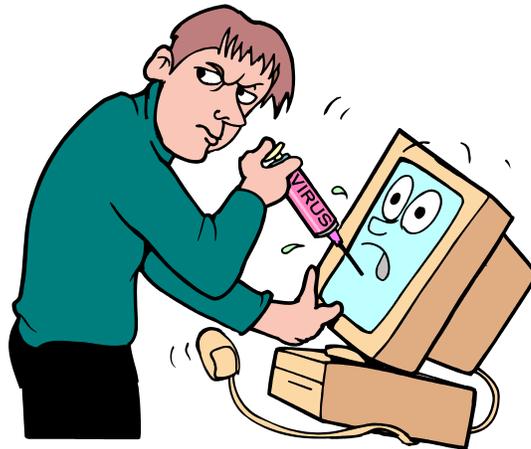


State of Nebraska
Information Security Systems (ISS)



Security Officer Instruction Guide

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

December 31, 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>

Security Officers Instruction Guide

Version 1.0
December 31, 2001

Prepared by:

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

Table of Contents

Chapter 1 Getting Started	1
The Importance of an ISS Program	1
Securing Information in the Digital Age	1
What makes up a good ISS Program?	2
About your ISS Project	2
About the ISS Template Package	3
What are Information Security Templates?	3
What makes up the Template Package?	3
Technology Dependent.....	3
Information Security Template Characteristics	4
Assumptions	4
Information Security Template Requirements	4
Initial vs. Existing Guides	5
Using the Template for Initial Setup	5
Using the Template to Update existing Manual	5
ISS Policies and Procedures	5
Policies, Standards, and Rules	5
Procedures	5
About the Security Officer Instruction Guide	7
About this Guide	7
Security Officer Policies and Rules.....	7
The Template Process	13
Assemble a Security Team	13
Conduct Business Impact Analysis	13
Publish Rules (using the templates).....	13
Implement an Incident Program	13
Implement an Awareness Program.....	13
Chapter 2 Assemble a Security Team	15
The Security Team	15
Security Day-to-Day.....	15
Security Advisory Committee(s).....	15
Incident Response Team.....	16
The Security Officer	17
Appointing the Security Officer	17
The Activities of the Security Officer	17
Security Officer Training	18
Security Staff	20
Security and the IS Department.....	20
Security Guards	20
Copyright Contact	20
Security Auditors	21
Security Audits	21
What should you audit?	21
Daily Audit/ Tracking Logs.....	22
Chapter 3 Conduct Business Impact Analysis	25
About Business Impact Analysis	25
Business Impact Analysis Process.....	25
The Business Impact Analysis Process	25
The Business Impact Analysis ProcessThe Qualitative Approach.....	25
The Qualitative Approach	26

Information Technology Inventory.....	26
What are Information Assets?	26
Assets Types.....	26
About Each Asset	29
Classifying Information Assets.....	31
What is classifying information?	31
Application vs. General Systems.....	32
What should you protect?	32
Security Classification Levels	32
Classification Levels	32
Reclassification	33
Assigning Values to Assets.....	35
About Asset Values	35
Calculating the Loss Impact	35
Loss Impact Calculation(s).....	35
Integrity Scale.....	36
Unavailability Scale	36
Disclosure Scale	36
Cost \$ to Replace.....	37
Calculating the Value	37
Value Calculation	37
Threats and Risks to Assets.....	38
Asset Threats	38
Threat Types.....	38
Threat Likelihood.....	39
Threat Impact	39
Asset Risks	40
Calculating the Risk Factor	40
Risk Factor Calculation	40
Acceptable Risk Rating.....	41
Safeguards and Assets.....	42
What are Safeguards?.....	42
Safeguards Types	42
Assigning Safeguards	42
Recalculate the Risk Factor.....	43
Assume the Residual Risk	43
Safeguard Costs.....	43
Implementing and Testing Safeguards	44
Safeguard Tools.....	44
Chapter 4 Publishing the Rules.....	47
About Publishing ISS Rules.....	47
Using the Templates to Publish your Rules.....	47
Writing in the Templates	48
Communication and Addressing your Audience.....	48
Templates Design and Organization.....	48
Modular Documentation.....	48
How are the Rules Organized?	48
Updating Text.....	48
Technology Dependent Areas	48
Template Mechanics.....	50
MS Word Features Used	50
Underlined Words	52
Rule Statements	54
Maintaining Rules	54
Adding a Rule.....	54
Rule Formats	54

Condensed Format.....	54
Full Format.....	55
Full Format Rule Fields.....	56
Assigning Priorities to Rules.....	56
Template Parameters { }.....	57
Completing the Templates.....	60
About Completing the Templates.....	60
The Sections of the Template(s).....	60
Chapter 5 Implement an Incident Program.....	63
What is an Incident Program?	63
Suspicious and Incidents.....	63
Suspicious and Incidents	63
Prevention	64
Detection.....	64
Intrusion Detection Methods	64
Tracking Intrusions.....	64
Incident Patterns.....	64
Response/ Reaction.....	65
Your Incident Response Team	65
Incidents Response Centers.....	65
Catastrophic Event	65
Secured Area Intrusion.....	65
Virus Reporting	66
Electronic Intrusion	66
Unauthorized Access Intrusion.....	66
Notifying the Intruder – yes or no?	66
Web Site - Contact Information	66
Notifying Employees of Incidents.....	67
Evidence.....	67
Collecting Evidence	67
Preserving Evidence.....	67
Incident Response.....	67
Gather Evidence ... Report it .. and Be Prompt!	67
Internal Response	68
Centralized Response	68
External Response	68
Investigating Incidents	69
Conducting Internal Investigations.....	69
Documenting the Incident	70
Incident Reporting Form	70
Incident Reporting Retention	70
Incident Follow Up.....	70
Enforcement	71
What if an employee violates a Rule?	71
Legal Responsibility.....	71
Incident Handling.....	71
Chapter 6 Implement an Awareness Program.....	75
What is ISS Awareness?	75
Awareness Briefings.....	75
Continuous Awareness Materials	76
What is an Awareness Program?.....	77
Incorporating your Awareness Program.....	77
Security is Everyone’s Business.....	77
Awareness Applies to Everyone.....	77
Security and Performance Reviews.....	77

Mandatory Awareness Training	78
Signed Agreements.....	78
What makes up an Awareness Program	80
Awareness Campaign	80
Campaign Mottoes/ Themes.....	80
Campaign Ideas	80
Awareness Materials	81
Awareness Training.....	81
Training Purpose	81
Training Logistics.....	81
Other Special Training Topics.....	82
Training Audience.....	82
Management.....	82
Computer User (permanent staff)	82
Computer User (temporary staff).....	82
Contractors, Agents, Auditors and non-Employees.....	82
Technical Staff/ Management.....	83
Security Officer/ Staff	83
Chapter 7 Getting Help with the ISS Program.....	85
About Getting Help	85
Call for Support (?).....	85
Troubleshooting the Template.....	85
Appendix.....	87
Appendix B - NITC Security Architecture Document	87
Appendix C - Reference List	87
Index.....	89

Chapter 1

Getting Started

The Importance of an ISS Program

Information Systems Security (ISS) has become more and more important to organizations of all industries worldwide. ISS is much 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 evaluated and protected accordingly.

It is the purpose of this guide to help the security professions implement an ISS program throughout their organization. It provides the instruction and materials necessary to roll out an awareness program and publish a set of security policy and procedures. It is independent of any technology, but gives you the structure to customize and enter your technical details.

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 upon their services.

Chapter 1 - Getting Started

What makes up a good ISS Program?

What do you need to put the right security practices into your organization's business operations?

Consider incorporating the following into your ISS program:

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

Each of these components is included in this ISS program package. They are designed to be modular in their procedures, so you can do one or all of them.

About your ISS Project

It is important that the security officer/ team get 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 Project Charter in Appendix.*

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 organization's technology-specific instructions. The template structure was

Chapter 1 - Getting Started

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

Information Security Template Characteristics

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

Assumptions

- ◆ Knowledge of basic security practices
- ◆ Knowledge of MS Word

Information Security Template Requirements

- ◆ Office 2000. If you do not use Office 2000, you may experience problems.

Initial vs. Existing Guides

Using the Template for Initial Setup

Once you have installed the templates, you can use the procedures in *Chapter 4* to customize the content.

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. *See Adding a Rule in Chapter 4.*

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 published 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*

Chapter 1 - Getting Started

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 organization’s 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
- How to assemble a security team
- How to conduct a business impact analysis
- How to do an information asset inventory
- How to do a threat / risk assessment
- How to value asset inventories
- How to determine loss impact of assets
- 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

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.

Security Officer Policies and Rules

There are many rules throughout the template package that are the result of the NITC published policies. Below we review the 7 policies adopted by the NITC.

Policy - Information Security Management

Owners of systems must determine how critical and sensitive information is and must adopt and implement comprehensive security programs that offer a level of protection commensurate with the value of the asset. Information security programs must provide reasonable protection against unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. This applies to all systems that gather, generate, and store data.

Policy - Access Control

Access Control protects information by managing access to all entry and exit points, both logical and physical. Adequate perimeter security and logical security measures must protect against unauthorized access to sensitive information on a governmental facility, network, or application. These measures ensure that only authorized users, as determined by each governmental entity, have access to specific computer resources, networks, data, and applications.

Policy - Disaster Recovery

Each agency (organization) must have a disaster recovery plan that at least identifies and militates against risks to critical systems and sensitive information in the event of a disaster. The plan should provide for contingencies to restore information and systems if a disaster occurs. The disaster recovery plan for information technology may be a subset of an organization's comprehensive

Chapter 1 - Getting Started

disaster recovery plan. The concept of a disaster recovery focuses on business resumption.

Ⓟ Policy - Education, Training, Awareness

The information security policies and procedures of the agency or institution will be communicated to all employees. Information security policy and procedures will be available for reference and review by employees, contractors, agents acting on behalf of the state and all others in a position to impact the security and integrity of the information assets of the state. A program to maintain effective awareness of information security policy, standards, and acceptable practices will exist. Persons responsible for information technology resources must have adequate training on implementing proper security controls for the equipment, software, and networks under their control.

Ⓟ Policy - Individual Use

Agencies and institutions must adopt policies governing the use of computer and communication facilities by individuals. Like all communications conducted on behalf of the State of Nebraska, users must exercise good judgment in internet, e-mail, and other actions must always be able to withstand public scrutiny without legal liability or embarrassment to the agency or institution.

Ⓟ Policy - Network Security

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

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

Ⓟ Policy - Security Breaches and Incident Reporting

Agencies and institutions shall prepare procedures for monitoring, investigating, and reporting security breaches and incidents. Security breaches shall be investigated promptly and documented. If criminal action is suspected, the agency or institution must contact the appropriate law enforcement and investigative authorities as quickly as possible. Agencies and institutions shall cooperate with

local and national programs for reporting security incidents. The policies and standards pertaining to access controls, acceptable use, education and network security shall apply.

The following rule applies to the security officer, not the computer user or IS technical staff, so it is incorporated into this guide.



Rule - Incident Response and Reporting Procedure for State Government

Rule Statement	
State Agencies shall prepare procedures for reporting security breaches and incidents. Documentation on security incidents shall be filed with the Chief Information Officer for the State of Nebraska.	

Policy Category Security Breaches and Incident Reporting Policy		Policy Standard Incident Response and Centralized Reporting		Rule Number	
Rule Date		Rule Revision Date 09/27/01		Date Adopted	
Approval Name/ Code (signature) NITC		Rule Source		Audit Number/ Code	

Explanation/ Key Points

Security is a growing problem. Effective response and collective action are required to counteract security violations and activities that lead to security breaches. Agency management, law enforcement, and others must know the extent of security problems in order to make proper decisions pertaining to policies, programs, and allocation of resources. Responding to security alerts will help to preempt incidents from occurring. Quick reporting of some incidents, such as new viruses, is essential to stopping them from spreading and impacting other systems. Reporting computer crimes is the only way for law enforcement to deter and apprehend violators.

Effective response to security incidents requires quick recognition of problems and fast mobilization of skilled staff to return systems to normal. This requires prior documentation of procedures and responsibilities of everyone with a role in responding to the emergency. Continuous improvement by eliminating points of vulnerability and applying lessons learned is an essential component of incident response.

Centralized reporting serves the goal of increasing awareness of vulnerabilities and threats to state government as a whole. In particular, centralized reporting is necessary to discern patterns, identify areas of vulnerability, allocate resources, and develop statewide solutions. Centralized reporting does not substitute for internal reporting to management, reporting to law enforcement, or mobilizing a computer security incident response team (CERT). Agencies should develop procedures for internal and external reporting that will meet the needs of centralized reporting

Chapter 1 - Getting Started

with little or no additional work. The centralized reporting is designed to mesh with the postmortem analysis that should follow each incident.

The ultimate goal of security incident response and centralized reporting is to protect data and prevent obstruction of government operations.

Applicability

All non-education state agencies, boards, and commissions, which receive a direct appropriation from the Legislature or any state agency that has a direct connection to the state's network. Educational institutions and other entities are encouraged to develop their own security incident and centralized reporting procedures.

Step-by-step Procedures

The incident Response and Centralized Reporting Procedure for State Government requires that the agency implement the following steps for a complete security incident handling process.

1. Establish general procedures for responding to incidents;
2. Prepare to respond to incidents;
3. Analyze all available information to characterize an intrusion;
4. Communicate with all parties that need to be made aware of an incident and its progress;
5. Collect and protect information associated with an incident;
6. Apply short-term solutions to contain an incident;
7. Eliminate all means of vulnerability pertaining to that incident;
8. Return systems to normal operation;
9. Closure: Identify and implement security lessons learned.

Step 1 should include establishing a computer security incident response team (CSIRT) that can take responsibility for managing security incidents. The CSIRT can be a virtual team that includes people with a wide range of expertise. Agencies should consider forming a CSIRT that serves multiple entities. A clear description of roles and responsibilities is essential.

Step 2 should include methods for placing the CSIRT on alert status and ready to take preventative measures. It should include procedures for activating the team once an incident occurs.

Step 4 includes contacting users affected by an incident, security personnel, law enforcement agencies, vendors, the CERT Coordination Center (<http://www.cert.org/>) and other CSIRTs external to the organization. It is essential that each agency establishes and follows a single channel of communication. Multiple sources of information while the incident is underway creates confusion, interrupts the work of the response team and increases vulnerability if the perpetrator is monitoring communications within the agency.

Step 9 "Closure" is intended to give the organization an opportunity to learn from the experience of responding to an incident. Every successful intrusion or other incident indicates potential weaknesses in systems, networks,

operations and staff preparedness. These weaknesses provide opportunities for improvement. Steps should include the following points (from CERTCC security practices, <http://www.cert.org/security-improvement/practices/p052.html>):

1. Hold a post mortem analysis and review meeting with all involved parties. Do this within three to five working days of completing the investigation of an intrusion. Use the attached reporting form to gather information and guide discussion.
2. Prepare a final report for senior management and the Office of the CIO. This ensures awareness of security issues. Use the attached form (or online version) to report information about the security incident to the Office of the Chief Information Officer. Incidents should be reported no later than 5 working days after returning systems to normal operation.
3. Revise security plans and procedures and user and administrator training to prevent future incidents. Include any new, improved methods resulting from lessons learned.
4. Determine whether or not to perform a new risk analysis based on the severity and impact of an intrusion.
5. Take a new inventory of your system and network assets.
6. Participate in investigation and prosecution, if applicable.

Terminology

Agency	As used here, an agency is any non-educational agency, board or commission, which receives a direct appropriation from the Legislature.
Security Incident	<p>A security incident includes, but is not limited to the following events, regardless of platform or computer environment:</p> <ol style="list-style-type: none">1. Evidence of tampering with data;2. Denial of service attack on the agency;3. Web site defacement;4. Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources);5. Social engineering incidents6. Virus attacks affecting servers or multiple workstations;7. Other incidents that could undermine confidence and trust in the state's information technology systems.

Related Rules

Draft security standards for the federal Health Insurance Portability and Accountability Act (HIPAA) would establish administrative procedures to guard data integrity, confidentiality, and availability. These include security incident procedures (45 CFR Part 142.308 (a)(9):

Chapter 1 - Getting Started

“(9) Security incident procedures (formal documented instructions for reporting security breaches) that include all of the following implementation features:

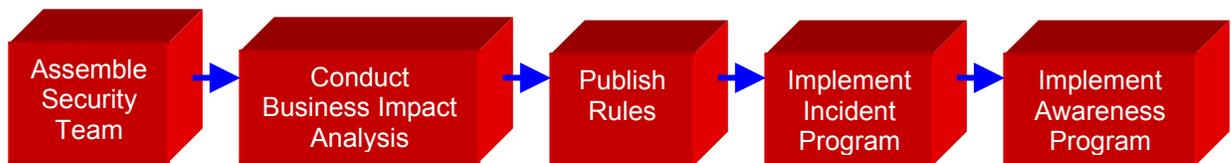
- (i) Report procedures (documented formal mechanism employed to document security incidents).
- (ii) Response procedures (documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report).”

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

Initially you must build your security team. You cannot have a successful incident response program and conduct a business impact analysis without the right team. Your awareness program will emphasize the results of your analysis and incident response program.

Assemble a Security Team

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.*

Publish Rules (using the templates)

It is important that you publish ISS rules and procedures for all computer users and technical staff. Keeping ISS visible and alive requires materials and guides for on-going support. *See Chapter 4 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 critical. *See Chapter 6 for complete details.*

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

Chapter 2

Assemble a Security Team

The Security Team

Responsibility for information security is everyone's duty as it affects every department and every person in an organization. Information appears everywhere in an organization, and almost every worker uses information to do their job.

In addition to having aware employees, it may also be necessary to have a security team that concentrates on protecting and monitoring systems. There may be several security teams:

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

Security Day-to-Day

Protecting and monitoring information security is a daily task. There are security administration tasks that involve new authorizations and access controls. Security monitoring involves checking logs and intrusion reporting systems, and reviewing plans and procedures as needed.

Checking critical reports and system usage is one of the most important daily tasks. A good set of procedures should be put in place to effectively manage the security function(s).

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 officer coordinates this effort.

Each organization should also select a member for the incident response, or Computer Emergency Response Team (CERT). This CERT team provides assistance and gets involved with your organization in the event of an incident.

Chapter 2 - Assemble a Security Team

Incident Response Team

Each organization should assemble an Incident Response Team to handle all suspicions and incidents. This team may be some of the Security Advisory Committee members.

ⓘ *Important !* It is critical that someone on the incident 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.

The Activities 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
- ◆ 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

Chapter 2 - Assemble a Security Team

- ◆ 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:

Chapter 2 - Assemble a Security Team

- MISTI
- SAN
- The Computer Security Institute
- ... and many others.

Conferences are held throughout the year nationwide. The following are recommended:

- CERT
- InfoSecurity
- IBM Global Services
- InfoWar
- WebSec
- RSA
- Black Hat Briefings
- ... and many others.

Certifications can be received in:

- CISSP
- CISA
- ... and many others.

Chapter 2 - Assemble a Security Team

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.

 **Tip:** 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 another 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.

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 organizations 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.

It is not the intent of this guide to give instructions on doing an information security audit, however, this section is dedicated to listing ideas and examples of the types of reporting and logs you could produce to audit your security operations.

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 (For example: # user 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 Log on 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 on once a month to keep token synchronized with the Citrix. Automatically expires battery – forced to replace it.

Chapter 2 - Assemble a Security Team

Daily Audit/ Tracking Logs

Logs, or reports should be used to manage and monitor activity on your system. The following logs are recommended:

- Logs Required On Application Systems Handling Sensitive Information
- Keystroke Logs Required For All Production System Privileged User-Ids
- Security Relevant Events In System Logs
- Computer System Logs Must Support Audits
- Accountability And Traceability For All Privileged System Command
- Contents Of Logs For Systems Running Production Applications
- Required Retention Period Of Logs
- Daily Removal Of Logs From Internet-Accessible Computers
- Logs Of User-Initiated Security Relevant Activities
- Retention Of Access Control Privilege Logs
- Reconstructibility Of Changes To Production Information
- Information To Capture When Computer Crime Or Abuse Is Suspected
- Logs Required For Rapid Resumption Of Production System Activities
- Systems Architecture For Logging Activities
- Clock Synchronization For Accurate Logging Of Events On Network
- Logs Of All Inbound And Outbound Faxes
- Resistance Of Logs Against Deactivation, Modification, Or Deletion
- Writing Logs To WORM Storage Media Prevents Alteration
- Persons Authorized To View Logs
- Regular And Prompt Review Of System Logs
- Notification Of Users About Logging Of Security Violations

Suggested logs by User ID:

1. Log on 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.

Procedure #1 How to assemble Security Team(s)

Use: Working Paper #1

1. Review the list of the ISS Tasks in *Chapter 2* and *Working Paper #1*. Add, modify, delete ISS Tasks.
2. For each task, assign the Agency / Department responsible for completing the task. Example: IM Services could be entered for any agencies that use the services of IM Services to do that task.
3. For each task, assign the Division/ Unit responsible for completing the task. Example: IS Department
4. For each task, assign a name of the person(s) responsibility for completing the task.
5. For each person(s), enter their position.
6. Is this person(s) also a member of the Security Advisory Committee (SAC)? Y or N
7. Is this person(s) also a member of the Incident Response Team (IRT)? Y or N
8. Identify day-to-day security team.

You have now identified your ISS TEAM!

Chapter 2 - Assemble a Security Team

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

Chapter 3

Conduct Business Impact Analysis

About Business Impact Analysis

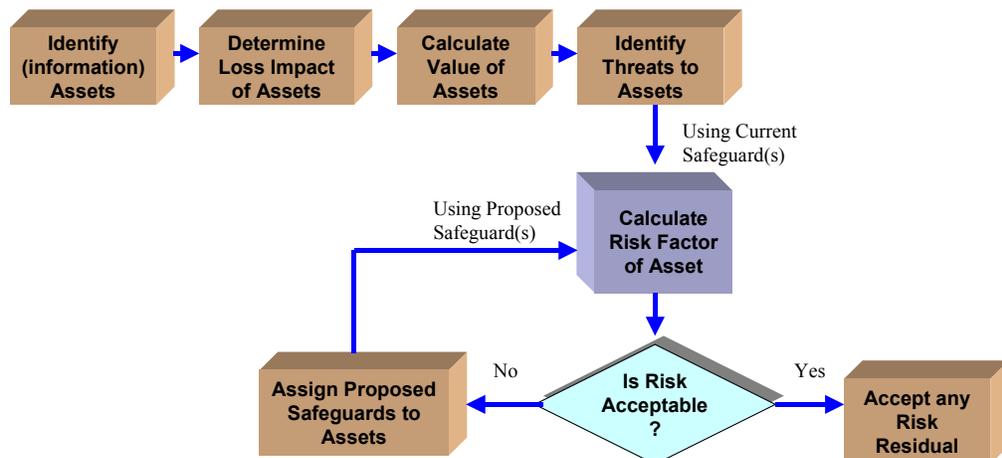
Now that you have assembled your security team, you can begin the process of creating your information inventory. This step performs an organization wide business impact analysis study of your information assets.

This chapter will guide you through the process of conducting a business impact analysis study. You have been provided with the necessary working papers and procedures to capture and organize this task.

Business Impact Analysis Process

The steps outlined in this template package guide you through the business impact analysis process.

The Business Impact Analysis Process



The Business Impact Analysis Process

Chapter 3 - Conduct Business Impact Analysis

The Qualitative Approach

There are many ways to conduct a business impact analysis of your information assets. The approach used in this template package is *qualitative* in nature.

Working with a qualitative approach means you should not attempt to assign numeric values to the exact dollars and cents. Qualitative approaches are often associated with measuring in terms of quality as indicated through a scale or ranking. It relies on scenarios and is subjective. As long as you are consistent and measure all assets using the same strategy, then the exact dollar figure does not matter.

Quantitative approaches, however, are still widely used, but require more extensive research in getting to exact figures and balancing totals. It is often associated with measuring in terms of dollars and cents and attempts to assign independently, objective numeric values (ex. monetary) to the components of the analysis.

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 even if they are a low priority, low risk, or easy to replace.

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 organization.

Assets Types

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

 **Tip:** You should have a log/ report that lists the following assets within their asset types. Many projects revolve around this type of log.

This template package uses the following asset types to group your information inventory. It is suggested you do all asset types, however, they are modular and can be done exclusively of each other.

Chapter 3 - Conduct Business Impact Analysis

- Platform
- Applications
- General Software
- Hardware
- Communications

Platform

If you want to safeguard your assets at the platform level, you do not need to itemize all systems. For example, all applications might be safeguarded the same way at the platform level. You could list them here at the platform level so they are accounted for, but you would safeguard them collectively at the platform level.

Applications

You may want to value/ safeguard your information by business application. For example, if you want to safeguard the payroll application higher than general information applications, you would need to list business applications, their classification, and resulting safeguards.

Applications include both the data and the programs that run the application. All applications should be grouped here regardless if the software is purchased, rented, in-house developed, or third party.

Typically applications are identified by business purpose like payroll, general ledger, purchasing, customer service, driver's licenses, e-mail, and such.

General Software

The general or global systems that run cross multiple applications or not affiliated with any application. These core systems may want to be separated from applications and protected in a different fashion. This would also include software that all employees use globally as a tool in their every day work place.

This software includes operating systems, utilities, compilers, employee tools (MS Word).

Hardware

All equipment and computer hardware is grouped into this category. You would want to group it separately from software as it is not classified or safeguarded in the same way.

Chapter 3 - Conduct Business Impact Analysis

This hardware includes all processors (laptops, PCs, servers, mainframes, etc.), printers, UPS, tape drives, storage (DASD) drives, and all other equipment.

Communications

All communication points need to be safeguarded. This category also considers modems, communication lines, switches, routers, bridges, networks, and such.

Simply list the device and its quantity by model. For example:

40 IBM routers
20 IBM switches

The key questions here are “What’s connected to what?” “Who are you connected to? (ex. telephone company)”

Chapter 3 - Conduct Business Impact Analysis

About Each Asset

Location (physical or logical)

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

Inventory Number

You may want to give the asset an inventory number for auditing or tracking purposes. (Optional)

Effected by HIPAA?

Are the assets/ threats/ risks/ safeguards being dictated by HIPAA?

IM Services Supported/Owned?

Is this asset supported and owned by IM Services? If so, you do not need to include it in your Business Impact Analysis as it would be part of the IM Services ISS Program.

Storage/ space/ size

The amount of storage required to contain an asset is important to identify large applications. This may impact its value and its risk.

We recommend you use the following scale:

Scale	Storage / Size/ Space Capacity Range
25	Example: 50 gig – >
20	20 - 49
10	10 – 19
5	1 - 9
1	less than 1 gig

Users - usage and sharing

If an application is used by many users and shared, it may be more valuable.

Scale	# Users - usage and sharing Range
25	Example: 5000 – >
20	1000 - 4999
10	300 – 999
5	50 - 299

Chapter 3 - Conduct Business Impact Analysis

Scale	# Users - usage and sharing Range
1	less than 50

Owner

Each application and general software asset can 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.

Classification Scale

The classification scale represents the sensitivity of the information. For details on the classifications levels, *see Classifying Information in this chapter.*

Scale	Classification Level
25	Highly Restricted
20	Confidential
10	Internal Use Only
1	Unclassified/ Public

Classifying Information Assets

What is classifying information?

Now you are ready to classify your platform, application, or general software assets to put 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.

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

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.
- Confidentiality – describes the impact from disclosure and the protection of sensitive information.
- Integrity – reflects the severity of the damage that could be caused to the accuracy and completeness of the information and processing methods.
- Availability - urgency of the information and the systems that use it.
- Non-repudiation - proving transfer and receipt of an unforgeable electronic transaction

Chapter 3 - Conduct Business Impact Analysis

Application vs. General 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.

Applications are software systems that provide a certain purpose, driver's licenses, payroll, personnel data, financial data, and such.

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. Those that are the most critical 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

- **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

Chapter 3 - Conduct Business Impact Analysis

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.

Chapter 3 - Conduct Business Impact Analysis

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 organization’s 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 organization’s 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.

Assigning Values to Assets

About Asset Values

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.

i 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.

Calculating the Loss Impact

Taking a qualitative approach to evaluating your assets is very effective in grouping assets and applying ranges of impact losses. This saves a lot time and energy and is just as effective as getting to the exact dollars and cents. The loss impact can be based on the replacement value, the immediate impact of the loss, and the consequence.

Loss Impact Calculation(s)

Loss Impact (software) = Integrity + Unavailability + Disclosure

Loss Impact (hardware) = \$ to Replace + Unavailability

Chapter 3 - Conduct Business Impact Analysis

Integrity Scale

Integrity measures the amount (cost) of damage that could be caused to the accuracy and completeness of the information and processing methods.

Scale	Integrity Range
25	\$1,000,000,000 and >
20	\$100,000,000 - 1,000,000,000
15	\$10,000,000 - 100,000,000
12	\$1,000,000 - 10,000,000
10	\$100,000 - 1,000,000
5	\$10,000 - 100,000
4	\$1,000 - 10,000
3	\$100 - 1,000
2	\$1 – 100
1	< \$1

Unavailability Scale

The cost of unavailability involves both time and dollars. The inability to access information quickly can be devastating to many organizations. It depends on timing, duration, and the situation. For example with timing, you may not need to know something until it happens and then you need it, like how to shut down a nuclear power plant.

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

Scale	Unavailability Range
25	\$1,000,000,000 and >
20	\$100,000,000 - 1,000,000,000
15	\$10,000,000 - 100,000,000
12	\$1,000,000 - 10,000,000
10	\$100,000 - 1,000,000
5	\$10,000 - 100,000
4	\$1,000 - 10,000
3	\$100 - 1,000
2	\$1 – 100
1	< \$1

Disclosure Scale

Disclosure can be measures by its adverse effect of your organization.

Chapter 3 – Conduct Business Impact Analysis

Scale	Disclosure Impact
25	Stock price / bond rating impacted
20	Adverse national press
10	Public made aware through local coverage
5	Disclosure spread throughout your organization
2	Disclosure spread to another work area in your organization
1	Disclosure restricted to within the project or work area

Cost \$ to Replace Scale

The cost \$ to replace is the cost of recreation or replacement for hardware and communications devices only. It is the cost of purchasing, building, or having a service provide the replacement of the asset. It is both time and dollars.

If the cost of recreation is high, it must be given high rated safeguards, like redundant storage of asset, backup and recovery.

Scale	Cost to Replace Range
25	\$1,000,000,000 and >
20	\$100,000,000 - 1,000,000,000
15	\$10,000,000 - 100,000,000
12	\$1,000,000 - 10,000,000
10	\$100,000 - 1,000,000
5	\$10,000 - 100,000
4	\$1,000 - 10,000
3	\$100 - 1,000
2	\$1 – 100
1	< \$1

Calculating the Value

The value of an asset can be represented in terms of the potential loss and its effect on the business and its users. This value is used later in the asset risk factor calculation.

Value Calculation

$$\text{Value} = \text{Storage} + \text{Users} + \text{Classification} + \text{Loss Impact}$$

Threats and Risks to Assets

Asset Threats

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 and what threats need to be countered.

A threat assessment is a critical part of the business impact 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.

 **Remember:** A threat is not an incident. With a threat, no event occurred, nothing has happened.

 **Tip:** Good employee relations help to minimize threats.

Threat Types

Threats can be deliberate or non-deliberate, internal or external. The following table can be updated to reflect all threat and new attacks that could potentially occur.

Threat/ Risk Types
Hackers
Social Engineering
Competitors
Insiders – authorized
Insiders - unauthorized
Former Employees
Script Kiddies
Cybercrime
Techno-crime
Virus, worm
Trojan Horse
Time bombs, stealth bombs, logic bombs
Stealing information
Disclosure
Defacement/ destroy and ruin
Change environment
Denial of Service attack
Human error
System failures
Natural Disasters

Chapter 3 – Conduct Business Impact Analysis

Threat/ Risk Types
Others ??

Threat Likelihood

One of the main components in calculating asset risk factors is to determine the likelihood of a threat occurring to that asset. Estimating the chance that the threat will cause a loss is the main purpose. As specific threats are identified and assigned to each asset, a likelihood measure needs to be associated with the threat / asset pair.

Scale	Threat Likelihood
25	Once a day or more
20	Several times a week
10	Several times a month
5	Several time a year
1	Never

or

Scale	Threat Likelihood
25	High likelihood
10	Moderate likelihood
1	Low likelihood

Threat Impact

Impacts describe the effect of a threat on an asset. What are the immediate damages of the threat being realized? Impacts can be very specific (For example: change accounting data, falsify money transfers). The impact the threat could cause to that asset can be measured using the following scale:

Scale	Threat Impact
25	High impact. The effect is catastrophic, the company will not survive. The project will fail.
20	Medium to high impact. Significant loss to business operations or customer confidence or market share. Customers may be lost. The effect is disastrous, but the organization can survive, at a significant loss.
10	Medium impact. Business operations are unavailable for a certain amount of time, revenue is lost, customer confidence is

Chapter 3 - Conduct Business Impact Analysis

Scale	Threat Impact
	affected minimally (unlikely to lose customer).
5	Low to medium impact. Effect is minor, major business operations would not be affected.
1	Low impact. Impact is negligible.

Asset Risk Factor

A risk factor is required to understand the potential impact on information assets and to justify the expenditures on security safeguards. This 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.

Security safeguards reduce risks. 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.

Calculating the Risk Factor

The risk factor can be considered the representation of the kinds of adverse actions that may happen to information, the degree of likelihood that these actions may occur and the value of the asset. The outcome of this process should indicate the degree of risk associated with the defined value of the assets. This outcome is important because it is the basis for making safeguard selection and risk mitigation decisions.

Risk Factor Calculation

$$\text{Risk Factor} = \text{Value} + \text{Threat Likelihood} + \text{Threat Impact}$$

The total possible points for the risk factor using the scales outlined in this template package is

8 - 200 possible points

where 8 is no risk and 200 is high risk.

The levels of high, moderate, low can be normalized and used to compare risks associated with each threat. This simple methodology that looks only at loss and likelihood. You can change the scales and adjust the acceptable risk rating as your needs change.

Sometimes a risk factor that was derived from a high loss and low likelihood results in the same risk factor as one that resulted from a low loss and high likelihood. In these cases, you

Chapter 3 – Conduct Business Impact Analysis

need to decide if the risk factor derived from the high loss is more critical than the risk factor derived from the high likelihood.

Acceptable Risk Rating

All assets will have some risk attached to them. You must decide on the acceptable risk rating for your organization.

This number would be somewhere between 8 – 200. Let's say, for example, 36 is the cut off for allowable risk. All risks having a value higher than 36 are unacceptable risks which must be safeguarded.

_____ **Acceptable Risk Rating**

Safeguards and Assets

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 business impact analysis process. Once you have assigned the appropriate safeguards, you can then re-evaluate the asset and bring its acceptable risk rating to an acceptable level. Safeguards may also be called security measures, protective means, or counter measures.

All assets do not have the same potential of loss and do not require the same expenditure of protection. It is important to place the proper safeguard(s) on an asset that justifies the cost and maintenance. Remember, threats cannot be eliminated, but can be anticipated, and safeguards put in place to minimize their impact.

Safeguards Types

Safeguard Types
Firewalls
Vpns ?
Incident Monitors
Install all Patches
Intrusion Detection systems
Policies/ Rules/ Procedures
Awareness/ training
Logs - daily monitoring
Physical access means
Encryption/ disguise information
Mechanisms - password generator, token based, biometrics.
Software that will trace the source of attacks.
Block all .exe files coming in from the outside
Backup and recovery
Redundant storage of asset
New hardware
Reporting
Password protection
Others ??

Assigning Safeguards

Safeguards should be assigned based on knowledge of the threats, the loss impact and the likelihood of its occurrence. Select those effective safeguards that will reduce the risk of an

Chapter 3 – Conduct Business Impact Analysis

asset to an acceptable level. Safeguards can be used in combination and is a subjective process.

 **Remember:** You don't have to protect everything!

Recalculate the Risk Factor

After applying the proposed safeguard(s) to the asset, you must recalculate the risk factor for that asset. Is the remaining risk acceptable? The greater the risk factor, the more important it is to implement better safeguards.

Risk acceptance is described as an activity that compares the current risk factor with acceptance criteria and results in a determination of whether the current risk factor is acceptable. While effective safeguards 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.

Assume the Residual Risk

After all safeguards are determined and the results of the new risk factor have been examined, the risk factor associated with the threat/ asset relationship should now be reduced to an acceptable level or eliminated.

Your 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 must be carefully considered. 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 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.

 **Remember:** The measures taken to protect assets should correspond to the value of the assets.

Safeguard Costs

When considering the cost measure of the mechanism, it is important that the cost of the safeguard be related to the risk factor to determine if the safeguard will be cost effective. The cost of the safeguard is the amount needed to purchase or develop and implement each of its mechanisms. To calculate risk/ cost relationships use the risk factor and the cost associated with each safeguard and create a ratio of the risk to the cost. A ratio that is less

Chapter 3 - Conduct Business Impact Analysis

than 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.

Implementing and Testing 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, and user learning curve. 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 it 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.

Safeguard Tools

There are many technical tools in the market to assist in protecting your information assets. Software is available to track systems activity and trace the source of attacks.

Procedure #2

How to do a Business Impact Analysis

Use: Working Papers #2a, #2b, #2c, #2d

A. How to identify information assets:

1. Using *Working Paper #2b*, choose your information assets types: platforms, applications, general software, hardware, communications.
2. Update platforms in the Platform Table. Here you can list all applications or general software to safeguard them at the platform level and then you do not need to list them in the Applications table.
3. Update applications in the Applications Table. You do not need to list those that are accounted for at the platform level. Example: payroll, drivers license, e-mail (Lotus Notes)
4. Update general software in the General Software Table. Example: utilities, compilers, operating systems, user tools (MS Word)
5. List hardware in the Hardware Table.
6. List communications devices and entry points in the Communications Table.

For all asset types,

7. Assign a physical or logical location (optional)
8. Assign an inventory number (optional)
9. Is this a HIPAA requirement? Yes or No.
10. Is the asset IMS supported/ owned? Yes or no. If yes, do not continue with this asset. It is already accounted for, valued, and safeguarded by IM Services.

For all asset types (except communications):

11. Using Working Paper #2a, enter your ranges for the amount of storage/ disk space. Using this range, enter the scale for each asset in Working Paper #2b. *See About Each Asset section in Chapter 3.*
12. Using Working Paper #2a, enter your ranges for the number of users. Using this range, enter the scale for each asset in Working Paper #2b. This is the number of users that rely upon that asset. *See About Each Asset section in Chapter 3.*

For asset types - platform, applications, and general software:

13. Enter the owner of the asset.
14. Enter the classification scale for that asset. *See About Each Asset section in Chapter 3.*

B. How to determine loss impact of an asset:

For asset types - platforms, applications, general software:

15. Using *Working Paper #2a*, enter your ranges for cost into the Integrity Scale Table. Using this range, enter the scale for each asset in *Working Paper #2b*. *See How to Calculate Value section in Chapter 3.*
16. Enter your ranges for cost into the Disclosure Scale Table. Using this range, enter the scale for each asset in *Working Paper #2b*. *See How to Calculate Value section in Chapter 3.*

Chapter 3 - Conduct Business Impact Analysis

For all asset types:

17. Enter your ranges for cost into the Unavailability Scale Table. Using this range, enter the scale for each asset in *Working Paper #2b*. See *How to Calculate Value* section in Chapter 3.

For asset types - hardware, communications:

18. Enter your ranges for the cost into the Cost \$ to Replace Scale Table. Using this range, enter the scale for each asset in *Working Paper #2b*. See *How to Calculate Value* section in Chapter 3.

C. How to calculate the value of an asset:

For asset types - platforms, applications, general software:

19. Calculate the value = Storage + # Users + Classification + Loss Impact. This value is used later to calculate the asset risk factor.

For asset types - hardware, communications:

20. Value = Storage + # Users + Loss Impact. This value is used later to calculate the asset risk factor.

D. How to identify threats/ risks to assets:

21. Update the Threats/ Risk Types table with your organizations threat/ risk types in *Working Paper #2c*.
22. Using *Working Paper #2b*, assign a threat type to each asset.
23. Assign the threat likelihood that it will occur to that asset.
24. Assign the threat impact it will have on that asset.
25. Calculate the Risk Factor for each asset.
26. Determine the Acceptable Risk Factor for your organization.

E. How to safeguard your assets:

27. Update the Safeguards Table in *Working Paper #2d* with both current and proposed safeguards.
28. Enter current safeguard(s) for each asset from the list in the Safeguards table.
29. Enter proposed safeguard(s) for each asset from the list in the Safeguards table.
30. Recalculate the Risk Factor by reevaluating asset.
31. Enter the safeguard cost. Select cost effective safeguard.
32. Accept Residual Risk

Chapter 4

Publishing the Rules

About Publishing ISS Rules

Publishing the security rules at an organization provides the framework under which business practices develop. Distributing rules to all employees is a critical component of any ISS program and can be done at new hire orientation or during security awareness training.

Using the Templates to Publish your Rules

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
- ◆ 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 in both of the templates are security rules. You can use the entire template as it is and not change any of the rules needing to only fill in your own parameters. Or you can add, change or remove any of the template rules or other content that does not apply to your organization's security issues.

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

ⓘ Important ! 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

Chapter 4 - Using the Templates

Writing in 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.

Updating Text

All text in the templates can be edited to reflect what you want to tell your audience. Most sections are completely written, so you may not need to change the text at all if you are satisfied with the content.

There are, however, some sections that are organization-dependent, but the heading has been given to you and all you need to do is write that section for your organization's needs. These fill-in-the-blank sections you will need to edit or remove can be identified as shown below within (...parentheses...):

(...Explain the purpose of the)

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 of this template package is to provide enough information without touching on any particular technology.

 **Tip:** For technology-dependent rules, use the full format and detail the step-by-step procedure and other fields. *See Full Format section in this chapter.*

Chapter 4 - Using the Templates

Template Mechanics

The templates use basic MS Word functions. 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 an MS Word Guide.

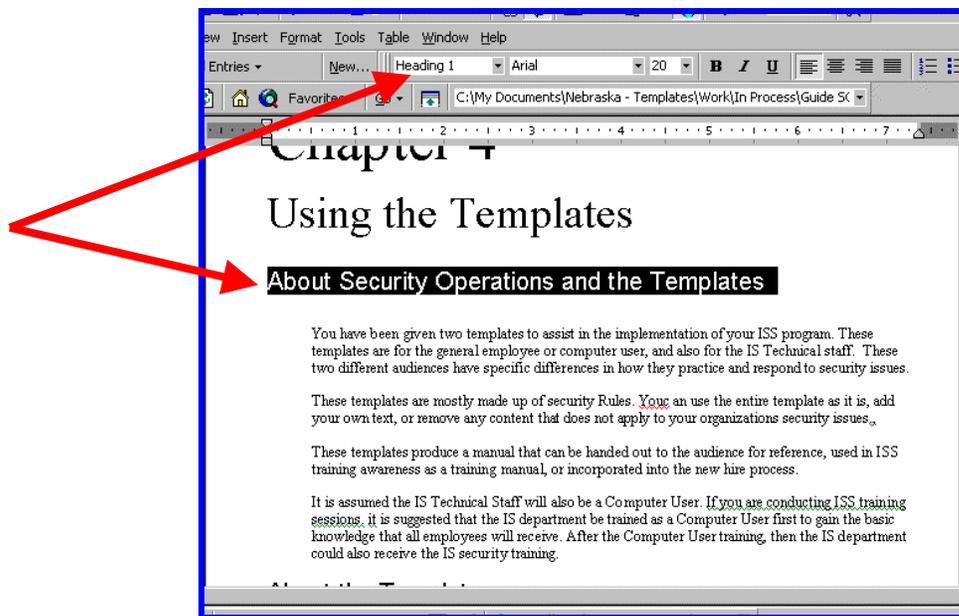
MS Word Features Used

MS Word templates

You may want to install the template document files into the template area of MS Word. To access MS Word templates, click on File, New, then in the Create New section, click Templates, then OK.

MS Word styles

All of the chapter and section heading 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, and allows for global updates. This template package uses Heading 1, Heading 2, and Heading 3.



Warning! When changing headings, you may receive a pop-up window that asks “Update the style to reflect recent changes”. Do NOT select this choice, as it will change the style throughout the entire document!

MS Word Tables

Some of the content in the templates reside in tables. They use standard MS Word Table maintenance.

MS Word Automatic Table of Contents

The templates Table of Contents has been designed with the structure and alignment automatically built using the chapter names, sections and sub-sections.

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

To update the Table of Contents to reflect changes in the documents:

1. Click on any text to highlight the entire Table of Contents.
2. Hit [F9]. This will update the page numbers and any headings you have changed.
3. You may be asked:



4. It is suggested that you select *Update entire table*.

MS Word automatic Index

The templates Index has been designed with the structure and alignment automatically built using marked text.

To update the Index to reflect marked text:

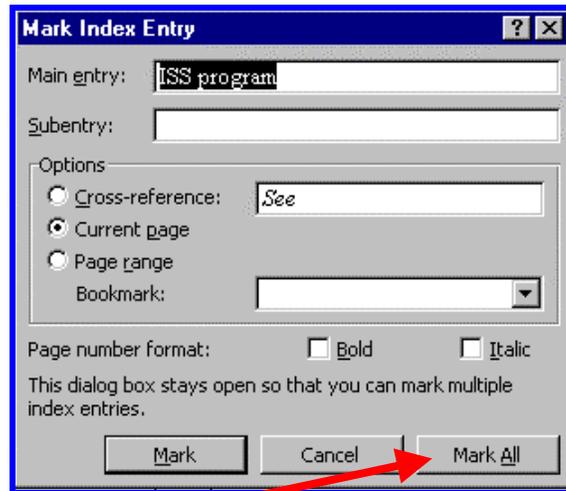
1. Click on any text to highlight the entire Index.
2. Hit [F9]. This will update the page numbers and any new entries you have marked.

To add an entry to the Index:

1. Highlight any text you want to appear in the Index.
2. Hit [Shift] + [Alt] + [x] simultaneously.

Chapter 4 - Using the Templates

3. You will receive:

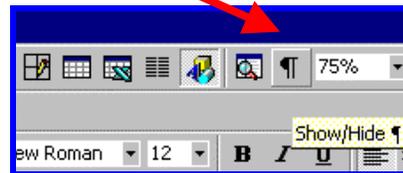


4. Click on the *Mark All* button to mark all occurrences of the selected text.
5. The selected text will appear on your screen as :

ISS program {·XE"ISS Program"·}

and will put you into the Show/ Hide mode.

 **Tip:** To exit the Show/ Hide mode, click on the Show/ Hide icon .



6. To continue to mark Index entries, highlight desired text and click in the Main entry field.
7. Repeat steps 4-5.

Underlined Words

Many terms, phrases, and acronyms are underlined throughout the template package to denote that there is more information about that topic elsewhere in the document. For example, glossary words could be 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*.) the list of categories is displayed in this underlined format:

Network Security Rules

This underlined format is telling you there is more information about this topic. You can also consider it to be an index as what's ahead in this chapter.

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 go to links (rules categories list) and pop-ups (glossary definitions).

Chapter 4 - Using the Templates

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 organization's needs. The content can be used "as is" or modified to reflect your security operations.

You can determine the size of your rules guides.

 **Remember:** If you have less rules, that does not mean they need to be written at a higher level.

Maintaining Rules

Initially you will want to review all rules in the templates and see if you want to modify, delete, or add to the rules.

Adding a Rule

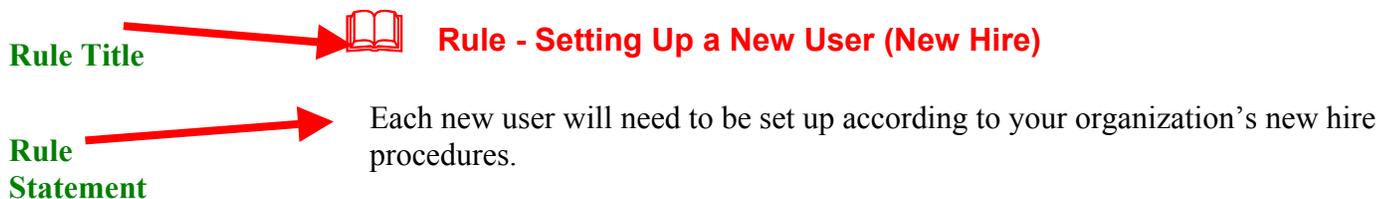
Initially and on-going you will maintain the rules templates. You should review your rules guides periodically to see if a new rule should be adopted. New rules are usually triggered by changes in security practices, technology, business operations, NITC / HIPAA/ regulation requirements.

Rule Formats

The templates provide 2 formats for a rule. You can choose the full or condensed format..

Condensed Format

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



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:



Rule - Setting Up a New User (New Hire)

Rule Statement

“Each new user will need to be set up according to your organizations new hire procedures.”

Policy Category Access Control	Policy Standard Employment Change	Rule Number XX.XX.XX
Rule Date mm/dd/yy	Rule Revision Date mm/dd/yy	Date Adopted mm/dd/yy
Approval Name/ Code (signature) Sabcdefg	Rule Source abcdefg	Audit Number/ Code XX.XX.XX

Explanation/ Key Points

In order for a new employee to do their job, they must be set up to access specific areas.

Procedure

To set up a new employee:

1. Assign a User ID.
2. Set the password to the default password.
3. Inform the new user to change the password immediately.
4. Give employee rule guide.
5. New employee orientation.

Timing

Immediately upon hiring.

Related Rules



Rule - Handling Terminations

Chapter 4 - Using the Templates

Full Format Rule Fields

You can opt to create a full format for each selected rule giving more details to each rule. Below are the suggested fields you could use for additional information about each rule:

Identify the Rule	Rule Title Rule Statement Rule Number 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	Description	Use the ...
1	Critical Rules	full format
2	Strongly Suggested Rules	full format or condensed format
3	Optional Rules	condensed format

Template Parameters { }

Some rules require additional information to be inserted into the text. These rules use parameters to fill in a value pertaining to that rule. You will need to determine the parameter values before you can publish the rules or accept the default values as shown in the templates. Rule parameters that require a value are identified by blue brackets { }.

The following parameters have been incorporated into the templates:

# attempts to log on	You will be allowed {3} failed attempts to try to log on.
# 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 differ 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	

Chapter 4 - Using the Templates

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

Chapter 4 - Publishing the Rules

	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 organization's 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 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}

Chapter 4 - Using the Templates

Completing the Templates

About Completing the Templates

The majority of the template contents are rules that may or may not require a lot of edits. Most of the general overview information at the beginning of the chapters in general enough that you may not need to edit it.

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
- (back matter)
- Index

Procedure #3 How to Publish Rules

Use: Working Papers #3a, #3b

Note:

If you are not changing the template content, the only step you need to do is step 6 - complete the parameters.

First things first:

❗ Important ! Copy the templates before using them!

Beginning chapters:

1. Update the Title Page. Enter your {Organization Name} and the title of the manual {Computer User's Security Handbook} and {IS Technical Staff Handbook}. (i.e. General Employee ISS Booklet, ISS User Reference Guide)
2. Update the front matter which is any preludes or precontent before the numbered pages begin. For example: Proprietary Statement, Copyright information, Publishing information.
3. Skip Table of Contents until later in this procedure.
4. Update Chapter 1 - About Information Security. In both templates, Chapter 1 covers general topics about ISS and the guide itself. You can use this chapter "as is" since it is generic. Be sure to update the section *Handbook Structure - How Its Organized* if you add, delete or change chapters.

Rules chapters:

5. Using *Working Papers #3a and #3b*. For each rule, determine if you want to keep it, delete it, or modify it.
6. Determine values for rules with parameters.
7. Each template has a different set of rules for each perspective, Computer User and IS Technical staff.
8. To change a rule, simply edit the text as you would any MS Word document.
9. To add a rule that is not listed in the template:
 1. determine audience - computer user or IS
 2. determine category (i.e. Access Control)
 3. go to step 12. If you add a rule, you must also add it to the List of Rules in the Appendix.
10. To delete a rule, use the standard MS Word deletion techniques.
11. For all selected rules, determine priority. 1 Critical 2 Strongly suggested 3 Optional
12. For all selected rules, determine if you want to use a full format or condensed format. Use full format if you have additional rule information, have a technology-based procedure, or a high priority rule.

Ending Chapters:

13. Update Chapter 10 – Getting ISS Help. Enter the support phone number and Troubleshooting Chart.
14. Update the back matter or appendix. For all new and changed rules, update the List of Rules.

Chapter 4 - Using the Templates

- 15.** Update the Glossary with any new terms.
- 16.** Update the Table of Contents to reflect changes in the documents. *See Chapter 4 for details.*
- 17.** Update the Index to reflect changes in the documents using [F9]. *See Chapter 4 for details.*

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 to 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 incident 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 incident response team to provide the technical knowledge and evidence preservation.

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

- Prevention
- Detection
- Response

Suspicious 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.

Suspicious 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.

Chapter 5 - Implement an Incident Program

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 chose, be sure it is used daily and incorporated into your incident program.

Tracking Intrusions

Your 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

It is important that all suspicions and incidents be logged and carefully tracked for patterns in behavior, timing, or other such tracking technique.

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 an incident 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 incident 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.

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.

Chapter 5 - Implement an Incident Program

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 other designated contacts (i.e. security guard) must immediately be sought. It is every employee's responsibility to be aware of strangers or unidentified persons on the premises.

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 organization's 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, 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.

Web Site - Contact Information

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 suspicions and incidents.

Evidence

When an incident occurs, you must gather the facts of what happened, how it happened, and note any indicators 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

If possible, you should preserve the evidence for further investigation. For example, you should leave important system messages on the screen and not erase important information. This should only be done if it doesn't interfere with business resumption or if it doesn't cease the attack.

Recording Evidence

All suspicions and incidents should be carefully documented. This includes recording examples of the evidence, attaching screen shots, system printouts, and any other such system supporting evidence.

Incident Response

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 organization's 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.

Chapter 5 - Implement an Incident Program

Internal Response

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

- 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 response reporting should only be done in an extreme emergency.

Centralized Response

It is sometimes necessary to centralize the ISS department to better control ISS issues. This department may include those not on the incident 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.

You can establish a centralized Information Security Department as the focal point for all reports of suspicions and incidents. 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 Response

Information describing 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.

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:

Chapter 5 - Implement an Incident Program

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

Note: Most organizations do not go directly to the FBI. Typically, they will first report incidents to the state patrol who will then accelerate it to the FBI if necessary.

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.

Investigating Incidents

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 conduct full investigations if violent 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

Chapter 5 - Implement an Incident Program

"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. All documentation should be restricted to the facts.

The written report(s) should include:

- Incident Summary
- Detailed Technical Summary
- Relevant logs
- Details on systems compromised (hardware/ os)
- Source of vulnerability exploited
- List of individuals involved

Your 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.

 **Remember:** All documentation you provide may potentially become public.

Incident Reporting Form

You employees should have an Incident Reporting Form to capture the events they witnessed.

See [http://www.nitc.state.e.us/tp/workgroups/security/documents/Incident Reporting Procedure](http://www.nitc.state.e.us/tp/workgroups/security/documents/Incident%20Reporting%20Procedure) for sample Incident Reporting form.

Incident Reporting Retention

Information describing all reported information security problems and violations must be retained for a period of time, usually around 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. This applies to computer logs and internal correspondence, as well as notes from investigations.

Incident Follow Up

Chapter 5 - Implement an Incident Program

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 on an 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. Giving out “security tickets” can be effective.

Legal Responsibility

Perpetrators of crime should be prosecuted by the organization to the full extent of the law. Suitable procedures should 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.

Incident Handling

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

1. Verify that it is indeed an incident
2. Follow your general procedures for responding to incidents
3. Notify your Incident Response Team
4. Analyze the intrusion
5. Communicate with all appropriate parties
6. Set up barriers to block the intrusion (if possible)
7. Image target system(s) and securely retain the information
8. Investigate the incident by reviewing system logs and other monitor information
9. Formulate a trail leading back to the source.
10. Synchronize the activities on different systems, if possible.
11. Apply short term solutions to contain an incident
12. Eliminate all means of vulnerability
13. Return systems to normal operation (after evidence is gathered)
14. Determine if outside help required
15. Collect and protect evidence
16. Gather accurate loss data

Chapter 5 - Implement an Incident Program

17. Document the incident
18. Recover from the incident
19. Follow up on the incident
20. Focus on all communications, internal and external
21. Handle media inquiries (if necessary)
22. Take appropriate measures to secure your system against this happening again
23. Notify law enforcement through proper channels
24. Closure: Identify and implement security lessons learned
25. Hold a post mortem analysis and review meeting with all involved parties. Do this within three to five working days of completing the investigation of an intrusion. *See Incident Reporting form in Appendix.*
26. Prepare a final report for senior management and the Office of the CIO. This ensures awareness of security issues. Use the attached form (or online version) to report information about the security incident to the Office of the Chief Information Officer. Incidents should be reported no later than 5 working days after returning systems to normal operation.
27. Revise security plans and procedures and user and administrator training to prevent future incidents. Include any new, improved methods resulting from lessons learned.
28. Determine whether or not to perform a new risk analysis based on the severity and impact of an intrusion.
29. Take a new inventory of your system and network assets.
30. Participate in investigation and prosecution, if applicable.

Procedure #4 How to implement an Incident Program

Use: Working Paper #4

1. Assemble / educate your Incident Response Team.
2. Write Incident Response Team names in both templates in *Chapter 2*.
3. Complete the Incident Response Chart in *Working Paper #4*.
4. Have periodic practice drills.
5. Implement an Incident Reporting Form.
6. Have procedure for mobilizing the team.

Chapter 5 - Implement an Incident Program

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

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



The purpose of this chapter is to provide structure to an awareness program for the security officer to rollout to the general employee and the specialized technical staff. It suggests training techniques, materials to produce, and communication correspondence to announce, deliver, and support your awareness program.

Awareness Briefings

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

Chapter 6 - Implement an Awareness Program

any ISS program design. Increased awareness increases the proper use of security principles and the likelihood that suspicious activities will be noticed and reported.

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

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 organization’s 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.

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. Every employee 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 employee utilizes information in order to do their job. It is only natural that every employee should be specifically charged with responsibility for information security.

Awareness Applies to Everyone

All employees (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 organization's information resources. Management must allocate sufficient on-the-job time for employees to acquaint themselves with the organization's security rules, procedures, and related ways of doing business.

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 employees exactly what is expected of them.

Chapter 6 - Implement an Awareness Program

Mandatory Awareness Training

ISS training should be mandatory. Every employee must attend an information security awareness class soon after 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.

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

Chapter 6 - Implement an Awareness Program

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.

Chapter 6 - Implement an Awareness Program

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
- Materials
- Training

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 employee’s 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 having the concept that we will have to all work together to make it a success.

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 rule violations. (i.e. workstations not logged out or locked during a fire drill)
- ◆ Initiate an unannounced “unauthorized software duplication” inventory where PCs are checked for illegal software.
- ◆ Adopt an annual ISS day with special educational materials and events.
- ◆ Develop a “tagline” or theme that represents ISS at your organization.

Awareness Materials

The template package helps to prepare your ISS program materials. You may need to develop additional training materials, checklists, and such for your organization's particular needs.

Suggested awareness materials:

- Computer User Security Rule Handbook* (results from templates)
- IS Technical Staff Rule Handbook* (results from templates)
- Incident Response Handout*
- Training Guides
- E-mail messages
- Articles in your organization's newsletter
- Magazines, internet articles for circulation
- Bulletins and alerts
- Posters
- FAQs
- Web announcements
- Labels for system (PC), diskettes, etc.
- Handouts
- Overhead slides
- Exercise workbook
- Quiz (to measure results)
- Practice sessions (do mock security drills)
- Presentation tool
- Class Evaluation
- Giveaways – buttons, pens, certificates, t-shirt's, mouse pads, ...

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 Logistics

- ◆ Self-teaching or classroom
- ◆ Informal, workshop, seminar
- ◆ Role playing

Chapter 6 - Implement an Awareness Program

- ◆ 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 Audience

The training audiences can be very general or very specific to certain job tasks. The following lists the main audiences that require 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 Computer User (permanent staff) course.

Computer User (permanent staff)

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

Computer User (temporary staff)

The computer user (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 computer user (permanent staff) class. They could also be combined/ incorporated with computer user (permanent staff).

Contractors, Agents, Auditors and non-Employees

Chapter 6 - Implement an Awareness Program

See Computer User (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.

This audience will also take the computer user (permanent staff) class.

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.

Procedure #5

How to implement an Awareness Program

Use: Working Paper #5

1. Determine audience(s) in *Working Paper #5*. See *Training Audience* section of *Chapter 6*.
2. What is purpose of awareness? Program rollout, awareness refresher course, new hire orientation.

Campaign:

3. Develop a “tagline” or theme.
4. Give small prizes for exemplary staff and traffic ticket warnings for violations
5. Adopt an annual ISS day with special educational materials and events.

Training:

6. For each audience, what is training curriculum?
7. What training materials are needed?
8. Should training be self-teaching or classroom?

Materials:

9. Review and select from materials list in *Chapter 6*.

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.

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

Appendix

The following documents are contained in this appendix:

Appendix A - NITC Security Architecture Document

Appendix B - Reference List

Appendix B - NITC Security Architecture Document

See www.nitc.state.ne.us/standards.

Appendix C - Reference List

Although many resources were used, the following references were very helpful in gathering the information contained in this template package:

“Information Security - Protecting the Global Enterprise” by Donald L. Pipkin

“Inside Internet Security - What Hackers Don’t Want You to Know” by Jeff Crume

“Information Systems Security Guide - Establishing and Managing an Information Protection program” by Dr. Gerald L. Kovacich

“Information Security Risk Analysis” by ? Thomas R. Peltier

“Internet Security Policy, A Technical Guide” <http://csrc.nist.gov/isptg/html>

“Guideline for Developing an Agency Information Systems Security Policy”
<http://spr.das.state.or.us/guidelin>

“Federal Information Technology Security Assessment Framework” CIO Council (NIST)

“ISI Swiss Army Knife Reference Resource for Security and Audit Professionals” MIS Training Institute

“IT Security Cookbook”

“Information Security Policies Made Easy” by ? Charles Cresson Wood

“RU Secure Policies” Think Secure Corporation

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

Index

A

Acceptable Risk Rating	41
Access Control	7, 8, 22, 61
Adding a Rule	54
Applications	21, 22, 27, 32, 45
Asset Risk Assessment	2
Assets Types	26
automatic Index	51
Automatic Table of Contents	51
Awareness Program	10, 12, 13, 2, 13, 75, 77, 80, 84
Awareness Training	78, 81

B

Business Impact Analysis	10, 13, 25, 29, 45, 64
--------------------------	------------------------

C

Campaign	13, 80, 84
Centralized Response	68
CERT team	15
Classification Levels	11, 32, 34
Classification Scale	30
Communications	27, 28, 45
Computer User's Security Handbook template	3, 60, 82
Condensed Format	12, 54
CONFIDENTIAL	32, 34
copyright	20
Cost \$ to Replace Scale	37, 46

D

Detection	12, 42, 63, 64
Disaster Recovery	7
Disclosure Scale	11, 36, 45
Documenting the Incident	12, 70

E

Electronic Intrusion	12, 66
Enforcement	12, 56, 71
Evidence	12, 11, 67
External Response	68

F

Full Format	12, 49, 55, 56
-------------	----------------

G

General Software	27, 45
------------------	--------

H

Hardware	27, 45
----------	--------

HIGHLY RESTRICTED	32, 34
HIPAA	4, 11, 29, 31, 32, 54, 75

I

Incident	63, 65
Incident Handling	12, 71
Incident Program	10, 12, 13, 63, 73
Incident Reporting Form	12, 70, 73
Incident Response	10, 12, 2, 9, 16, 23, 67, 71, 73, 81
Incidents	8, 9, 10, 11, 12, 16, 18, 63, 64, 65, 67, 68, 69, 71, 72, 82
Individual Use	8
Information Assets	11, 26, 31
Information Security Management	7
Information Systems Security	1, 75, 87
Integrity Scale	11, 36, 45
Internal Response	68
INTERNAL USE ONLY	33, 34
Investigating	12, 69
IS Technical Staff template	3

L

Logs	10, 22, 42
Loss Impact	11, 35, 46

M

Materials	12, 13, 2, 76, 80, 81, 84
-----------	---------------------------

N

Network Security	8, 52
NITC	13, 4, 5, 7, 9, 54, 87

O

occurrences	52, 63
Owner	30, 34

P

Parameters	12, 57
Platform	26, 27, 45
Policy	5, 7, 8, 9, 79, 87
Prevention	12, 63, 64
Priorities	12, 56
Procedures	10, 2, 5, 10, 42

Q

Qualitative Approach	10, 26
----------------------	--------

R

Reporting Procedure	9, 10
Residual Risk	11, 43, 46

Response	12, 10, 12, 15, 63, 65
Risk Factor	11, 40, 43, 46
Risks	11, 38
Rule	11, 12, 5, 9, 17, 54, 55, 56, 57, 71, 81
Rule Formats	54

S

Safeguard Costs	11, 43
Safeguard Tools	11, 44
Safeguards	42
Safeguards Types	11, 42
Security Advisory Committee	10, 15, 16, 23
Security Audits	10, 21
Security Breaches and Incident Reporting	8, 9
Security Officer	17
Security Team	10, 13, 15, 23
Standard	5, 9
Storage/ space/ size	29
Suspicion	63

T

Technology Dependent	10, 11, 3, 48
Template Mechanics	50
template package	3, 5, 6, 7, 18, 25, 26, 40, 48, 50, 52, 81, 87
Threat Impact	11, 39
Threat Likelihood	11, 39
Threat Types	11, 38
Threats	11, 38, 46
Training	10, 13, 8, 18, 59, 80, 81, 82, 84, 87

U

Unavailability Scale	11, 36, 46
UNCLASSIFIED/ PUBLIC	33, 34

V

Value	35
Value Calculation	11, 37
Virus	66