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

Logon/ logoff — 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)

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

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

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 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