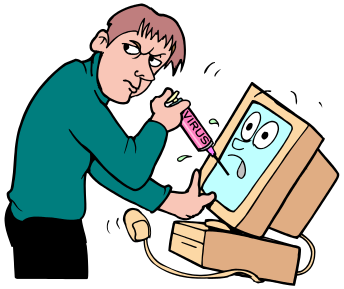
State of Nebraska

Information Security Systems (ISS)



Security Officer Instruction Guide

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

Final Draft
August 24, 2001

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

State of Nebraska
Information Security Guidelines

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

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

Computer User's Security Handbook

Version 1.0
August 24, 2001

Prepared by:

Table of Contents

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

Chapter 1
Getting Started

The Importance of an ISS Program

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

Securing Information in the Digital Age

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

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

What makes up a good ISS Program?

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

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

About your ISS Project

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

About the ISS Template Package

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

What are Information Security Templates?

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

What makes up the Template Package?

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

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

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

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

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

Technology Dependent

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

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

Information Security Template Characteristics

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

Assumptions

- Knowledge of basic security practices
- Knowledge of MS Word

Benefits

- Standardization
- Others?

Information Security Template Requirements

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

Initial vs. Existing Guides

Using the Template for Initial Setup

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

Using the Template to Update existing Manual

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

Keeping the Template current

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

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

ISS Policies and Procedures

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

Policies, Standards, and Rules

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

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

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

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

Procedures

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

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

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

The following procedures are incorporated into the template package:

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

About the Security Officer Instruction Guide

About this Guide

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

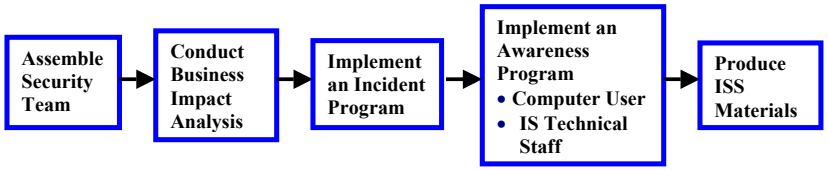
This guide provides the necessary working papers and checklists to help you to gather and analyze information.

The Template Process

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

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

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



ISS Program Process

Assemble a Security T.E.A.M.

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

Conduct Business Impact Analysis

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

Implement an Incident Program

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

Implement an Awareness Program

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

Prepare all ISS Materials (Use the templates)

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

Chapter 2

Assemble a Security TEAM

The Security TEAM

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

There may be several security teams:

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

Security Day-to-Day

There …

Security Advisory Committee(s)

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

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

Incident Response Team

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

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

The Security Officer

Appointing the Security Officer

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

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

The Tasks of the Security Officer

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

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

Rule Tasks

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

Systems Tasks

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

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

Security Tasks

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

Security Officer Training

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

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

- MISTI
- SAN
- … (add new ones?)

Security Staff

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

Security and the IS Department

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

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

Security Guards

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

Copyright Contact

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

Security Auditors

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

Security Audits

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

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

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

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

What should you audit?

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

Daily Audit/ Tracking Logs

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

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

Suggested logs by User ID:

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

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

Working Paper #1
Assemble a Security TEAM
Tasks and Responsibilites

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

(See list above)

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

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

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

0 you need to identify your team.

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

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

You have now identified your ISS TEAM!

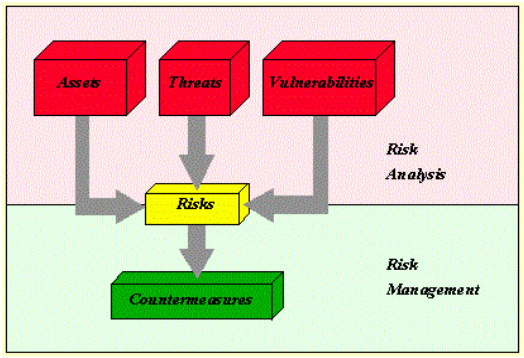
Chapter 3

Conduct Business Impact Analysis

About Business Impact Analysis

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

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



Business Impact Analysis Procedure

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

Steps:

Assets

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

Value

3. Assign a Value to each Asset

Threats

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

Risk

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

Classify

11. Classifying Assets (after Value and Risk)

Safeguards

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

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

Identify your Information Technology Inventory

What are Information Assets?

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

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

Assets Types

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

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

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

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

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

Asset Ownership

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

The Owner can also be another agency or regulated data.

Location

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

Inventory Number

(Optional?)

Working Paper #2
Business Impact Analysis
Information Inventory

---

1. List your Asset Types:

(See list above)

ISS Asset Types

1 _____
2 _____
3 _____
4 _____
5 _____
…

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

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

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

(By Asset Type)

ISS Asset	Owner	Location (physical or logical)	Inventory Number

Assign Values to Assets

What is the Value of an Asset?

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

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

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

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

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

How do you Calculate the Value?

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

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

OR use this approach:

Value Sum of Invested and Loss Impact

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

Impact (A code/ plus values?)

Re-creation

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

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

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

Unavailability / Denial of Service

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

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

Disclosure

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

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

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

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

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

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

Working Paper #2
Business Impact Analysis
ISS Asset Value

---

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

(By Asset Type)

ISS Asset	** Value **

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

OR

2. Use this method …

(See field descriptions above)

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

OR …….any other you wish to use.

Calculate the Risk Rating/ Measure (?)

What is Risk Analysis?

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

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

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

How do I Measure Risk?

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

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

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

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

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

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

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

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

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

Calculating Risk?

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

Risk Rating = Threat (+ or X) Vulnerability

Risk Rating = Threats + Impact + Likelihood

OR

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

OR

One Dimensional Approach to Calculate Risk (also confusing?)

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

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

OR

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

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

Likelihood	Loss	Risk

1	1	1 - low
1	2	2 - low
1	3	3 - low
2	1	2 - low
2	2	4 - moderate
2	3	6 - high
3	1	3 - moderate
3	2	6 - high
3	3	9 - high

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

OR

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

2-10 Low Risk

11 – 29 Medium Risk

30-50 High Risk

Acceptable Risk Rating

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

Working Paper #3
Business Impact Analysis
Risk Analysis

---

1. Make a list of all Risks.

…

2. For each Asset, calculate a Risk Rating.

ISS Asset	Threat (?)	Risk Rating

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

Assess Threats and Vulnerabilities

What is an ISS Threat?

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

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

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

TIP: Good employee relations help to minimize threats.

Identify Potential Threats

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

Threat Types:

- human error
  accident or lack of knowledge, the most common threat, reduce by education and reducing authorizations – least privileges
- system failures
  information systems: hardware (most solvable), software, infrastructure, power and communications.
- natural disasters

  (See Disaster Recovery in the IS Guide)
- malicious acts
  internal and external
  Ex. fraud, espionage, vandalism, theft, hackers,

- software virus

Threat Likelihood

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

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

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

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

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

OR

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

1 The threat is highly unlikely to occur.

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

3 The threat is likely to occur once per year.

4 The threat is likely to occur once per month.

5 The threat is likely to occur once per week.

6 The threat is likely to occur daily.

OR

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

5 Nearly certain

Threat Impact/ Consequences

Threat Impacts

Impacts describe the effect of a threat.

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

Impact Analysis - a number 0-6 as follows:

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

OR

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

Threat Consequences

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

Threat Calculations

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

Identifying Vulnerabilities

(Vulnerability is hard to understand?)

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

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

Vulnerability - common sources:

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

Working Paper #3
Business Impact Analysis
ISS Risk Measurement

1. Identify Potential Threats and Types.

Threat Type	Threat

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

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

Threat	Threat Likelihood (to that asset)	Impact	Vulnerability

4. For each …

Information Classification

What is classifying information?

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

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

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

(Link classifications > rules > safeguards > incidents?)

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

Classifying Your Information

When doing a Classification with your information, consider:

- Sensitivity of the data

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

- Regulated/ legal and contractual obligations and penalties

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

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

- Standards and guidelines

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

- Information lifecycle

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

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

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

General vs. Critical Systems

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

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

What should you protect?

Typically, the high risk information areas are:

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

- Executive plans
- others ??

Security Classification Levels

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

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

Classification Levels (4 Scale)

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

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

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

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

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

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

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

  Examples: annual reports, press statements approved for public use

Reclassification

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

Classification Levels Quick Reference

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

Working Paper #4
Business Impact Analysis
Asset Classification

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

ISS Asset	Risk Rating	Classification
Hardware		
Software		
Communications		
Databases		

Developing Safeguards

What are Safeguards?

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

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

Ways to protect:

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

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

Why safeguards?

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

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

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

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

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

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

Safeguard Types

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

Safeguard Tools

Tools

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

Others?

Software that will trace the source of attacks.

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

Assigning Safeguards to Risk and Assets

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

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

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

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

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

What do I do to assign Safeguards?

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

Select appropriate safeguards

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

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

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

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

After the needed security services are determined, consider the list of security mechanisms for each service. For each security service selected, determine the candidate mechanisms that would best provide that service. Using the threat/ vulnerability/ risk relationships developed (above), choose those mechanisms that could potentially reduce or eliminate the

vulnerability and thus reduce the risk of the threat. In many cases, a threat/ vulnerability relationship will yield more than one candidate mechanism. For example, the vulnerability of using weak passwords could be reduced by using a password generator mechanism, token based mechanism, biometrics, … Choosing the candidate mechanisms is a subjective process that will vary from one organization to another. Not every mechanism is feasible to use in every system. Some filtering of the mechanisms needs to be done to make this step beneficial.

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

Calculating Cost Measure

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

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

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

Comparing Risk and Cost

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

Implement and test safeguards

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

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

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

Accept Residual Value

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

Working Paper #5
Business Impact Analysis
Safeguards

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

ISS Asset	Classification	Safeguard (current)	Safeguard (proposed)

Business Impact Analysis Checklist ✓

____ Assets

____ Identify Your Information Inventory – Assets

____ Assign an Owner to each Asset

____ Assign a Value to each Asset

____ Threats, Risks

____ Identifying vulnerabilities to threats and damage potential

____ Prioritizing impact of threats

____ Develop a Risk Profile

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

____ Assign a Risk to each Asset

____ Classification

____ Classifying Assets (after Value and Risk)

____ Safeguards

____ Selecting cost-effective safeguards
____ Risk Acceptable

Chapter 4

Using the Templates

About the Templates

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

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

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

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

Using the Templates

Communication and Addressing your Audience

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

In the *Computer User's Security Handbook*, it is written using the term "you" to refer to your audience.

In the IS Technical Staff Handbook, the audience is addressed as "IS department" since there are many technical positions within the IS department and this handbook is general to anyone in the IS department. The role of the IS department is to support the end user, so there is reference to the "user" as the main target for the IS activities.

Templates Design and Organization

Modular Documentation

The design of the contents of the ISS template package is modular, that is, keeping topics contained in small sections, clearly labeled and in the chapter to which they relate.

How are the Rules organized?

This guide organizes the rules into categories for easy access and access. (expand)

Template Mechanics

(…)

Technology Dependent Areas

The templates structure was developed to be independent of any technology you have implemented into your security systems. One of the challenges in the design is to give the SO as much info as is needed without getting into any particular technology. For example,

Getting Started

- ***IMPORTANT***: Copy the template before you use it. (expand and add to *Quick Start Card*.)

MS Word Features Used

It is assumed you know how to use MS Word features in order to update the templates. There are a few MS Word features, however, that require some explanation. For complete details on using MS Word features, refer to a MS Word Guide.

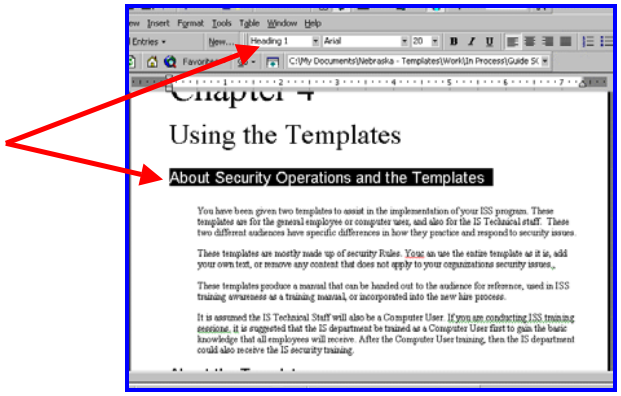
MS Word templates

The document files reside in the template area of MS Word. To see what templates you have available, …

When you install your template package, it will automatically …

MS Word styles

All of the chapter and section names have been chosen from the style guide. As you can see in the example below, the heading "About Security Operations and the Templates" is a Heading 1. This keeps your document consistent, automatically builds the Table of Contents, the allows for global updates.



WARNING: Do not choose " Update … style …" (get exact message …). This will change the style throughout the entire document!

MS Word Tables

Some of the content in the templates reside in tables. The table features are:

Table headings (expand on style)
Table text (expand on style)

MS Word Fields

MS Word allows you to enter parameters to globally be inserted into the document. For example, …

To add a field, …

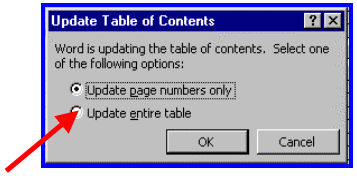
MS Word Linking

The list of Rules in the appendix of both templates have been automatically assembled from the Rules throughout all the chapters. So that you do not have to maintain the appendix list, a link has been set up for every rule. As you change a Rule in a chapter, it is also changed in the appendix list.

If you add a Rule, you will also have to add a link to keep the appendix list current. To do this, …

MS Word automatic Table of Contents

To update the Table of Contents, click on any text to highlight the entire Table of Contents, and then hit [F9]. This will update the page numbers and any headings you have changed. You may be asked:

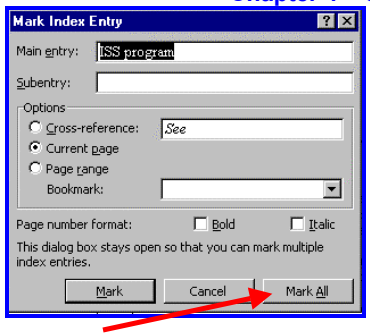


It is suggested that you always select *Update entire table*. (Put better sample with it checked).

MS Word automatic Index

To update the Index, click on any text to highlight the entire Index and then hit [F9]. This will update the page numbers and any new entries you have marked.

To add an entry to the Index, highlight the text you want to appear in the Index, and hit [Shift] + [Alt] + [x]. You will receive:

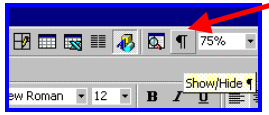


Click on the *Mark All* button to mark all occurrences of the selected text. It will appear on your screen as :

(show example) { …..}

and will put you into the Show/ Hide mode.

TIP: To exit the Show/ Hide mode, click on the Show/ Hide icon ¶.



Underlined Words

Many terms, phases, and acronyms are underlined throughout the template package to denote that there is more information about that topic elsewhere in the document. For example, all Glossary words are underlined implying that term is in the glossary.

The Rules are organized into meaningful security categories to facilitate locating a Rule. At the beginning of each Rule chapter (Chapters 3 -9 of the *Computer User's Security Handbook* and the *IS Technical Staff Handbook*.) For example,

Example: Physical Access Rules tells you there is more information about the topic.

If you decide to automate the template into an on-line system (e.g. Robo Help), you would use these underlined topics to build your links (go to) and pop-ups (glossary definitions).

Rule Statements

The Computer User's Security Handbook and the IS Technical Staff Handbook contain a comprehensive set of security Rules that you can tailor to meet your individual organizations needs. The content can be used "as is" or modified to reflect your security operations.

You can determine the size of your Rules guide. Important: If you have less rules, that does not mean they need to be written at a higher level.

Updating Rules

Initially you will need to review each Rule and determine:

1. … if you want to keep it, delete it, or modify it
2. … if you want to prioritize it – 1, 2, or 3
3. … if you want to use a full format or condensed format

On-going - what triggers a new Rule?

(Security changes, Technology changes, Business operations changes, NITC requirements change, HIPAA requirements change, …

Adding a Rule

(i.e. not listed in our template - their own) – copy and paste.

Adding a technology/ organization-dependant policy (i.e. not listed in our template - their own)

REMEMBER: If you add a Rule, you must add a link for the appendix list. See *MS Word Features Used* on how to add a MS Word link.

Changing a Rule

Deleting a Rule

Use the standard MS Word deletion techniques. If you delete all the Rules in a category, then you will also need to delete the category.

Rule Formats

The templates provide 2 formats for a Rule. You can choose the Full or Condensed format..

Condensed Format

(Explain how to incorporate with full format).

Most of the Rules in the templates are in the condensed format which states the Rule Title and Rule Statement. as follows:

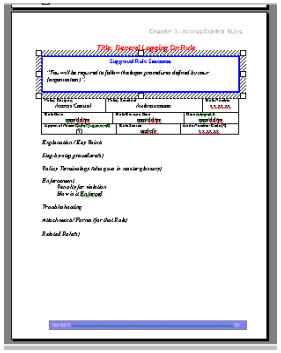
Rule - Unique User ID and Password

You MUST have a unique User ID and a confidential Password to log on. This User ID and Password combination will be required for access to your organizations information systems. *See Password Rules in this chapter.*

Full Format

The templates also have a full format if you want to add additional information to your Rules. You can insert any Rule in the condensed format into the full format by putting the Rule Title and Rule Statement in the format as follows:

(Get new screen shot and use same rule as in condensed to show how it is actually done?)



Full Format Rule Fields

You can fill in the full format for each selected Rule. Below are the suggested fields you could use.

Identify the Rule	Rule Name/ Title Rule Description/ statement Rule Number - how is it assigned? Who? Rule Category(s)
Dates	Date of Rule (history) Revision Date(s)

	Date Adopted/ approved (?)
About the Rule	Timing Process (flowchart) Responsibility (who does it) Key Points Step-by-step procedure(s) Rule Terminology (goes in master glossary)
Enforcement	Penalty for violation How is it Enforced (What if..) Reporting requirements
Supporting Topics	Troubleshooting Attachments/ Forms (for that policy) Related Rules

Assigning Priorities to Rules

You may want to assign priorities to your Rules to know which ones to emphasize and which ones to enforce. It is suggested you use the following priority levels:

Priority 1 Critical Rules
Use full format

Priority 2 Strongly Suggested Rules
Use full format or condensed format.

Priority 3 Optional Rules
No Format, just a list of Rule Title and Suggested Rule Statement. It will require less printing of pages and more cutting and pasting.

Template Parameters { }

You will need to decide certain values that are inserted into parameters. They are identified by the brackets { }. These parameters can appear in any of the 3 guides.

The following parameters have been incorporated into the templates:

# attempts to log on	You will be allowed {3} failed attempts to try to logon.
# daily log ons	You are not permitted to log on more than {10} times a day.
# days passwords expire	Your passwords will expire every {10} days.
auto log off	You will automatically be logged off if there has been no activity on your workstation for {10} minutes. This can different from platform to platform.
dormant User ID	Your User ID will automatically have the associated privileges revoked after {30} days of inactivity. If you are a temporary employee, contractor, or consultant, it will be revoked in {15} days.
#password attempts	You will be allowed {3} failed attempts to successfully enter your Password. OR You will be allowed 3 failed attempts within {5} minutes."
reusing passwords	You cannot reuse your Password for {15} changes. OR You must not use the same password more than once in a {12} month period.
inspection advance notice	Your organization maintains the right to conduct inspections of your telecommuter offices with {1} day advance notice.
# password attempts dial-in	The maximum permissible Password attempts for dial-up access is {3}. If you have not provided a correct password after three consecutive attempts, the connection must be immediately terminated.
# months expire Internet	Your User ID on Internet accessible computers must be set to expire {3} months from the time they are established.

Confirm e-offers	All contracts formed through electronic offer and acceptance messages (fax, Electronic Data Interchange, E-mail, etc.) must be formalized and confirmed via paper documents within **{2}** weeks of acceptance.
# minutes for unattended workstation	If you leave your workstation unattended for **{10}** minutes, your screen will lock up.
# days valid temporary badge	If you forgot your badge, you must obtain a temporary badge by providing positive proof of identity. A temporary badge is valid for **{1}** day only.
# weeks to respond privacy disclosure	A subject must be given advance notice that their personal data held by your organization has been requested by a third party. Unless compelled to release the data by clear and authoritative law or regulation, a reasonable period of **{2}** weeks must be provided for the subject to block this disclosure. No response from the subject can within that period can be considered to be acquiescence to the disclosure.
# years to keep records of disclosure	If you have the proper authority and disclose information to a third party, you must keep records of all such disclosures including specifically what information was disclosed, to whom it was disclosed, and the date of such disclosure. These records must be maintained for at least **{5}** years.
# weeks notice to customer to get info	If you must get customers information (i.e. via a subpoena), the customer will be given **{2}** weeks advance notice prior to the release to provide the information.
# months to see personnel records	You could allow each employee a copy of their own personnel records to review and to ensure that it contains no errors every **{12}** months.
# years data retention	You must retain all financial accounting, tax accounting, and legal records for a period of at least **{7}** years. All other records must be retained for a period of at least **{5}** years.
# day input retention	Business source documents containing input data must be retained for at least **{90}** days beyond the date when this information was entered into your organizations computer system(s).
phone numbers	If you need to ask ISS questions, call (xxx) xxx-xxxx. If you need to report an incident, IMMEDIATELY call (xxx) xxx-xxxx.
Remote # days backups	You must make periodic backups of all critical information and store it away from the portable device. These backups should be performed every **{1}** day. They should be stored elsewhere than the portable computer's carrying case.
Training	Employees should be have a formal security briefing within **{3}** days of their start date/ receiving their ISS packet.
Organization Name	Enter your **{Organization Name}**
Guide(s) name	Enter the title of your **{Guide name}**

Completing the Templates

About Completing the Templates

The majority of the templates are Rules …

Computer User's Security Handbook template is … (About Employee/ User Awareness / Individual Use)

The IS Technical Staff Handbook template is used the same way as the Computer User's Security Handbook Template.

The Sections of the Template(s)

The sections of the Computer User's Security Handbook template and the IS Technical Staff Handbook template are:

- Title Page
- Table of Contents
- (front matter)
- Chapter 1 About Information Security
- Chapter 2 Security Incidents
- Chapter 3 – 9 Rules
- Chapter 10 Getting ISS Help
- Appendix
- Index

Updating each Section

Title Page

1. Enter your **{Organization Name}.**

2. Enter the title of the **{Computer User's Security Handbook}** and **the {IS Technical Staff Handbook}**. Other possibilities are:

   General Employee ISS Booklet
   ISS User Reference Guide

   IS Department Security Handbook
   Technical Security Guide

Table of Contents

The templates Table of Contents has been designed with the structure and alignment automatically based on the chapter names, sections and sub-sections used throughout the documents.

It is recommend that you do not change the Table of Contents (TOC). You can change chapter names, headings and sub-headings, but not the Table of Contents format and structure.

REMEMBER: Hit F9 and the Table of Contents will automatically update chapters, sections, sub-sections, and page numbers. See *MS Word Features Used* in this chapter.

(front matter)

Insert any information you want to be separate from the page numbered guide, yet a part of the guide. For example: Proprietary Statement, Copyright / Trademark information, organization logo, and such.

Chapter 1 – About Information Security

In both templates, Chapter 1 covers all the general information about ISS. It is the introduction to ISS and to the guide itself. Here you can get an overview of what ISS is all about and learn some of the key areas of concern. You can use this chapter as it is or make changes. It is mostly boilerplate. You might want to add sections unique to your organization like: marketing ISS, your organizations support, and such.

Chapter 2 – Security Incidents

This chapter is slightly different between the templates due to the nature of the audience. The computer user needs to know the basic incident reporting requirements, while the IS technical staff may need to get more involved in the technical detection and evidence preservation.

A chart has been provided to summarize the reporting structures. You can update this chart to reflect your incident reporting structures.

Chapter 3 - 9 Rules

The templates contain a different set of Rules for each audience. The IS technical staff should be aware of the Rules in both templates.

Review each Rule and determine:

- if you want to keep it, delete it, or modify it
- if you want to prioritize it (1, 2, or 3)
- if you want a full format or condensed format

Computer User's Security Handbook template

The Computer User's Rules are arranged in the following categories:

Chapter 3 - Access Control Rules
Chapter 4 - Network Rules
Chapter 5 - E-mail, Internet, and E-commerce Rules
Chapter 6 - Individual Use/ Copyright Rules
Chapter 7 - Acceptable Use Rules
Chapter 8 - Workstation Rules
Chapter 9 - Physical Security Rules

IS Technical Staff Handbook template

The IS Technical Staff Rules are arranged in the following categories:

Chapter 3 - Access Control Rules
Chapter 4 - Network Rules
Chapter 5 - E-mail, Internet, and E-commerce Rules
Chapter 6 - Workstation and Equipment Rules
Chapter 7 - Systems Development Rules
Chapter 8 - Disaster Recovery Rules
Chapter 9 - Physical Security Rules

Chapter 10 – Getting ISS Help

This chapter is dedicated to helping the reader to answer any questions or concerns about ISS.

Review the Troubleshooting Chart and …

Appendix

Insert any information you want to be used as reference for the guide. This is where you put lists, supporting documents, and such. They are usually part of the page numbered guide. (unlike front matter).

The templates both contain the following appendix items:

List of Rules	This is a consolidated list of all the Rules in the guide. This list or Rules-at-a-glance is automatically linked to the Rules in chapters 3-9. (not yet!!)
Glossary	An ISS glossary. It is the same in both templates.
Attachments	…

Index

To help your reader find the topic they want to read, an Index is critical. Using standard MS Word indexing, you can update your index to include any words, phases, or acronyms. See *MS Word Features Used* section in this chapter.

Working Paper #x
Templates Checklist / Procedures

Be sure to follow these steps to use the templates:

1. ***IMPORTANT***: Copy the templates.
2. Review each Rule and determine:
   -if you want to keep it, delete it, or modify it
   -if you want to prioritize it (1, 2, or 3)
   -if you want a full format or condensed format
3. …

Chapter 5
Implement an Incident Program

What is an Incident Program?

In your ISS plan, the most important program you can implement is one that handles suspicions and incidents quickly and thoroughly. You need to be in position react, detect, and resolve. The key to a good response is having your team established, trained, and ready to react to any and all occurrences.

Your Incident program will usually involve your security team, but you may want to include others in your response team. For example, making managers of user departments aware of how to respond may be critical especially if the incident is occurring in their area with their information. The IS department will probably be a big part of the response team to provide the technical knowledge and evidence preservation.

The three main components that make up the Incident Program are:

- Prevention
- Detection
- Response

Suspicions and Incidents

Security Incidents or security breaches can occur at anytime. Your prompt attention to reacting to reported incidents could greatly deter the amount of damage, loss, or disclosure that has taken place.

Suspicions and Incidents

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

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

Prevention

Prevention is the key to good security practices, however, even with all the proper protection methods in place, there are always ways to compromise it. In order to know how to prevent incidents, you need to know what your assets are, where the risks lay, and how to protect critical information from being targeted. For complete details, see *Chapter 3 Business Impact Analysis* section *Safeguards*.

Detection

Detection is the only way of knowing when a system is being compromised. Without proper detection, you may never know when an incident has occurred and therefore it may continue to happen. Even worse that having a security incident is having one and not knowing it.

To understand intrusion detection, you must be aware of the intruder, where attacks come from, what motivates them, how attacks occur, and who the attackers are. Not all organizations have the resources to conduct their own intrusion detection and analysis. In these situations, it may be necessary to identify other sources for assistance in tracking and responding to possible incidents.

- ***IMPORTANT***: The difference between an incident and a disaster is detection!

Intrusion Detection Methods

There are many methods used to detect suspicious system behavior. Some methods will keep the intruder busy, while he is tracked down. Others will lock the intruder out until he is discovered.

It is important that detection methods not only find known attacks scenarios, but also new scenarios. Detection methods should look for the unusual and unexpected.

Intrusion detection systems (IDS) exist to help you safeguard your assets. These systems can monitor configurations, compare user actions, and distinguish conflicts in activities. IDS runs constantly with your system in the background and only notifies you when it detects something suspicious or illegal.

Whatever method you choose, be sure it is used daily and incorporated into your Incident program.

Tracking Intrusions

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

Incident Patterns

Response/ Reaction

Now that you have all your safeguards in place and are actively practicing good detection techniques, you can only hope that you have thought of everything. As many ways as there are to prevent mishap, there are just as many to circumvent your safeguards.

The key to further protecting your information even in the event of an attack is to have a good response plan implemented. A quick reaction can greatly diminish the damage.

If you do not have a response team established, you are depending on the reactions of users, IT and management to react, thus possibly turning a containable incident into a serious problem.

Your Incident Response Team

The security team you assembled in Chapter 2 may or may not be the same group that is responsible for the reaction to an incident. Be sure your response team knows who they are and have been trained in ISS issues.

- ***TIP***: Periodic mock drills are recommended for each possible type of attack.

Incidents Response Centers

There are companies that can assist in the incident handling process, but your internal response is the key. These companies can help you after the fact, with collecting and processing evidence and furthering the reporting to law enforcement and such if required.

Responding to ISS Incidents

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

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

Catastrophic Event

For catastrophic disasters such as fire, bomb threats, hostage situations, floods or destructive storms, the goals of employee safety and damage containment apply. Notification procedures

will include the appropriate public service departments (Fire Department or Police Department).

Secured Area Intrusion

For intrusion of secured areas, the goals of employee safety, intruder identification, and if warranted, the intruder's removal from the premises apply. Notification procedures will include building security or local police.

Virus Reporting

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

Electronic Intrusion

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

Unauthorized Access Intrusion

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

Notifying the Intruder – yes or no?

In some cases, a stern cease and desist message must be sent to the source of all attacks against your organizations computers whenever the source or intermediate relay points can be identified. The intention of this is to send a message to attackers that their activities have been noticed and that they should stop immediately. Such a message may, in some instances, be enough to discourage an intruder from further efforts. If an attacker is using a shield such as a relay site (need to define?), then the message can still be sent to the relay site's administrator. Even if the attacker doesn't get the cease and desist message, someone who manages that site can still take action, such as revoke the privileges of the offending User ID or otherwise tighten-up security.

Sometimes someone outside your organization can be valuable in helping to detect an incident. For example, if a web page were to be modified by hackers, and then noticed by a potential customer. In an indirect way, this solicits outsiders to assist with information security. Often customers and prospects are the first to notice there is a problem. The inclusion of contact information on web pages helps outsiders to report problems. You could even add to your web site along with the contact information: "Please report any suspected security violations or problems to **{contact name}**".

Notifying Employees of Incidents

When appropriate, notify your employees of known incidents.

Evidence

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

Collecting Evidence

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

Preserving Evidence

(…)

Recording Evidence

(…)

Incident Reporting

Gather Evidence … Report it… and Be Prompt!

- ***IMPORTANT***: The most important thing to remember is to be PROMPT.

All information security suspicions and incidents must be reported as quickly as possible through your organizations proper internal channels. If problems and violations go unreported, they may lead to much greater losses for the organization than would have been incurred, had the problems been reported right away. Delays in reporting can mean massive additional losses for the organization.

Internal Reporting

This reporting structure is internal to your organization and includes the following (response team):

- security department
- Help desk
- your manager
- security guard
- information owners
- IS system administrator
- others… ?

Initially problems should be reported internally rather than externally, reducing any adverse publicity or loss announcements. External reporting should only be done an extreme emergency.

In many organizations, the help desk would then contact information security technical specialists (typically by pager).

Internal reporting could include violations of policies and other non-legal requirements.

Centralized Reporting

If is sometimes necessary to centralize the ISS department to better control ISS issues. This department may include those not on the response team.

The reporting process can be to a central group such as the Help desk as opposed to line management or a service provider. The reporting process should not always go through management, since this additional step takes longer and is likely to delay corrective actions.

Establish a centralized Information Security Department as the focal point for all reports of vulnerabilities and violations. In many organizations, these reports go only to lower level managers (such as department managers), and never find their way back to a centralized group. Unless there is centralized reporting, no loss history can be compiled, no loss analysis can be conducted, and no related decision-making can be performed. Centralized reporting is also useful for the mobilization of a computer emergency response team (CERT), an organization-wide contingency plan, and other important defensive resources. It also alleviates the reporting party's concerns about short-circuiting the chain of command.

External Reporting

Information describing information security problems is valuable, certain government regulations (such as those pertaining to commercial banks in the United States) now require the reporting of information security problems to government regulators.

(Note: You must report incident to state patrol and then they may accelerate it to the FBI. Most organization's will not go directly to the FBI.)

If criminal action is suspected, the organization must contact the appropriate law enforcement and investigative authorities as quickly as possible.

While internal reporting is to be encouraged and required, external reporting is sometimes necessary and includes the following:

- law enforcement, police
- fire department
- FBI
- external auditors
- outside authorities
- local and national organizations.
-
-

(From NITC Agencies and institutions shall report potential criminal violations to the Nebraska State Patrol and the Federal Bureau of Investigation.)

If required by law or regulation, management must promptly report information security violations to external authorities. If no such requirement exists, in conjunction with representatives from the Law Department, the Security Department, and the Internal Audit Department, management must weigh the pros and cons of external disclosure before reporting incidents. Many organizations still refrain from reporting computer crimes because the public embarrassment, cost, and diversion of staff resources appear to outweigh the benefits. Benefits include setting an example to discourage other violations, giving employees the impression that management believes in the criminal justice system, and obtaining restitution. It is often desirable that management be given the ability to choose to report violations on case-by-case basis. Some organizations may wish to establish a committee that will evaluate the merits of external reporting on a case-by-case basis. As it stands, a significant number of computer crimes go unreported, and a significant number go undetected.

Incident Reporting At-a-Glance

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

Investigating Incidents

Investigating the Cause and Impact of IS Incidents

(…)

Ensuring the integrity of IS Incident Investigations

(…)

Conducting Internal Investigations

Until charges are pressed or disciplinary action taken, all investigations of alleged criminal or abusive conduct must be kept strictly confidential to preserve the reputation of the suspected party.

Whenever evidence clearly shows that your organization has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that: (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

Some organizations - instead of requiring investigations after an organization has been shown to have been victimized, investigations can be required if such acts are only suspected. Or you can require that an investigation be performed after an abuse has been noted, even if this abuse is not legally a crime; this approach of course requires that the term "abuse" be defined. An example of a computer abuse that is not a computer crime in many jurisdictions is privacy violation.

Documenting the Incident

Documenting the incident is critical for the investigation and also to track future similar attacks. Someone should be designated to the task of preparing and maintaining all incident reports.

You organization should require a written report following the initial oral report. The scope could be expanded to include "suspected problems," not just "problems and violations." The word "weaknesses" may also be used instead of "problems." While internal reporting is to be encouraged and required, external reporting is not encouraged unless necessary.

Incident Reporting Form

You employees should have an Incident Reporting Form to capture the events they witnessed. (See attachment for sample form?)

Incident Reporting Checklist

(…)

Incident Reporting Retention

Information describing all reported information security problems and violations must be retained for a period of {3} years.

Certain important information security related information must not be destroyed. It can be helpful when doing risk assessments, when planning information security projects, and when developing budgets. It may also be useful for prosecution or disciplinary actions. The applies to computer logs and internal correspondence, as well as notes from secret investigations, "unless approved in advance.

Incident Follow Up

You must follow up on all reported incidents or suspicions. Without a good follow up process in place, you will discourage your employees from future reporting.

Enforcement

Enforcement is sometimes difficult in a working environment, but without enforcement the policies and procedures you have put in place with your ISS program may not be taken seriously.

What if an employee violates a Rule?

It is up to your organization to determine how and when to take action onan employee that has violated a Rule. Even if the violation was an accident, you may still want to take action in the form of a warning or other corrective activity.

Legal Responsibility

Perpetrators of crime should be prosecuted by the organization to the full extent of the law. Suitable procedures are to be developed to ensure the appropriate collection and protection of evidence for these purposes.

In order to prosecute successfully, you need proof. This can be difficult to provide unless your organization's information systems have adequate controls and audit capabilities.

(For non-criminal attacks, your organization should …)

Chapter 6
Implement an Awareness Program

What is ISS Awareness?

Information Systems Security (ISS) awareness is an important part of any security plan or program. Employees at all levels need to understand that they play a large part in protecting their organizations information assets. Awareness teaches employees that they are a key piece of the total security environment. Through training and on-going reinforcement, everyone will begin to "Think Security" as a matter of daily practice. Only with full support and cooperation of all employees can a successful ISS program be established and maintained.

While training is sometimes one of the first items to feel the budget pinch, its importance is acknowledged and supported not only as one of the seven security principles adopted by the Nebraska Information Technology Commission, but it is also a requirement for HIPAA compliance. An awareness program process has two major parts:

- awareness briefing (initial rollout)
- continuous awareness materials

Awareness Briefings

Before granting access to systems, all employees should receive at least a Security Awareness information packet.

All employees should be taught the importance of information security, what the rules are that must be followed, and what to do if there is a violation. An ISS awareness program is critical to any ISS program design. Increased awareness increases the proper use of security principles and the likelihood that suspicious activities will be noticed and reported.

ISS policy and standards are ineffective if individuals at any level of the organization are unaware of the importance of security policy, do not understand established standards or fail to perform required practices for any reason. Good security is "a state of mind" that can best be achieved by a program or process that reinforces the concern and appropriate actions on a regular and ongoing basis.

Continuous Awareness Materials

Information Security is not a one-time event, nor is it a "volume of rules sitting on the shelf". Good security practices are not always obvious, intuitive or easily incorporated into established routines. To have maximized effectiveness information security standards must be known, understood, believed to have value, and appropriately and consistently practiced.

A program that offers continuous reinforcement of the organizations position with regard to handling the many aspects of ISS provides the tone and commitment to support greater sensitivity to the potential of an unwanted compromise or loss of assets.

On-going and positive reinforcement for the necessity for information security policy and standards provides awareness and a "mind set" that encourages the intended practice of the established procedures. Without such reinforcement, policies or standards may be perceived as not relevant, necessary, or valuable and may be "followed" but not be practiced in a manner that supports full effectiveness.

The following are suggestions for ways to keep your awareness program alive:

- Refresher classes
- Regular updates to materials
- Top management communications to staff
- Conduct regular readiness drills
- Poster reminders

As technology and business needs change, the program will need to be revamped accordingly. Awareness never ends.

What is an Awareness Program?

An ISS awareness program brings ISS to a personal level. Everyone is responsible for the security of the information they use. The purpose of an awareness program is to teach the audience how to incorporate the rules and procedures into their daily operations.

Two awareness programs have been included in this template package:

- Computer User Awareness – broad based awareness for all employees/ contractors
- IS Awareness – focused awareness on the technical security issues

Incorporating your Awareness Program

ISS awareness can be incorporated into the following workshops:

- Initial ISS program rollout
- Continuous awareness refresher courses
- New hire orientation
- New hire package

Security is Everyone's Business

ISS is every worker's duty on a day-to-day basis. Specific responsibility for information security is NOT solely vested in the Information Security Department. Information security is multi-departmental, multi-disciplinary, and multi-organizational in nature.

This means that information security cannot possibly be adequately addressed by a single department within your organization. Thus every worker must do their part in order to achieve appropriate levels of information security. After all, information can be found nearly everywhere in the organization and nearly every worker utilizes information in order to do their job. It is only natural that every worker should be specifically charged with responsibility for information security.

Security and Performance Reviews

Some organizations may want to go one step further and incorporate a question into performance review forms. The question could read something like this: "Does the employee observe information security policies in the course of his/her work?"

This must be supplemented with additional instructions, telling workers exactly what is expected of them.

Signed Agreements

Without confirmation that all new and existing employees are aware of security policy there is no assurance that the desired actions are understood or followed. Failure to follow policy or practice standards for any reason reduces the value of such statements to "documents of prosecution" and negates the positive reinforcement and protective intent for which the information policy and standards exist.

Some organizations require users to sign a statement that they agree to: (*See Appendix for samples.)*

- abide by information security policies and procedures. A signature on a form with this statement, and perhaps a summary of the policies and procedures, can be required before a user is given a user-ID and a password.

- their understanding of the code of conduct by annually signing a form acknowledging that they agree to subscribe to the code. The intention is to annually remind employees that they must abide by the organization's code of conduct. From a legal standpoint, it is desirable to have employees acknowledge in writing that they have read and understand that a code of conduct is a required part of their job. If they are subsequently terminated due to code of conduct related problems, there is no doubt that the employee understood what was required of him or her. This agreement therefore reduces the probability of a wrongful termination lawsuit.

- to provide evidence that every employee has attended ISS class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions. For existing employees, a modification of this agreement could state they must attend within **{6}** months of the date when such courses become available.

- Every worker must understand the ISS rules and procedures and must agree in writing to perform his or her work according to such rules and procedures.

- All employees with access to computer systems must be informed of security policies and procedures and their responsibilities in writing. All new employees with access to critical systems or sensitive information will sign a statement acknowledging they have received and read the policy and understand their responsibilities. This should include knowledge of the consequences of violations of security procedures.

- A signed statement indicating awareness, compliance and intent of continued compliance with information security policy and standards will be required upon annual review of each employee with access to critical systems or sensitive information.

- Contractors, agents acting on behalf of the state, auditors, and other non-employees in a position to impact the security or integrity of information

assets of the state will be made aware of the Information Security Policy. These individuals must sign a statement acknowledging they have received and read the policy and understand their responsibilities.

Mandatory Awareness Training

ISS training should be mandatory. Every worker must attend an information security awareness class within {3} months of the date of employment. To provide evidence that every employee has attended such a class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions.

Awareness Applies to Everyone

All workers (employees, consultants, contractors, temporaries, etc.) are required to receive the same level of ISS awareness and training. This training requirement should be included as appropriate in all contracts. Workers must be provided with sufficient training and supporting reference materials to allow them to properly protect your organizations information resources. Management must allocate sufficient on-the-job time for employees to acquaint themselves with the organizations security rules, procedures, and related ways of doing business.

What makes up an Awareness Program

Your awareness program can be delivered in many ways. Initially, when you rollout your ISS program, it is suggested that you offer awareness training in a classroom environment. A classroom environment with a standardized curriculum gives a consistent message to all attendees and encourages interaction and discussion.

An awareness program can consist of the following:

- Campaign
- Training
- Materials

Awareness Campaign

An awareness campaign is a good way to initially incorporate the ISS program. A campaign can "advertise" that the ISS program is coming soon and with good promotional items, you can gain employees attention, emphasize key points, and even educate them on key security issues.

Campaign Mottoes/ Themes

You may want to start a theme that identifies the ISS program or the awareness program itself. For example: call the training class "Security 101", or "Think Security" .

The T.E.A.M. approach (Together Everyone Achieves More) is also effective to bring everyone together as one complete ISS program and the concept that we will have to all work together to make it a success. Everyone is responsible for the security of the information they use.

Campaign Ideas

- Stage vulnerability demonstrations.
- Give small prizes (i.e. free lunch) for exemplary staff (i.e. reported a violation)
- Give "traffic ticket" warnings reflecting policy statement violations. (due it when they are all out for a drill, ….)
- Initiate an unannounced "unauthorized software duplication" inventory where PCS are checked for illegal software.
- Adopt an annual ISS day on with special educational materials and events.
- Develop a "tagline" or theme that represents ISS at your organization.

Awareness Materials

The template package prepares your ISS program materials. You may need to develop additional training materials, checklists, and such for your organizations particular needs.

Suggested awareness materials:

Reference Rule Guide (results from templates)
Training Guide (results from templates)
E-mail messages
Articles in your organizations newsletter
Magazines, internet articles for circulation
Bulletins and alerts
Posters
FAQs
Web announcements
Labels for system (PC), diskettes, etc.

Awareness Training

The best way to educate your employees on ISS awareness is in a training classroom environment. The curriculum for the class can follow the same sequence as the guides you created from the templates.

Training Purpose

To teach the attendees how to recognize security issues, to be involved in the overall security of the organization, and to know what to do if they encounter an incident.

Training Specs

- Self-teaching or classroom
- Informal, workshop, seminar
- Role playing
- Stage mock incidents to see responses
- On-the-job training

Other Special Training Topics

There may be additional training classes needed for some specialty ISS areas. These are areas that require getting deeper into the topic content for certain computer users that have a special need. These specialty classes may be:

- Remote access — You must complete an approved remote systems access training course prior to being granted privileges to use dial-up, Internet, or any other remote access data communications system.
- Copyright — ?

Training Materials

For classroom awareness training, you may want to create the following class materials:

- Training Guide (from templates)
- Handouts
- Overhead slides
- Exercise workbook
- Quiz (to measure results)
- Practice sessions (do mock security drills)
- Presentation tools
- Class Evaluation
- Classroom posters
- Giveaways – buttons, pens, certificates, t-shirt's, mouse pads, …

Training Audience

The training audiences can be very general or very specific to a certain job taks. The following lists the main audiences Guides that requires ISS awareness training.

Management

Management at any level many require a different view of ISS business practices. Upper level management may need simply an executive overview, while middle management and user department management may need to know more about prevention, detection, and incident reporting.

Although management is a separate audience, the materials and curriculum are a subset of the Permanent Staff course.

Permanent Staff

The largest of all audiences, the permanent staff audience requires a unique training class and can use the *Computer User's Security Handbook* template to produce the training manual.

Temporary Staff

The temporary staff audience may not need as much training as the permanent staff since HR issues and such do not apply. They are not necessarily a separate audience, but are a subset of the Permanent Staff course. They could also be combined/ incorporated with Permanent Staff.

Contractors, Agents, Auditors and non-Employees

See Temporary Staff (above).

Technical Staff/ Management

This is a highly specialized and separate audience from the Permanent Staff group. They require a unique training class and can use the *IS Technical Staff Handbook* template to produce the training manual.

Security Officer/ Staff

The security department consisting of a security officer and security staff is a separate audience and they require a unique training class and can use the *Security Officer Instruction Guide* to produce the training manual.

Working Papers and Checklists

1. Who do you want to make aware of ISS …

ISS Topic	Audience	Class

2. For each audience, define the curriculum agenda.

Computer User Agenda

- About ISS
- Rules
- Procedures
- Questions and Answers
- Quiz
- …

IS Technical Staff Agenda

- About ISS
- Rules
- Procedures
- Questions and Answers
- Quiz
- …

Chapter 7
Getting Help with the ISS Program

About Getting Help

(describe high level)

Call for Support (?)

(Notes. What do they do if they need help understanding the templates? Call xxx-xxx-xxxx for assistance …?)

Troubleshooting the Template

Problem/ Question	Explanation	Action
What should I do if …	You are not ..	1. 2. 3.

Appendix

Appendix A - Attachments

NITC Security Architecture Document

Policies from Other agencies (already developed by other agencies, refer to them in the details of the content))

IMS Charter – project level

Appendix B - Reference List

The following resources were used to gather the information contained in this template package:

"Information Security - Protecting the Global Enterprise" by Pipkin

"Inside Internet Security - What Hackers Don't Want You to Know" by Crume

…

Index