blank for pagination of double-sided printing. ⌨

Chapter 6

Individual Use/ Copyright Rules

About Copyright Information

Courts have found organizations and their officers liable for copyright infringement where unauthorized copies were used to the organizations benefit -- even when the copying of software or other copyrighted material was done without management's knowledge.

You must comply with copyright laws. Agencies and institutions must train/ communicate this policy to users. Agencies shall designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

Copyright Rules

Copyright Rules

Copyright Rules

Rule - Copyright Laws for Software and Paper

You must comply with copyright laws for software and written materials.

Rule - Copyrighted Inquiries

You organization shall designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

Rule - Copying Copyright Materials

You may not copy documents or software protected by copyright without the written permission of the copyright holder. Any unauthorized reproduction of the copyrighted material may subject you to disciplinary action, civil liability, or both.

Rule - Protection of Software and Copyrighted Materials

The organization is not obligated to defend or indemnify employees in actions based on copyright violation.

Rule - Copyright Enforcement Statement

"According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $100,000, and criminal penalties, including fines and imprisonment. If you make, acquire or use unauthorized copies of computer software, you shall be disciplined as appropriate under the circumstances. Such discipline may include termination. Your organization does not condone the illegal duplication of software."

Rule - Making Excess Copies Prohibited

You must not make more copies of licensed software than are allowed.

Rule - Copying Vendor Software

You must never copy (called bootlegging) unlicensed software that has not been properly licensed by your organization with the vendor. If you copy software, you are doing so on your own behalf, since all such copying is strictly forbidden by your organization. You organization allows reproduction of copyrighted material only to the extent that it is legally considered "fair use" or with the permission of either the author or publisher.

Rule - Sending Copyrighted Information Electronically

You must never send your organizations copyright materials through E-mail or via the Internet without proper approvals, encryption methods, and safeguards being put in place.

Rule - Violation of Copyright Laws

You must not violate the legal protection provided by copyright and licensing laws applied to programs and data.

Explanation/ Key Points

It is assumed that information and resources available via your network or state-owned resources are private to those individuals and organizations owning or holding rights to such information and resources, unless specifically stated otherwise by the owners or holders, or unless such information and resources clearly fall within the statutory definition of a public record. It is unacceptable for you to use the state-owned resources to gain access to information or resources not considered a public record without the granting of permission to do so by the owners or holders of rights to such information or resources.

Rule - Using Copyrighted Information from the Internet Rule

Much of the material on the Internet is copyrighted or otherwise protected by intellectual property law (for instance by license agreement). If you must use Internet information for your business, be sure you have followed the proper copyright laws.

Rule - Ownership of Copyrighted Materials

While an employee of your organization, you grant to your organization exclusive rights to patents, copyrights, inventions, or other intellectual property you originate and/or develop for them.

This page is intentionally left blank for pagination of double-sided printing. ⌨

Chapter 7

Individual Use/ Acceptable Use Rules

About Acceptable Use

This chapter is focused on you, the employee. Your organization has Rules governing the use of computer and communication facilities by individuals. Like all communications conducted on behalf of the State of Nebraska, you must exercise good judgement in your daily business practices.

Acceptable Use Rules

Acceptable Use (of systems) Rules

Rule - Storing Games on your Computer

You may not store or use games on your organizations computer systems or state owned resources.

Rule - Personal Use of your Computer

The computer you are given by your organization to do your job must be used for business purposes only.

Explanation/ Key Points

Incidental personal use is permissible if the use does not interfere with your job functions.

Rule - Other Business Activities

As a user of your organizations computing and communications services, you must not use these facilities for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by your organization.

Rule - Using State-Owned Resources Unrelated to Business

You must not use the state-owned resources for fund-raising or public relations activities unrelated to an your employment by the State of Nebraska. You must not use state-owned resources in conjunction with for-profit or activities, unless such activities are stated as a specifically acceptable use. You must not use the state-owned resources for unsolicited advertising, unless authorized by the governing body of the organization.

Rule - Using State-Owned Resources in an Acceptable Way

You must use state-owned resources as consistent with laws, regulations or accepted community standards. Transmission of material in violation of any local, state or federal law or regulation is prohibited. It is not acceptable to transmit or knowingly receive threatening, obscene or harassing material.

Rule - Misrepresentation on State-Owned Resources

You must not represent yourself, an agency, or the State of Nebraska when using the state-owned resources.

Rule - Using Others Users Data on the State-Owned Resources

You cannot access or attempt to access another individual's data or information without proper authorization.

Rule - Preventing Services to Others

You must not prevent others from accessing services they are entitled to in your organization.

Rule - Using State Resources in an Acceptable Way

You must not use state resources that you are not authorized to be using. You must not use state resources for unauthorized or illegal purposes.

Rule - Giving Information to a Third Party

You must not sell or transfer your organizations software, documentation, and all other types of internal information to any outsider (third party) for any purposes, unless authorized to do so. You must not disclose co-worker information to a third party unless required by law, or unless permitted by clear and explicit consent of the subject.

Explanation/ Key Points

If you have the proper authority and disclose information to a third party, you must keep records of all such disclosures including specifically what information was disclosed, to whom it was disclosed, and the date of such disclosure. These records must be maintained for at least {5} years.

Rule - Handling Third Party Confidential Information

If you handle sensitive information entrusted to your organization by a third party, you must protect it as though it was your own organizations sensitive information.

Explanation/ Key Points

NOTE: If an outside agent, employee, consultant, or contractor is to receive sensitive information from a third party on behalf of your organization, this disclosure must be preceded by the third party's signature approval or release form.

Rule - Other Business Activities

479. Signing Third Party Confidentiality Agreements Without Approval. Rule: Workers must not sign confidentiality agreements provided by third parties without the advance authorization of Company X legal counsel designated to handle intellectual property matters.

Rule - Exposure of Sensitive information Public Places

You must not be read, discuss, or otherwise exposed on airplanes, restaurants, public transportation, or in other public places any organization sensitive information.

Rule - Time Sensitive Information

You must not handle time sensitive information by E-mail, voice mail, telephone calls, or other computerized systems until the specifics have been publicly announced.

Explanation/ Key Points

This includes organization issues, like mergers and acquisitions, up-coming layoffs, and such.

Rule - Sensitive Disclosure Statement

All disclosures of Highly Restricted, or Confidential information to third parties must be accompanied by an explicit statement describing exactly what information is restricted and how this information may and may not be used. (?)

Other Employees/ Organization Rules

Rule - Disclosing Co-worker(s) Contact Information

You must not disclose the names, titles, phone numbers, locations, or other contact particulars of your co-workers unless required for business purposes.

Rule - Disclosing Co-worker(s) Change in Status Information

You must not disclose the change of status of any co-worker. This includes: reason for terminations, retirement, resignation, leave of absence, leave of absence pending the results of an investigation, inter-departmental transfer, relocation, and changes to consultant/contractor status.

Explanation/ Key Points

Exceptions will be made when law requires such a disclosure or when the involved persons have previously clearly consented to the disclosure.

Rule - Personal Identifiers Prohibited

Any co-worker identifier, such as name or social security numbers, must not appear in any publicly accessible location managed by or controlled by your organization. This includes web pages, Internet commerce sites, product manuals, and magazine advertisements.

Rule - Disclosing Organization Information

You must not disclose organization information to outsiders or internal departments, which do not require this information to do their jobs.

Explanation/ Key Points

This includes business plans, marketing strategies, new products, budgets and financial standings, executive meeting results, trade secrets, research results, corporate strategies, customer information, and any sensitive data or information that could harm, interrupt, or embarrass the organization.

Rule - Disclosing Organization Secured Areas

You should never disclose the location of your organizations computer center, cash holding area, or other secured building, floor, or special room. The physical address should be confidential and must not be disclosed to those without a demonstrable need-to-know.

Rule - Disclosing Organization Future Plans Prohibited

You are forbidden from making any public representations about your organizations future earnings or the prospects for new products.

NOTE: This can avoid shareholder class-action lawsuits.

Rule - Sensitive Information and Meetings

If sensitive information is to be discussed orally in a meeting, seminar, lecture, or related presentation, the speaker must clearly communicate the sensitivity of the information. The speaker must also remind the audience to use discretion when disclosing it to others. Visual aids such as slides and overhead transparencies must include the appropriate confidentiality markings.

Explanation/ Key Points

Persons other than those specifically invited must not attend meetings where sensitive information will be discussed.

Rule - Sensitive Information and Meeting Rooms

You must erase black boards and white boards in conference rooms after meetings.

Explanation/ Key Points

When sensitive information has been recorded on black boards or white boards, it must be erased (with water or special cleaning fluids) before you leave the area.

Rule - Employee Health and Safety Disclosure

Your organization must fully disclose to you, the results of toxic substance tests and other information relating to the health and safety of workers.

Rule - Organizations Documentation

You must not take your organizations computer related documentation off-site or out of a secured area without proper permission.

Public Records/ Privacy (of citizens) Rules

Public records can also be private. If the information is a public record, yet you are not identified as the individual associated with the information, then it is considered to be private. However, if you are identified uniquely, such as by name, address, social security number, and such, then there is no longer privacy.

Rule - Privacy of Citizens

You must not … the privacy of citizens. This information can be soft or hard copy.

Rule - Managing Public Records

(Assign responsibility for efficient and economic management of public records?)

Rule - Privacy and E-mail

You must treat E-mail messages and files as private information. E-mail must be handled as a private and direct communication between a sender and a recipient.

Rule - Violating Others Privacy

You must not violate the privacy of other users and their data. For example, you shall not intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users, or represent themselves as another user unless explicitly authorized to do so by that user.

Rule - Public Records

Public records need to be accessed, yet protected against corruption, and loss.

Rule - Personal Identification Information (PII)

(??)

Rule - Consent to Disclose Information to Law Enforcement

You must consent to allow all information your use and store on your organizations systems to be divulged to law enforcement at the discretion of your organizations management.

However, you must not allow police or other law enforcement to have access to your organizations information without a properly executed search warrant.

Rule - Collecting Private Information

You must not collect private information (race, religion, political opinions, sexual orientation, etc.) unless the collection effort has been approved in advance by your organization.

Rule - Children's Privacy

You cannot gather personal information about children without first obtaining clear and unambiguous consent from the involved parents or guardians.

Rule - Customers Privacy

You must only access customer information on a need-to-know basis and the information must be used only for internal business purposes. The collection of personal information about potential customers and others with whom your organization does business is customary and expected.

Explanation/ Key Points

Unless the clear and unambiguous consent of the party described by the information is first obtained, all third party sale, exchange, or other distribution is prohibited.

If you must get customers information (i.e. via a subpoena), the customer will be given **{2}** weeks advance notice prior to the release to provide the information.

NOTE: You should never discuss customers private information in public places such as in building lobbies or on public transportation. This applies even when the identity of the customer is kept confidential.

All identifying information about customers such as credit card numbers, credit references, and social security numbers, must be accessible only to those personnel who need such access in order to perform their jobs.

Rule - Customers Disclosure

You must not disclose information about your customers identity to third parties without proper permission from the customer.

Explanation/ Key Points

If given the proper approvals by the customer, you can provide the customer with the disclosure information, like contact names, telephone numbers and addresses of the third parties.

Rule - Explanation for Private Information

If you are requested to provide private information for business purposes, the full and complete reasons for collecting this information must be disclosed.

Explanation/ Key Points

You should report any refusal from any entity to provide private information if you have provided the proper identification and gathering reason.

Rule - Disclosure Notification / Blocking Privacy Request

The subject (citizen, customers, employee, etc.) must be given advance notice that their personal data held by your organization has been requested by a third party.

Explanation/ Key Points

Unless compelled to release the data by clear and authoritative law or regulation, a reasonable period of **{2}** weeks must be provided for the subject to block this disclosure. No response from the subject can within that period can be considered to be acquiescence to the disclosure.

Rule - Public Records Source Owner

Information generated by your organization and released to the public must be accompanied by the name of a designated staff member (?) acting as the single recognized official source and point-of-contact. All updates and corrections to this information that are released to the public must flow through this official source.

Rule - Materials Released to the Public

All information to be released to the public must have first have been reviewed and approved.

Explanation/ Key Points

Every speech, presentation, technical paper, book, or other communication to be delivered to the public must first have been approved for release by the proper authorities.

Paper Information Rules

Rule - Copying Sensitive Information

You must not photocopy or reprint sensitive information without proper authorization from the information Owner.

Explanation/ Key Points

If additional copies of sensitive information are required, it must be recorded to include: number of copies, and recipients. Each of the recipients must be informed that distribution or copying is forbidden.

HINT: You may want to number the copies of confidential documents individually with a sequence number to ensure that the persons responsible for the documents and the location of the documents can both be readily tracked.

Rule - Copying Sensitive Information and Special Paper

If you are releasing sensitive information to a third party, it can be distributed on special paper that cannot be copied using ordinary photocopy machines.

You may also want to print sensitive information on special paper that will clearly show whether it is an original or a copy. This can achieved with color borders, watermarks, or other technology approved for such use.

Rule - Copier / Printer Malfunction

If you are making copies of sensitive information and the copy machine jams or malfunctions, you must not leave the copy machine / printer until all copies have been removed from the machine or are destroyed beyond recognition.

Rule - Waste Copies

All waste copies of sensitive information that are generated in the course of copying, printing, or otherwise handling such information must be destroyed according to approved procedures.

Rule - Attending to Printers

You must not leave the printers unattended if sensitive information is being printed or will soon be printed. You must be authorized to examine the information being printed.

Rule - Sensitive Information – Page Numbering

All sensitive organization information in paper form must indicate both the current and the last page. (?)

For example: "page 6 of 51”

Rule - Third Party Copying Sensitive Information

Prior to sending any sensitive information to a third party for copying, printing, formatting, or other handling, the third party must sign an organization non-disclosure agreement. (?)

Rule - Mailing Envelopes for Sensitive Information

If you are handling sensitive information by internal mail, external mail, or courier, it must be double wrapped.

Explanation/ Key Points

The outside envelope or container must plain and not indicate the sensitivity of the contents contained therein.

The inside sealed envelope or container should be opaque and must be labeled Highly Restricted”, “Confidential” or "To Be Opened by Addressee Only”. (Is that safe?)

Rule - Tracking Mailed Sensitive Information

If you mail / deliver sensitive information, you must be able to track the information. For example, most couriers, UPS, Federal Express, and such offer a tracking process with a weigh bill number. It should always be marked for the recipient "signature required."

Rule - Delivery of Sensitive Information

If you are responsible for delivering sensitive information, you must never leave it at an unattended desk, or left out in the open in an unoccupied office.

Even if you have given the information to a receptionist/ guard, it is recommended that you contact the intended recipient to acknowledgement receipt of the information.

Rule - Filing Sensitive Information

If you handle sensitive information in hard copy, you must file it in a locked file cabinets, closets, or desk drawer.

Rule - Destroying Unwanted Hard Copies

If you need to discard unwanted hard copies of information, you need to shred it before it is thrown away.

Using Software and Data Rules

Rule - Downloading Software

You must not download software from electronic bulletin board systems, the Internet, or any other systems outside you organization. You must not use any externally provided software from a person or organization other than a known and trusted supplier. This is for protection against malicious software such as viruses, worms, Trojan horses, and other software which may damage your organizations information and systems.

You also must not download software that is in violation of license agreements.

Rule - Protecting Software / Handling a Virus

Because viruses have become very complex, you must not attempt to eradicate it yourself if you have encountered a Suspicion or Incident.

If you suspect a virus, call the appropriate authorities immediately. *See Incident Reporting.*

Rule - Malicious Intent is Prohibited

You must not intentionally develop programs that harass other users or infiltrate a computer system or damage or alter software components.

You are also prohibited from running or writing any computer program that can consume significant system resources or otherwise interfere with your organizations business activities.

You must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any of your organizations computer, network, or information.

Rule - Retaining Data

You must retain all financial accounting, tax accounting, and legal records for a period of at least {7} years. All other records must be retained for a period of at least {5} years.

Rule - Input Data Retention

Business source documents containing input data must be retained for at least {90} days beyond the date when this information was entered into your organizations computer system(s).

Rule - Copying Software

You must not copy software provided by your organization to any storage media (floppy disk, magnetic tape, etc.), transfer such software to another computer, or disclose such software to outside parties.

Rule - Purchasing and Installing New / Upgraded Software

You must not install newly purchased software on you office PC, network servers, or other machines without first getting the proper approvals for set up and security.

Using File and Directory Rules

Rule - Others User Directories

You must never go into the directories of other users.

Rule - Unauthorized Access Prohibited

You should never have unauthorized access to software, data, or files even if your organization has not properly secured and protected them.

Rule - Receiving Information on Disks

You should never …

Rule - Setting up new Folder/ Directories

You should never …

Rule - Amending Directory Structures

You should never …

Rule - Using Meaningful File Names

You should never …

Telephone, Faxes and Other Devices Rules

Rule - Telephone Disclosures

You must not disclose organization, customer, or other information by phone, unless the caller is positively identified and is authorized to have this information.

IMPORTANT: Be especially careful when using speaker phones to discuss business issues.

Rule - Cellular Telephones

Sensitive information should NEVER be discussed on cordless or cellular telephones.

HINT: You can use voice-line encryption if you need to discuss business on these telephones.

Rule - Tapped Telephone Calls

Telephone lines may be tapped or otherwise intercepted by unauthorized parties. For this reason, you should avoid discussing sensitive information regarding your organization when on the telephone.

Rule - Answering Machines

You must not leave messages containing sensitive information on answering machines or voicemail systems.

Rule - Credit Cards on Pay Phones

While using public pay telephones, you should swipe your telephone or other credit cards rather than typing or speaking the numbers for billing information.

Rule - Organization Telephone Book Security

Telephone books must not be distributed to outsiders or other third parties without specific authorization.

Rule - Consent to Record

In meetings or when using a telephone, you not use speakerphones, microphones, loudspeakers, tape recorders, or similar technologies unless you

have first obtained the consent of both the originator(s) and recipient(s) of the call.

Rule - Faxing Sensitive Information

If you need to fax sensitive information, the recipient must first have been notified of the time when it will be transmitted, and also have agreed that an authorized person will be present at the destination machine when the material is sent.

You must have the proper authority to fax the information. You should never fax sensitive information over unencrypted lines.

HINT: You can have a password protected fax mailbox to restrict unauthorized release of the materials.

You must never allow a third party to perform the fax, that is, hotel staff, retail clerk, etc.

Rule - Fax Cover Sheet

If you are sending sensitive information via the fax, a cover sheet should first be sent and acknowledged by the recipient. After this is performed, the sensitive information may be sent via another call occurring immediately thereafter.

Rule - Taping Sensitive Information

You should not record sensitive information with dictation machines, tape recorders, or similar devices.

Explanation/ Key Points

If you must use these devices in your job, the proper sensitivity classification must be specified at the beginning and end of each segment of sensitive information. The recording media must also be marked with the most stringent data classification found on the media. It should be erased as soon as possible.

Rule - Video Conferencing

You must not record video-conferencing sessions must unless it is approved and communicated in advance to all videoconference participants.

Rule - Other Devices - Transmissions

You must never transmit confidential information via wireless microphones, walkie-talkies, radio local area networks (LANs), radio personal computer docking systems, and other unencrypted radio transmissions.

HR Related Rules

Rule - Returning Organization Property

Employees, temporaries, contractors, and consultants should not receive their final paycheck (?) unless they have first returned all hardware, software, working materials, confidential information, and other property belonging to the organization.

Rule - Help Wanted Ads and Disclosure

All public help wanted advertising or announcements must be approved in advance by the Human Resources Department (?) prior to being placed. The will ensure that labor law requirements are met, and that sensitive internal information is not inadvertently released.

Rule - Gathering Prospective Employee Information

Personal information about a prospective employee may not be gathered unless it is both necessary to make an employment decision and also relevant to the job in question. This includes marital status, family planning objectives, off-hours activities, political affiliations, performance on previous jobs, previous employers, credit history, education, and other personal details. (?)

Rule - Employee Monitoring Notification

Your daily activities cannot be monitored without first securing your permission. You organization cannot use computers to automatically collect information about your job performance unless you have first agreed.

Explanation/ Key Points

An exception may be those instances where advance permission is likely to change the behavior in question (e.g., suspected criminal activity).

This does not include the type of monitoring required to protect organization property, your safety, and your personal property. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no electronic monitoring will be performed.

Rule - Personnel Records and the Employee

You should have open access to your personnel records at your organization.

Explanation/ Key Points

Your personnel records must not be kept from you. You may be required to request you records in writing. You should be allowed to make a copy for yourself.

HINT: You could allow each employee a copy of their own personnel records to review and to ensure that it contains no errors every **{12}** months.

The only exception to this Rule is personnel criminal investigation information.

File reviews must only be conducted at appointed times, during business hours, and in the presence of a Human Resources representative.

If employees object to the accuracy, relevance, or completeness of information appearing in their personnel file, they must be given an opportunity to add supplementary statements

Rule - Employee Job Performance Privacy

Individual employee job performance information must not be posted on bulletin boards or otherwise made available to others who do not have a legitimate business-related need-to-know.

Rule - Benefits Cannot be Denied

You cannot be denied benefits if you refuse to provide unnecessary private information. Disputes about the definition of "necessary private information" will be defined by your organization.

Rule - Using Employee Information

The HR Department must make reasonable efforts to ensure that all personal information is used only as intended, and that precautions preventing misuse are effective and appropriate.

Personal information about employees, consultants, or contractors, which has been gathered for one purpose, may not be used for another purpose without the clear and unambiguous consent of the parties to whom this information pertains.

This page is intentionally left blank for pagination of double-sided printing. ⌨

Chapter 8

Access Control/ Workstation / Office Rules

About Your Workstation / Office

One of the main ways that you, the employee, can contribute to your organizations ISS program is to be aware of your immediate surroundings, observe your working habits, and take the necessary precautions to safeguard your working area. Whether you have an office with a door, a cubicle or an open desk layout, you can be a major factor in the security of your information.

Workstation Rules

Workstation Rules

Rule - Clear Desk

You must not leave sensitive or other organization information in plain view on your desk or working area. Be sure all information is properly secured, especially during non-working hours.

Rule - Clear Screen

You must not leave sensitive or other organization information in plain view on your screen or terminal in your working area.

Rule - Office (with a door)

If your working area includes a door, it is important that you shut and/ or lock the door when you leave your working area for an extended period of time throughout the day and at the end of day.

Rule - Cubicle Security

If your working area is in a cubicle, you are in a more open environment with easier access to your information. You should take necessary precautions, don't leave items exposed on your desk or terminal and lock up your personal property.

Rule - Securing Unattended Workstations

You should log off your computer if you will be leaving your workstation for an extended amount of time. (i.e. meeting, lunch, break, end of day). If you leave your workstation unattended for **{10}** minutes, your screen will lock up.

Troubleshooting

Problem: What should I do if … I left for an extended period of time and my screen locked up?
Action: (?)

Rule - Loading Personal Screen Savers

Rule – Bringing your personal PC/ laptop to Work

You must properly secure and protect your personally owned computer equipment (i.e. PCs, laptops, …) that you have brought to work. This non-organization owned equipment needs to follow the same safeguards.

Explanation/ Key Points

These PCs or laptops have been used as stand-alone machines, but they still contain your organizations information.

🕮 Rule - Personal Equipment and Information Ownership

The information you create and develop on your personal equipment (at home or at the office) is owned by your organization.

🕮 Rule - Personal Equipment and Privacy

If you are using your personal equipment (at home or at work) containing organization information, you must follow your organizations privacy issues and keep the information confidential.

🕮 Rule - Home Computers Security

You must incorporate the proper security safeguards if you generate information on your personal equipment at home and then transfer it to their work PC.

🕮 Rule - Workstation Protection Security

Reasonable efforts should be made to safeguard your individual workstations to protect against unauthorized access to your workstation, network or data.

Explanation/ Key Points

Workstations can be secured by securing the rooms where they are located and by physically attaching them to tables or work areas so that special tools are required to remove them from the premises.

🕮 Rule - Sensitive Information While Working

You must cover sensitive information if another person enters the area around your desk. If the information is in physical form, the information can be covered with other material. If the information is displayed on a computer screen, you may invoke a screen saver or log off.

Explanation/ Key Points

If you handle sensitive information and are in the immediate vicinity of a conference room, all meetings with third party visitors (vendors, customers,

regulators, etc.) who are not authorized to have access to such sensitive information must take place in fully enclosed conference rooms.

🕮 Rule - Locking File Cabinets

If you handle sensitive information in the course of your regular business activities, you must be provided with locking file cabinets. You must lock all sensitive material in these file cabinets when away from your desk, and must provide a backup copy of the key(s) to the proper authorities.

🕮 Rule - Screen Positioning

If you handle sensitive information, you must position your computer display screen away from others view. This includes away from hallways, windows, doors, reception or public areas.

🕮 Rule - Moving and Relocating Your Equipment

You must not move or relocate any office computer equipment (desktop computers, fax machines, LAN servers, network hubs, etc.) without the proper approval.

Disposal Rules

You must be very careful when throwing away obsolete equipment or media devices for they may contain organization information.

Rule - Information Disposal/ Wiping

You must properly dispose of devices containing organization information. PCs must be wiped clean of data and software.

Explanation/ Key Points

There are products available to wipe data from media, CDs, diskettes and hard drives. This will "sanitize" it for disposal.

IMPORTANT: Be aware of what information is on all devices that are being re-sold.

Rule - Discarding Hardcopy Information

You must not throw away sensitive hardcopy materials into hotel wastebaskets or other publicly accessible trash containers. All sensitive information must be retained until it can be shredded, incinerated, or destroyed with other approved methods.

Explanation/ Key Points

This rule applies to paper, microfiche, typewriter ribbons, carbon papers, stencils and templates, photographic negatives, thermal fax transfer films, computer hardcopy output, photocopies, and such.

Rule - Personal Equipment Disposal

If you use your personal equipment (PCs, laptops) for work purposes, you must dispose of information properly. This applies to all the information on your equipment, whether you are at the office or have transported the information out of your working environment.

Rule - Destroying Unwanted Hard Copies

If you need to discard unwanted hard copies of information, you need to shred it before it is thrown away.

Rule - Sensitive Information Disposal/ Concealment

Before computer magnetic storage media is sent to a vendor for trade-in, servicing, or disposal, all your organizations sensitive information must be destroyed or concealed. (i.e. degaussed, demagnetized, wiped, or zeroized)

Rule - Erase and Zeroize

When you erase sensitive information from a disk, tape, or other magnetic storage media, it must be followed by a repeated overwrite operation (zeroization) which prevents the data from later being scavenged.

NOTE: This is especially important if you are transferring information to a third party.

Rule - Destruction Approval

You must not destroy or dispose of potentially important organization records or information without specific advance approval. Unauthorized destruction or disposal of your organizations records or information will subject you to disciplinary action including termination and prosecution. (?)

Explanation/ Key Points

Records and information must be retained if: (1) they are likely to be needed in the future, (2) regulation or statute requires their retention, or (3) they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts.

Destruction is defined as any action, which prevents the recovery of information from the storage medium on which it is recorded (including encryption, erasure, and disposal of the hardware needed to recover the information).

Media Security Rules

Media, that is CDs, diskettes, jazz drives, and such, may be required in your job to transport, store, or back up your daily information. This media may be used day-to-day and reside near your workstation for ease and usability.

One of the main concerns in ISS security is the safekeeping and day-to-day protection of your media that you use every day.

Rule - Media Safety

You must protect and safely store all media devices that you use to do your daily job.

Explanation/ Key Points

When not being used by authorized workers, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information must be locked in file cabinets, desks, safes, or other furniture. Likewise, when not being used, or when not in a clearly visible and attended area, all computer media (floppy disks, CD-ROMs, etc.) containing sensitive information must be locked in similar enclosures.

Rule - Hard Drive Security

Highly Restricted and Confidential information should not be on your workstation hard drive. Most workstations pose a risk of unauthorized access because the drives are accessible.

Rule - Sensitive and Non-sensitive on Same Media

You must not store Highly Restricted or Confidential information such that it is commingled with non-sensitive information on floppy diskettes or other removable data storage media.

This page is intentionally left blank for pagination of double-sided printing.

Chapter 9

Physical / People Security Rules

About Physical / People Security

When you enter a building, room, or office and need to gain entry by using a card, fingerprint, or other means, then your organization takes physical security measures. This type of security usually involves a device attached to a wall or door at the entry point. When you gain access to a secured area (i.e. computer operations room, cash handling room), you have been given prior access clearance or your identity has somehow been noted or recorded. Many organizations also require the same access methods to leave the building.

Typically organizations that house system operations will require physical security into the building and even the parking garage. Sometimes a security guard will be stationed at the entry point to further provide physical access security by observing employee traffic, handling deliveries and visitors.

Physical Security Rules

Physical / People Security Rules

Physical / People Security Rules

Rule - Tailgating and Piggybacking when Entering

If you are entering with someone else, you should still show your badge or show proof that you can enter. If someone else is entering with you, be sure to check them to see that they are authorized to enter.

Explanation/ Key Points

You must not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when you go through these entrances.

Rule - Handling Visitors

All visitors must show proper identification and sign in prior to gaining access to restricted areas controlled by the organization. Visitors must be admitted to only for specific authorized purposes.

Rule - Visitor Escorts

Visitors must be escorted at all times by an authorized employee, consultant, or contractor. This means that an escort is required as soon as a visitor enters a controlled area, and until this same visitor goes outside the controlled area.

Rule - Challenging Strangers

You should challenge any strangers you see on the premises that are not properly identified. (i.e. no badge). If they cannot promptly produce a valid badge, they must be escorted to the receptionist desk.

Explanation/ Key Points

If you notice an unescorted visitor inside your organizations restricted areas, the visitor must be immediately questioned about the purpose for being in restricted areas. The visitor must then be directly accompanied to either a reception desk, a guard station, or the person they came to see.

Rule - Lending Cards/ Keys, Tokens

You must never lend your access device: cards, keys, token, etc, to a secured area to anyone.

Rule - Social Engineering

Beware of people that ask a lot of questions about the organization and its security. They may be trying to gain knowledge to gain unauthorized access. It is called Social engineering and it the process of convincing people to divulge information that they should not. Often built on false pretenses, and misidentification, social engineering is extremely effective. This is accomplished by name dropping, gaining your confidence, and sometimes through intimidation.

Rule - Sensitive Information and Physical Access Controls

Access to every office, computer room, and work area containing sensitive information must be physically restricted. Suggestions: receptionists, metal key locks, magnetic card door locks, etc.

Rule - Lock Office Doors

If you have a separate offices with a door, you must lock the doors you're your office is not in use. This practice will help to restrict unauthorized access to sensitive information.

Rule - Visitors Entrances

Visitors and other third parties must not be permitted to use the employee entrances or other uncontrolled pathways leading to areas containing sensitive information.

Rule - Wearing ID Badges

When in your organizations buildings or facilities, all persons must wear an identification badge on their outer garments so that both the picture and information on the badge are clearly visible.

Rule - Temporary ID Badges

If you forgot your badge, you must obtain a temporary badge by providing positive proof of identity. A temporary badge is valid for {1} day only.

Rule - Reporting Stolen/ lost Access Badges/ Cards/ Tokens

ID badges and physical access cards that have been lost or stolen--or are suspected of being lost or stolen--must be reported to the Security Department (?) immediately. Likewise, all computer or communication system access tokens (smart cards with dynamic passwords, telephone credit cards, etc.) that have been lost or stolen--or are suspected of being lost or stolen--must be reported to the Security Department (?) immediately.

Rule - Presenting Your Badge

You must present your badge to the badge reader / guard before entering every controlled door within your organizations premises. Before proceeding through every controlled door, you must wait until the badge reader indicates that you have permission to enter the area.

Rule - Propping Open Doors

Whenever doors to a secured area are propped open (perhaps for moving computer equipment, furniture, supplies, or similar items), appropriate personnel must continuously monitor the entrance.

Rule - Stay away from Restricted Areas

You must not attempt to enter restricted areas in your organization for which you have not received access authorization.

Rule - Sensitive Information and Working Alone

You must never be permitted to work alone in restricted areas containing sensitive information.

Rule - Property Pass for Removing Equipment

PCs, cellular telephones, portable computers, modems, storage media and related information systems equipment must not leave the organization premises unless accompanied by an approved property pass. All such removals of storage media must be logged at the building's front desk.

Chapter 10
Getting ISS Help

Getting ISS Help

You will probably receive this Guide in a training class or seminar. You can also use it on-going for a reference guide as you need it. This chapter is written to answer any questions you may have on your ISS program.

Call for ISS Support

☎ If you need to ask ISS questions, call (xxx) xxx-xxxx.

☎ If you need to report an incident, IMMEDIATELY call (xxx) xxx-xxxx.

Troubleshooting Chart

Problem/ Question	Explanation	See Chapter …
What should I do if … I see something suspicious or an actual incident in action?	Do not handle it yourself. IMMEDIATELY Call xxx xxx-xxxx or your manager.	2

Appendix

Appendix A - Attachments

(Possible Attachments: These are forms that the employee needs to sign regarding ISS. We would design actual forms below or use existing ones?)

Non-disclosure Agreement

All employees and contractors (temporaries, consultants, outsourcing firms, etc.) must personally sign a Company ABC Non-disclosure agreement. (insert sample)

The provision of a signature must take place before work begins, or if a worker has been working without a non-disclosure agreement, a signature must be provided as a condition of continued employment.

Prior to sending any sensitive information to a third party for copying, printing, formatting, or other handling, the third party must sign an organization non-disclosure agreement. (?)

Acknowledgement of reading Rules (from NITC)

All new employees with access to critical systems or sensitive information will sign a statement acknowledging they have received and read the policy and understand their responsibilities. This should include knowledge of the consequences of violations of security procedures. (need sample?)

Contractors Acknowledgment of Reading Rules (from NITC)

Contractors, agents acting on behalf of the state, auditors, and other non-employees in a position to impact the security or integrity of information assets of the state will be made aware of the Information Security Policy. These individuals must sign a statement acknowledging they have received and read the policy and understand their responsibilities. (need sample?)

Compliance Agreement (from NITC)

(for committee decision?) A signed statement indicating awareness, compliance and intent of continued compliance with information security policy and standards will be required upon annual review of each employee with access to critical systems or sensitive information. (need sample?)

Computer Security Incident

Report Form used to detail an incident. (insert sample)

Risk Notification If you discover a risk that could become an incident. (insert sample)

Others ???

Appendix B - List of Rules

The following list is a summary of all the Rules in this Guide.

Logging On Rules

- Rule - Unique User ID and Password
- Rule - Prohibit Group User IDs
- Rule - Unsuccessful Logging On
- Rule - Limitation on Number of Daily Log Ons

Warning Banner Rules

- Rule - Display a Warning Banner
- Rule - Warning Banner Keystroke Monitoring
- Rule - Warning Banner Last Logon

Logging Off Rules

- Rule - Automatic Log Off
- Rule - Leaving Your Workstation - Logging Off / Locking
- Rule - General Logging On

Identification (User ID) Rules

- Rule - Unique User ID
- Rule - Sharing your User ID is Prohibited
- Rule - Using another Users ID is Prohibited
- Rule - Dormant User IDs
- Rule - Forged Messages
- Rule - Internet User ID Expiration

Authentication (Password) Rules

- Rule - Changing Your Default Password
- Rule - Difficult to Guess Passwords
- Rule - Minimum/ maximum Password Length
- Rule - Cyclical Previous Passwords
- Rule - Password Allowable Characters
- Rule - Passwords Lower and Upper Case
- Rule - Keeping Your Password Confidential
- Rule - Reusing Passwords / History
- Rule - Display and Printing Passwords
- Rule - Forced Expiration of Passwords
- Rule - Unsuccessful Passwords Attempts
- Rule - Same Password on Different Systems
- Rule - Disclosure Forces Password Change
- Rule - Writing Passwords Down
- Rule - Writing Previous Near Devices
- Rule - Proof Of Identify to Obtain a Password
- Rule - Choosing Your Password

Authorization (Privileges) Rules

- Rule - Authorized Privileges

Network Access Rules

- Rule - Approval for Connections
- Rule - Gaining Unauthorized Access
- Rule - LAN Backups
- Rule - Network Browsing Prohibited
- Rule - Backup Notification
- Rule - Altering Computer Equipment
- Rule - Overwhelming the Network
- Rule - Malicious Intent and the Network

Modem Rules

- Rule - Modems Connections to Internal Networks Prohibited
- Rule - Prohibit Modems in AutoAnswer Mode

Remote Access Rules

- Rule - Dial-up Password Attempts
- Rule - Remote Access Training

Remote Sites Rules

- Rule - Telecommuting Permissible Equipment
- Rule - Protections of Off-Site Property
- Rule - Information to be Returned
- Rule - Remote Working Environment
- Rule - Security at Home / Off-site
- Rule - Right to Conduct Inspections of Telecommute Office
- Rule - Sensitive Information on Portable Computers
- Rule - Backing up Portables Computers
- Rule - Transportable Computers Hand Luggage on Airplanes
- Rule - Portable Computer Security

E-mail Rules

- Rule - E-mail Virus Protection Software
- Rule - E-mail for Business Purposes Only
- Rule - E-mail and Confidential Information
- Rule - Forwarding E-mail
- Rule - Blanket Forwarding E-mail
- Rule - Forwarding External E-mails
- Rule - Forwarding E-mail to Archival Records
- Rule - E-mail Retention
- Rule - Certainty of E-mail File Attachments Origin
- Rule - Using another Users E-mail Account
- Rule - Using E-mail as a Database
- Rule - Deleting and Destroying E-mail
- Rule - Privacy and E-mail

- Rule - E-mail is Public Communication
- Rule - E-mail as a Public Record (government)
- Rule - E-mail Profanity
- Rule - Responding to Junk (SPAM) E-mail
- Rule - Ownership of E-mail Messages and Attachments
- Rule - Disclosure of E-mail Messages and Attachments
- Rule - Authorization to Issue Broadcasts in E-mail
- Rule - Scanned Signatures in E-mail
- Rule - Misrepresentation of identity in E-mail

Internet Rules

- Rule - Downloading Internet Files and Information
- Rule - Sending Sensitive Information Over the Internet
- Rule - Reliability of Downloaded Information Over the Internet
- Rule - Uploading via the Internet
- Rule - Using the Internet for Personal Use
- Rule - Using Internet Search Engines
- Rule - Filtering Inappropriate Internet Information
- Rule - Using the Internet in an Acceptable Way
- Rule - Using Copyrighted Information from the Internet
- Rule - Approval for Internet Connections
- Rule - Training for Internet Use
- Rule - Internet User ID Expiration
- Rule - Personal Messages Disclaimer on Internet
- Rule - Internet Products and Services
- Rule - Disclosure of Personal Information on the Internet
- Rule - Public Area of Your Organizations Web Site
- Rule - Unofficial Web Pages on the Internet
- Rule - Concealing your Identity on Internet is Prohibited
- Rule - Exchanges of Information on the Internet
- Rule - Updating Organization Information on the Internet

E-commerce Rules

- Rule - Giving Information when Ordering Internet Products
- Rule - E-transactions
- Rule - Forming E-contracts
- Rule - Validating Identity of External Parties on Internet
- Rule - Electronic Offers
- Rule - Internet Customers

Copyright Rules

- Rule - Copyright Laws for Software and Paper
- Rule - Copyrighted Inquiries
- Rule - Copying Copyright Materials
- Rule - Protection of Software and Copyrighted Materials
- Rule - Copyright Enforcement Statement
- Rule - Making Excess Copies Prohibited
- Rule - Copying Vendor Software
- Rule - Sending Copyrighted Information Electronically
- Rule - Violation of Copyright Laws
- Rule - Using Copyrighted Information from the Internet Rule

- Rule - Ownership of Copyrighted Materials

Acceptable Use (of systems) Rules

- Rule - Storing Games on your Computer
- Rule - Personal Use of your Computer
- Rule - Other Business Activities
- Rule - Using State-Owned Resources Unrelated to Business
- Rule - Using State-Owned Resources in an Acceptable Way
- Rule - Misrepresentation on State-Owned Resources
- Rule - Using Others Users Data on the State-Owned Resources
- Rule - Preventing Services to Others
- Rule - Using State Resources in an Acceptable Way
- Rule - Giving Information to a Third Party
- Rule - Handling Third Party Confidential Information
- Rule - Other Business Activities
- Rule - Exposure of Sensitive information Public Places
- Rule - Time Sensitive Information
- Rule - Sensitive Disclosure Statement

Other Employees/ Organization Rules

- Rule - Disclosing Co-worker(s) Contact Information
- Rule - Disclosing Co-worker(s) Change in Status Information
- Rule - Personal Identifiers Prohibited
- Rule - Disclosing Organization Information
- Rule - Disclosing Organization Secured Areas
- Rule - Disclosing Organization Future Plans Prohibited
- Rule - Sensitive Information and Meetings
- Rule - Sensitive Information and Meeting Rooms
- Rule - Employee Health and Safety Disclosure
- Rule - Organizations Documentation

Public Records/ Privacy Rules

- Rule - Privacy of Citizens
- Rule - Managing Public Records
- Rule - Privacy and E-mail
- Rule - Violating Others Privacy
- Rule - Public Records
- Rule - Personal Identification Information (PII)
- Rule - Consent to Disclose Information to Law Enforcement
- Rule - Collecting Private Information
- Rule - Children's Privacy
- Rule - Customers Privacy
- Rule - Customers Disclosure
- Rule - Explanation for Private Information
- Rule - Disclosure Notification / Blocking Privacy Request
- Rule - Public Records Source Owner
- Rule - Materials Released to the Public

Paper Information Rules

- Rule - Copying Sensitive Information
- Rule - Copying Sensitive Information and Special Paper
- Rule - Copier / Printer Malfunction
- Rule - Waste Copies
- Rule - Attending to Printers
- Rule - Sensitive Information – Page Numbering
- Rule - Third Party Copying Sensitive Information
- Rule - Mailing Envelopes for Sensitive Information
- Rule - Tracking Mailed Sensitive Information
- Rule - Delivery of Sensitive Information
- Rule - Filing Sensitive Information
- Rule - Destroying Unwanted Hard Copies

Using Software and Data Rules

- Rule - Downloading Software
- Rule - Protecting Software / Handling a Virus
- Rule - Malicious Intent is Prohibited
- Rule - Retaining Data
- Rule - Input Data Retention
- Rule - Copying Software
- Rule - Purchasing and Installing New / Upgraded Software

Using File and Directory Rules

- Rule - Others User Directories
- Rule - Unauthorized Access Prohibited
- Rule - Receiving Information on Disks
- Rule - Setting up new Folder/ Directories
- Rule - Amending Directory Structures
- Rule - Using Meaningful File Names

Telephone, Faxes and Other Devices Rules

- Rule - Telephone Disclosures
- Rule - Cellular Telephones
- Rule - Tapped Telephone Calls
- Rule - Answering Machines
- Rule - Credit Cards on Pay Phones
- Rule - Organization Telephone Book Security
- Rule - Consent to Record
- Rule - Faxing Sensitive Information
- Rule - Fax Cover Sheet
- Rule - Taping Sensitive Information
- Rule - Video Conferencing
- Rule - Other Devices - Transmissions

HR Related Rules

- Rule - Returning Organization Property
- Rule - Help Wanted Ads and Disclosure
- Rule - Gathering Prospective Employee Information

Workstation Rules

- Rule - Clear Desk
- Rule - Clear Screen
- Rule - Office (with a door)
- Rule - Cubicle Security
- Rule - Securing Unattended Workstations
- Rule - Loading Personal Screen Savers
- Rule - Bringing your personal PC/ laptop to Work
- Rule - Personal Equipment and Information Ownership
- Rule - Personal Equipment and Privacy
- Rule - Home Computers Security
- Rule - Workstation Protection Security
- Rule - Sensitive Information While Working
- Rule - Locking File Cabinets
- Rule - Screen Positioning
- Rule - Moving and Relocating Your Equipment

Disposal Rules

- Rule - Information Disposal/ Wiping
- Rule - Discarding Hardcopy Information
- Rule - Personal Equipment Disposal
- Rule - Destroying Unwanted Hard Copies
- Rule - Sensitive Information Disposal/ Concealment
- Rule - Erase and Zeroize
- Rule - Destruction Approval

Media Security Rules

- Rule - Media Safety
- Rule - Hard Drive Security
- Rule - Sensitive and Non-sensitive on Same Media

Physical Access Rules

- Rule - Tailgating and Piggybacking when Entering
- Rule - Handling Visitors
- Rule - Visitor Escorts
- Rule - Challenging Strangers
- Rule - Lending Cards/ Keys, Tokens
- Rule - Social Engineering
- Rule - Sensitive Information and Physical Access Controls
- Rule - Lock Office Doors
- Rule - Visitors Entrances
- Rule - Wearing ID Badges
- Rule - Temporary ID Badges
- Rule - Reporting Stolen/ lost Access Badges/ Cards/ Tokens
- Rule - Presenting Your Badge
- Rule - Propping Open Doors
- Rule - Stay away from Restricted Areas
- Rule - Sensitive Information and Working Alone
- Rule - Property Pass for Removing Equipment

This page is intentionally left blank for pagination of double-sided printing. ⌨

Appendix C - Glossary

This glossary contains words, phrases and acronyms that your will find useful in understanding your ISS program.

Term	Definition
Access Control	
Agency	Any government entity, including state government, local government, or third party entities under contract to the agency. (This definition is taken right from NITC - we call it organization - should we leave it here?)
Authentication	
Authorization	
"Black night"	With this method, passwords may be taped in a conspicuous spot because they have been altered using some standard approach, such as bump the first letter up the alphabet one letter, bump the second letter down one letter, etc.
Broadcasts	
Critical Systems	Those systems or system components (hardware, data, or software) that if lost or compromised would jeopardize the ability of the system to continue processing.
Confidential	
Copyright	
Cyber Crime	
Denial of Service	
Disaster	Any event that threatens the destruction of information or availability of computer systems. A disaster may affect the physical security of computer systems, including equipment failures, fire, flood, other natural calamities, or theft of equipment. A disaster mayinvolve destruction or information or availability of computer systems due to system failure, human error, or intentional acts including computer crimes.
Disclosure	
"Dumpster-diving"	(going through the trash) could recover passwords printed on
E-commerce	
E-mail	The exchange and/ or sharing of messages, attachments, and calendar and scheduling information.
E-mail bombing	
FERPA	Family Education Rights and Privacy Act
GLB	
Hacker	
Highly Restricted	
HIPAA	
Identification	
IIHI	Individually Identifiable Health Information
Incident	
Information Availability	Ensuring that information and services are available when required.
Information Confidentiality	Protecting the sensitive information from unauthorized disclosure or intelligible interception.
Information Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Information Non-repudiation	Providing transfer and receipt of an unforgeable electronic transaction.
Information Security	The protection of data against accidental or malicious destruction, modification, or disclosure.
Internal Use Only	
Internet	
Intruder	
IS	
ISS	

Logon/ logoff	The processes by which users start and stop using a computer system.
Organization	Refers to any state agency, university, or other government facility.
Password	A private string of characters that is used to authenticate an identity.
Physical Access	
Piggybacking	
PII	Personally Identifiable Information
Policy	Highest level. *See NITC Security Architecture in appendix*.
Public records	
Privacy	
Procedures	A chronological event, usually contains steps 1,2,3. Procedures can be with and without rules. Most of the procedures are here in the Security Officer guide, complete with checklists and working papers. In the IS and GE Guide, the procedures are technology-dependent. You can add your procedures in the full format for any rule.
Remote Access	
Risk	
Rule	Lowest level
Security Policy	A statement of the goals, responsibilities, and accepted behaviors required for maintaining a secure environment. Security policies set the direction, give broad guidance and demonstrate senior management support for security-related facilities and actions across the organization.
Security Standard	A set of tasks, responsibilities, or guidelines that provide metrics to policies. Security procedures are standards that are very specific in nature, applying to group or individual systems. Procedures are directive in nature, whereas policies provide principles.
Sensitive Information	That information which must be protected to insure only authorized access or if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.
"Shoulder-surf"	(look over the shoulder of the user) to obtain the password.

Social Engineering	
Spamming	
Standard	Medium level. *See NITC Security Architecture in appendix*
State Data Communications Network (SDCN)	Any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to state computers.
Suspicion	
Tailgate	Coming into a secured access entry point on the heels of an authorized person.
Telecommuter	
Threat	
Unclassified/ Public	
User ID	The
Users of Electronic Assets	Any employee, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of a state agency or institution.
Value of Information	The cost of collection, cost of reconstruction and legal or operational consequences if information is lost or compromised.
Virus	a software program which replicates itself and spreads onto various data storage media (floppy disks, magnetic tapes, etc.) and/or across a network. The symptoms of virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.
Vulnerability	
Warning Banner	
Zeroization	

81-1190
Act, how cited.

Sections 81-1190 to 81-11,102 shall be known and may be cited as the Information Technology Infrastructure Act.

Source:
Laws 1996, LB 1190, § 1; Laws 2000, LB 1349, § 3.
Operative date July 13, 2000.

81-1191
Terms, defined.

For purposes of the Information Technology Infrastructure Act:

(1) Commission means the Nebraska Information Technology Commission;

(2) Department means the Department of Administrative Services;

(3) Enterprise means the entirety of all departments, offices, boards, bureaus, commissions, or institutions in the state for which money is to be appropriated for communications or data processing services, equipment, or facilities, including all executive, legislative, and judicial departments, the Nebraska state colleges, the University of Nebraska, and all other state institutions and entities;

(4) Enterprise project means an endeavor undertaken over a fixed period of time using information technology, which would have a significant effect on a core business function and affects multiple government programs, agencies, or institutions. Enterprise project includes all aspects of planning, design, implementation, project management, and training relating to the endeavor;

(5) Fund means the Information Technology Infrastructure Fund;

(6) Information technology means computing and telecommunications systems and their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store, and disseminate information electronically;

(7) Information technology infrastructure means the basic facilities, services, and installations needed for the functioning of information technology; and

(8) Statewide technology plan means the plan developed by the Nebraska Information Technology Commission pursuant to section 86-1506.

Source:
Laws 1996, LB 1190, § 2; Laws 2000, LB 1349, § 4.
Operative date July 13, 2000.

81-1192
Legislative findings.

The Legislature finds that:

(1) The effective, efficient, and cost-effective operation of state government requires that information be considered and managed as a strategic resource;

(2) Information technologies present numerous opportunities to more effectively manage the information necessary for state government operations;

(3) Information technologies are changing and advancing at a very rapid rate, increasing the computing power available to individual users;

(4) The commission should have the responsibility to establish goals, guidelines, and priorities for information technology infrastructure; and

(5) Periodic investments in the information technology infrastructure are required to develop and maintain the foundation for the effective use of information technologies throughout state government.

Source:
Laws 1996, LB 1190, § 3; Laws 2000, LB 1349, § 5.
Operative date July 13, 2000.

81-1193
Repealed. Laws 2000, LB 1349, s. 14.

81-1194
Legislative intent.

It is the intent of the Legislature that:

(1) A program be created with the goals of:

(a) Improving the efficiency of and reducing the cost of state government and its various agencies;

(b) Improving the technical capabilities and productivity of state employees and students, faculty, and administrators in state educational institutions;

(c) Addressing enterprise-wide information technology issues; and

(d) Clearly identifying and providing accountability for the costs and benefits of information technology in state government; and

(2) A fund be created to provide resources for periodic investments in the information technology infrastructure.

Source:
Laws 1996, LB 1190, § 5; Laws 2000, LB 1349, § 6.
Operative date July 13, 2000.

81-1195
Information Technology Infrastructure Fund; created; use; investment.

The Information Technology Infrastructure Fund is hereby created. The fund shall contain revenue from the special privilege tax as provided in section 77-2602, gifts, grants, and such other money as is appropriated or transferred by the Legislature. The fund shall be used to attain the goals listed in section 81-1194 and the goals and priorities identified in the statewide technology plan. The fund shall be administered by the department. Expenditures shall be made from the fund to finance the operations of the Information Technology Infrastructure Act in accordance with the appropriations made by the Legislature. Any money in the fund available for investment shall be invested by the state investment officer pursuant to the Nebraska Capital Expansion Act and the Nebraska State Funds Investment Act.

Source:
Laws 1996, LB 1190, § 6; Laws 1998, LB 924, § 42;
Laws 2000, LB 1349, § 7.
Operative date July 13, 2000.

81-1196
Repealed. Laws 2000, LB 1349, s. 14.

81-1196.01
Fund allocation for enterprise projects; procedures.

The Legislature may allocate money from the fund for enterprise projects. The Legislature may recognize multiple-year commitments for large projects, subject to available appropriations, including remaining obligations for the century date change project managed by the department. No contract or expenditure for the implementation of an enterprise project may be initiated unless the commission has approved a project plan. The project plan shall include, but not be limited to, the objectives, scope, and justification of the project; detailed specifications and analyses that guide the project from beginning to conclusion; technical requirements; and project management. The commission may request clarification, require changes, or provide conditional approval of a project plan. In its review, the commission shall determine whether the objectives, scope, timeframe, and budget of the project are consistent with the proposal authorized by the Legislature in its allocation from the fund. The commission may also evaluate whether the project plan is consistent with the statewide technology plan and the commission's technical standards and guidelines. Pursuant to section 86-1510, the Chief Information Officer shall report the status of enterprise projects to the commission, Governor, and Legislature. In addition, the Chief Information Officer shall provide the Legislature a semiannual progress report for enterprise projects funded through the fund.

Source:
Laws 2000, LB 1349, § 8.
Operative date July 13, 2000.

81-1197
Repealed. Laws 2000, LB 1349, s. 14.

81-1198
Repealed. Laws 2000, LB 1349, s. 14.

81-1199
Commission; duties.

The commission shall:

(1) Develop procedures and issue guidelines regarding the review, approval, and monitoring of enterprise projects that benefit from the fund; and

(2) Monitor the status of projects implemented under the Information Technology Infrastructure Act, including a complete accounting of all project costs by fund source.

Source:
Laws 1996, LB 1190, § 10; Laws 1998, LB 924, § 43;
Laws 2000, LB 1349, § 9.
Operative date July 13, 2000.

81-11,100
Repealed. Laws 2000, LB 1349, s. 14.

81-11,101
Repealed. Laws 2000, LB 1349, s. 14.

81-11,102
Activities under act; reports required.

The commission shall report annually to the Governor and the Appropriations Committee of the Legislature concerning its activities pursuant to the Information Technology Infrastructure Act.

Source:
Laws 1996, LB 1190, § 13; Laws 2000, LB 1349, § 10.
Operative date July 13, 2000.