Working Papers

(The control points of the template system.)

A complete set of the working papers taken from the *Security Officers Instruction Guide*. This is to be used by the implementer(s) of this ISS program package.

December 31, 2001

You can complete these working papers on line or you can print them out and fill in the blanks manually. Online use assumes an intermediate level of skill with Microsoft Word. Print quality and layout may vary by printer.

Working Papers Overview

Working Paper #1: Assemble a Security TEAM

ISS Tasks	Agency/ Department (if different)	Division/Unit Responsible	Person(s) Responsible	Position	Member of SAC? (Y/N)	Member of IRT? (Y/N)
Rule Tasks						
Recommend, develop, and implement security Rules - the Rule Maker (use template).			John Doe	Network admin	N	Y
Enforce and monitor compliance to security Rules.						
Periodically evaluate effectiveness of ISS Rules and procedures.						
System Tasks						
Act as liaison between security department and IS.						
Coordinate followup procedures for ensuring proper adjustment of access privileges associated with changes in employee status and business arrangements.						
Review changes to the configuration of security administration facilities and settings.						
Participate in preparing a disaster recovery plan to help prepare for contingencies and be ready to implement the disaster recovery plan.						
Implement procedures for authentication of users and messages.						
Publish guidelines for creating and managing passwords.						
Approve/disapprove access by users to systems/set up access - passwords.						
Cooperate in the development and implementation of security technology.						
Perform security assurance reviews for new systems and changes to existing systems.						

ISS Tasks	Agency/ Department (if different)	Division/Unit Responsible	Person(s) Responsible	Position	Member of SAC? (Y/N)	Member of IRT? (Y/N)
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						
Gather facts and analyze information security issues/ keep current.						
Develop recommendations for IMServices on ISS matters.						
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.						

ISS Tasks	Agency/ Department (if different)	Division/Unit Responsible	Person(s) Responsible	Position	Member of SAC? (Y/N)	Member of IRT? (Y/N)
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.						

Working Paper #2a: Business Impact Analysis Ranges and Scales

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

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

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

Scale	Integrity Range
25	$100,000,000 and >
20	$10,000,000 - 100,000,000
15	$1,000,000 - 10,000,000
12	$500,000 - 1,000,000
10	$100,000 - 500,000
5	$10,000 - 100,000
4	$1,000 - 10,000
3	$100 - 1,000
2	$1 - 100
1	< $1

Scale	Unavailability Range
25	$100,000,000 and >
20	$10,000,000 - 100,000,000
15	$1,000,000 - 10,000,000
12	$500,000 - 1,000,000
10	$100,000 - 500,000
5	$10,000 - 100,000
4	$1,000 - 10,000
3	$100 - 1,000
2	$1 - 100
1	< $1

Scale	Disclosure Impact
25	Stock prices 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

Scale	Cost to Replace Range
25	$100,000,000 and >
20	$10,000,000 - 100,000,000
15	$1,000,000 - 10,000,000
12	$500,000 - 1,000,000
10	$100,000 - 500,000
5	$10,000 - 100,000
4	$1,000 - 10,000
3	$100 - 1,000
2	$1 - 100
1	< $1

Working Paper #2b: Business Impact Analysis — Platform Table

ISS Asset: Platform (option: list all categories)	**Location** (physical or logical platform/ location)	**Inventory Number** (number)	**Affected by HIPAA?** (y/n)	**IMServices Supported/ Owned?** (y/n) (If y, do not continue)	**Storage space/ size** (use scale)	**#Users: usage and sharing** (use scale)	**Owner** (name)	**Classifi-cation** (use scale)	**Loss Impact**			**Value** (Storage + Users + Class + Loss Impact)
									Integrity (use scale)	**Unavail-ability** (use scale)	**Disclosure** (use scale)	

ISS Asset: Platform (option: list all categories)	**Threat** (list all)	**Threat Likeli-hood** (use scale)	**Threat Impact** (use scale)	**Risk Factor** (Value + Threat Likelihood + Threat Impact)	**Current Safeguard(s)** (list)	**Proposed Safeguards**		
						(list)	**New Risk Factor** (Value + Threat Likelihood + Threat Impact)	**Costs** ($)

Working Paper #2b: Business Impact Analysis — Applications Table

ISS Asset: Applications (software and databases)	**Location** (physical or logical platform/ location)	**Inventory Number** (number)	**Affected by HIPAA?** (y/n)	**IMServices Supported/ Owned?** (y/n) (If y, do not continue)	**Storage space/ size** (use scale)	**#Users - usage and sharing** (use scale)	**Owner** (name)	**Classifi-cation** (use scale)	**Loss Impact**			**Value** (Storage + Users + Class + Loss Impact)
									Integrity (use scale)	**Unavail-ability** (use scale)	**Disclosure** (use scale)	

ISS Asset: Applications (software and databases)	**Threat** (list all)	**Threat Likeli-hood** (use scale)	**Threat Impact** (use scale)	**Risk Factor** (Value + Threat Likelihood + Threat Impact)	**Current Safeguard(s)** (list)	**Proposed Safeguards**		
						(list)	**New Risk Factor** (Value + Threat Likelihood + Threat Impact)	**Costs** ($)

Working Paper #2b: Business Impact Analysis — General Software Table

ISS Asset: General Software	**Location** (physical or logical platform/ location)	**Inventory Number** (number)	**Affected by HIPAA?** (y/n)	**IMServices Supported/ Owned?** (y/n) (If y, do not continue)	**Storage space/ size** (use scale)	**#Users - usage and sharing** (use scale)	**Owner** (name)	**Classifi-cation** (use scale)	**Loss Impact**			**Value** (Storage + Users + Class + Loss Impact)
									Integrity (use scale)	**Unavail-ability** (use scale)	**Disclosure** (use scale)	
Operating Systems												
Utilities												
Compilers												

ISS Asset: General Software	**Threat** (list all)	**Threat Likeli-hood** (use scale)	**Threat Impact** (use scale)	**Risk Factor** (Value + Threat Likelihood + Threat Impact)	**Current Safeguard(s)** (list)	**Proposed Safeguards**		
						(list)	**New Risk Factor** (Value + Threat Likelihood + Threat Impact)	**Costs** ($)
Operating Systems								
Utilities								
Compilers								

Working Paper #2b: Business Impact Analysis — Hardware Table

ISS Asset: Hardware	**Location** (physical or logical location)	**Inventory Number** (number)	**Affected by HIPAA?** (y/n)	**IMServices Supported/ Owned?** (y/n) (If y, do not continue)	**Storage space/ size** (use scale)	**#Users - usage and sharing** (use scale)	**Loss Impact**		**Value** (Storage + Users + Loss Impact)
							$ to Replace (use scale)	**Unavailability** (use scale)	
Processors									
Tape Drives									
Printers									
DASD									
UPS									

ISS Asset: Hardware	**Threat** (list all)	**Threat Likeli-hood** (use scale)	**Threat Impact** (use scale)	**Risk Factor** (Value + Threat Likelihood + Threat Impact)	**Current Safeguard(s)** (list)	**Proposed Safeguards**		
						(list)	**New Risk Factor** (Value + Threat Likelihood + Threat Impact)	**Costs** ($)
Processors								
Tape Drives								
Printers								
DASD								
UPS								

Working Paper #2b: Business Impact Analysis — Communications Table

ISS Asset: Communications	**Location** (physical or logical location)	**Inventory Number** (number)	**Affected by HIPAA?** (y/n)	**IMServices Supported/ Owned?** (y/n) (If y, do not continue)	**Loss Impact**		**Value** (Storage + Users + Loss Impact)
					$ to Replace (use scale)	**Unavailability** (use scale)	
Access points/ configuration points							
Modems							
Routers (list quantity by model)							
Networks							
Switches							

ISS Asset: Communications	**Threat** (list all)	**Threat Likeli-hood** (use scale)	**Threat Impact** (use scale)	**Risk Factor** (Value + Threat Likelihood + Threat Impact)	**Current Safeguard(s)** (list)	**Proposed Safeguards**		
						(list)	**New Risk Factor** (Value + Threat Likelihood + Threat Impact)	**Costs** ($)
Access points/ configuration points								
Modems								
Routers (list quantity by model)								
Networks								
Switches								

Working Paper #2c: Threats/Risks Types Table

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
Others ??

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

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 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.

_____ Acceptable Risk Rating

Working Paper #2d: Safeguards Table

Safeguard Types	What it Protects	Rating
Firewalls.		
VPNs?		
Incident monitors.		
Install all patches.		
Intrusion detection systems.		
Polices/rules/procedures.		
Awareness/training.		
Logs - daily monitoring.		
Physical access means.		
Encryption.		
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.		
Others?		

Working Paper #3a: Publishing Rules/Parameters — Computer User

Rule	Description	**Disposition:** Keep (K); Delete (D); Modify (M)	**Format:** Full (F); Condensed (C)	**Priority:** Critical (1); Strongly suggested (2); Optional (3)	**Parameter Value**
Logging On Rules (See Chapter 3)					
🕮 Unique User ID and Password					
🕮 Unsuccessful Logging On					
Warning Banner Rules (See Chapter 3)					
🕮 Display a Warning Banner					
🕮 Warning Banner Keystroke Monitoring					
🕮 Warning Banner Last Log on					
Logging Off Rules (See Chapter 3)					
🕮 Automatic Log Off					
🕮 Leaving Your Workstation - Logging Off / Locking					
Identification (User ID) Rules (See Chapter 3)					
🕮 Unique User ID					
🕮 Prohibit Group User IDs					
🕮 Sharing your User ID is Prohibited					
🕮 Using Another User ID is Prohibited					
🕮 Dormant User IDs					
🕮 Internet User ID Expiration					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Authentication (Password) Rules (See Chapter 3)					
🕮 Changing Your Default Password					
🕮 Difficult to Guess Passwords					
🕮 Minimum/ maximum Password Length					
🕮 Cyclical Previous Passwords					
🕮 Password Allowable Characters					
🕮 Passwords Lower and Upper Case					
🕮 Choosing Your Password					
🕮 Keeping Your Password Confidential					
🕮 Reusing Passwords / History					
🕮 Display and Printing Passwords					
🕮 Forced Expiration of Passwords					
🕮 Unsuccessful Passwords Attempts					
🕮 Same Password on Different Systems					
🕮 Disclosure Forces Password Change					
🕮 Writing Passwords Down					
🕮 Written Passwords Left Near Devices					
🕮 Proof Of Identify to Obtain a Password					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Authorization (Privileges) Rules (See Chapter 3)					
🕮 Authorized Privileges					
Network Access Rules (See Chapter 4)					
🕮 Approval for Connections					
🕮 Gaining Unauthorized Access					
🕮 Network Browsing Prohibited					
🕮 Network Backups					
🕮 Overwhelming the Network					
🕮 Malicious Intent and the Network					
Modem Rules (See Chapter 4)					
🕮 Modems Connections to Internal Networks Prohibited					
🕮 Prohibit Modems in AutoAnswer Mode					
Remote Access Rules (See Chapter 4)					
🕮 Dial-up Password Attempts					
🕮 Remote Access Training					
Remote Sites Rules (See Chapter 4)					
🕮 Telecommuting Permissible Equipment					
🕮 Protection of Off-Site Property					
🕮 Information to be Returned					
🕮 Remote Working Environment					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Right to Conduct Inspections of Telecommute Office					
Sensitive Information on Portable Computers					
Backing up Portables Computers					
Transportable Computers Hand Luggage on Airplanes					
Portable Computer Security					
E-mail Rules (See Chapter 5)					
E-mail for Business Purposes Only					
E-mail and Confidential Information					
Forwarding E-mail					
Forwarding External E-mails					
Forwarding E-mail to Archival Records					
E-mail Retention					
E-mail Virus Protection Software					
Certainty of E-mail File Attachments Origin					
Using another Users E-mail Account					
Using E-mail as a Database					
Deleting and Destroying E-mail					
Privacy and E-mail					
E-mail is Public Communication					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
E-mail as a Public Record (government)					
E-mail Profanity					
Responding to Junk (SPAM) E-mail					
Ownership of E-mail Messages and Attachments					
Disclosure of E-mail Messages and Attachments					
Authorization to Issue Broadcasts in E-mail					
Scanned Signatures in E-mail					
Misrepresentation of Identity in E-mail					
Internet Rules (See Chapter 5)					
Downloading Internet Files / Anti-Virus					
Sending Sensitive Information Over the Internet					
Uploading via the Internet					
Using the Internet for Personal Use					
Approval for Internet Connections					
Training for Internet Use					
Internet User ID Expiration					
Personal Messages Disclaimer on Internet					
Internet Products and Services					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Public Area of Your Organization's Web Site					
Unofficial Web Pages on the Internet					
Concealing your Identity on Internet is Prohibited					
Exchanges of Information on the Internet					
Updating Organization Information on the Internet					
E-commerce Rules (See Chapter 5)					
E-transactions					
Forming E-contracts					
Validating Identity of External Parties on Internet					
Electronic Offers					
Internet Customers					
Workstation Rules (See Chapter 6)					
Workstation Protection Security					
Securing Unattended Workstations					
Loading Personal Screen Savers					
Altering Computer Equipment					
Moving and Relocating Your Equipment					
Sensitive Information While Working					
Locking File Cabinets					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Screen Positioning					
Clear Desk					
Clear Screen					
Office (with a door)					
Cubicle Security					
Bringing your personal PC/ laptop to Work					
Personal Equipment and Information Ownership					
Personal Equipment and Privacy					
Home Computers Security					
Disposal Rules (See Chapter 6)					
Information Disposal/ Wiping					
Discarding Hardcopy Information					
Personal Equipment Disposal					
Media Disposal/ Concealment					
Erase and Zeroize					
Destruction Approval					
Media Security Rules (See Chapter 6)					
Media Safety					
Hard Drive Security					
Sensitive and Non-sensitive on Same Media					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Physical / People Security Rules (See Chapter 7)					
🕮 Tailgating and Piggybacking when Entering					
🕮 Lending Cards/ Keys, Tokens					
🕮 Challenging Strangers					
🕮 Handling Visitors					
🕮 Visitor Escorts					
🕮 Visitors Entrances					
🕮 Social Engineering					
🕮 Sensitive Information and Physical Access Controls					
🕮 Lock Office Doors					
🕮 Wearing ID Badges					
🕮 Temporary ID Badges					
🕮 Reporting Stolen/ lost Access Badges/ Cards/ Tokens					
🕮 Presenting Your Badge					
🕮 Propping Open Doors					
🕮 Stay away from Restricted Areas					
🕮 Property Pass for Removing Equipment					
Copyright Rules (See Chapter 8)					
🕮 Copyright Laws for Software and Paper					
🕮 Copyrighted Inquiries					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Copying Copyright Materials					
Protection of Software and Copyrighted Materials					
Copyright Enforcement Statement					
Making Excess Copies Prohibited					
Copying Vendor Software					
Sending Copyrighted Information Electronically					
Violation of Copyright Laws					
Using Copyrighted Information from the Internet					
Ownership of Copyrighted Materials					
Acceptable Use (of systems) Rules (See Chapter 9)					
Personal Use of your Computer					
Other Business Activities					
Using State-Owned Resources Unrelated to Business					
Using State Resources in an Acceptable Way					
Transmitting State-Owned Resources in an Acceptable Way					
Misrepresentation on State-Owned Resources					
Using Others Users Data on the State-Owned Resources					
Preventing Services to Others					
Storing Games on your Computer					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Giving Information to a Third Party					
Handling Third Party Confidential Information					
Third Party Agreements and Approvals					
Sensitive Disclosure Statement to Third Party					
Exposure of Sensitive information Public Places					
Time Sensitive Information					
Other Employees/ Organization Rules (See Chapter 9)					
Disclosing Co-worker(s) Contact Information					
Disclosing Co-worker(s) Change in Status Information					
Personal Identifiers Prohibited					
Disclosing Organization Information					
Disclosing Organization Secured Areas					
Disclosing Organization Future Plans Prohibited					
Organization Meetings and Sensitive information					
Sensitive Information and Meeting Rooms					
Organization's Documentation					
Public Records/ Privacy (of citizens) Rules (See Chapter 9)					
Privacy of Citizens					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Privacy and E-mail					
Violating Others Privacy					
Public Records					
Personal Identification Information (PII)					
Consent to Disclose Information to Law Enforcement					
Collecting Private Information					
Children's Privacy					
Customers Privacy					
Customers Disclosure to Third Party					
Explanation for Private Information					
Disclosure Notification / Blocking Privacy Request					
Public Records Source Owner					
Materials Released to the Public					
Paper Information Rules (See Chapter 9)					
Copying Sensitive Information					
Copying Sensitive Information and Special Paper					
Copier / Printer Malfunction					
Attending to Printers					
Sensitive Information - Page Numbering					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Third Party Copying Sensitive Information					
Mailing Envelopes for Sensitive Information					
Tracking Mailed Sensitive Information					
Delivering Sensitive Information					
Filing Sensitive Information					
Destroying Unwanted Hard Copies					
Using Software and Data Rules (See Chapter 9)					
Malicious Intent is Prohibited					
Downloading Software					
Protecting Software / Handling a Virus					
Copying Software					
Purchasing and Installing New / Upgraded Software					
Retaining Data					
Input Data Retention					
Using File and Directory Rules (See Chapter 9)					
Others User Directories and Files					
Unauthorized Access Prohibited					
Receiving Files on Disks / CDs					
Setting up a New Directory					
Amending Directory Structures					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Using Meaningful Directory and File Names					
Telephone, Faxes and Other Devices Rules (See Chapter 9)					
Telephone Disclosures					
Cellular Telephones					
Answering Machines					
Organization Credit Cards on Pay Phones					
Organization Telephone Book Security					
Consent to Record					
Faxing Sensitive Information					
Fax Cover Sheet					
Taping Sensitive Information					
Video Conferencing					
Other Devices - Transmissions					
HR Related Rules (See Chapter 9)					
Personnel Records (privacy) and the Employee					
Using Employee Information					
Returning Organization Property					
Help Wanted Ads and Disclosure					
Gathering Prospective Employee Information					
Employee Monitoring Notification					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Employee Job Performance Privacy					
Benefits Cannot be Denied					
Employee Health and Safety Disclosure					

Working Paper #3b: Publishing Rules/Parameters — IS Technical Staff

Rule	Description	**Disposition:** Keep (K); Delete (D); Modify (M)	**Format:** Full (F); Condensed (C)	**Priority:** Critical (1); Strongly suggested (2); Optional (3)	**Parameter Value**
Technical Specialists Rules					
🕮 Access by Technical Specialists					
🕮 Technical Specialists Security Check					
🕮 Security Administration Activities					
Application Requirements Rules					
🕮 Application Controls					
Logging On Rules					
🕮 Unique User ID and Password					
🕮 Unsuccessful Logon Attempts					
🕮 Single Sign On (Log On)					
🕮 Disclosure of Incorrect Logon Information					
🕮 Encrypted Logon Files					
🕮 Logon Scripts					
🕮 Third Party Logons					
🕮 Giving Logon Information to the User					
🕮 Limitation on Number of Daily Log Ons					
Warning Banner Rules					
🕮 Display a Warning Banner					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Warning Banner Keystroke Monitoring					
Warning Banner Last Logon					
Warning Banner Information Disclosure					
Logging Off Rules					
Automatic Log Off if No Activity					
Automatic Log Off at End of Day					
Identification/ User ID Rules					
Unique User ID					
Prohibit Group User IDs					
Dormant User IDs					
Internet User ID Expiration					
Granting Multiple User IDs					
Granting User IDs to Outsiders					
Re-use of User IDs					
Customer Privacy and User IDs					
Distribution of User IDs					
User ID Logs					
Authentication / Passwords Rules					
Assign a Default Password					
Minimum/ Maximum Password Length					
Cyclical Previous Passwords					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Password Allowable Characters					
Passwords Lower and Upper Case					
Reusing Passwords / History					
Forced Expiration of Passwords					
Unsuccessful Passwords Attempts					
Proof Of Identify to Obtain a Password					
Distributing Passwords to Users					
Typing Passwords					
Resetting Passwords					
Dynamic Password Tokens					
Seed for System Generated Passwords					
Immediate Issue of System Generated Passwords					
Storage of Passwords					
Zeroization of Password Materials					
Password Based Boot Protection					
Sending Passwords through the Mail					
Password Encryption					
Use of Duress Passwords					
Changing Vendor Default Passwords					
Passwords of Key Role Holders					
Review Digital Certificates					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Unauthorized Access to Passwords					
Authorization (Privileges) Rules					
Privileges Granted on a Need-to-Know Basis					
Dual Access Controls					
Privileges Granted by Groups					
Users that Leave the Organization					
Systems Privileges					
Separation of Duties					
Sanctions Rules					
Revoking Access					
Employment Status Change Rules					
Setting Up a New User (New Hire)					
Handling Terminations					
Network / Perimeter Security Rules					
Configuring Networks					
Managing the Network					
Defending against Virus Attacks					
Handling Hoax Virus Warnings					
Installing Virus Scanning Software					
Electronic Eavesdropping					
Modem Pool					
Scanning for Modems					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Dividing Large Networks					
Network Connections with other Organizations					
State-owned Resources					
Network Controls					
Unattended Network Terminals					
Sensitive Information Prohibited from Network Printer					
Controlling Network Analyzers					
Setting up Intranet Access					
Setting up Extranet Access					
Network Diagrams					
Default Passwords on Network Hardware					
Keeping Track of Modems					
Network Audit					
Perimeter Security					
Accessing Network Vulnerability					
Network Entry Controls					
Monitoring Network Entry					
Perimeter security 24/ 7					
Implementing Perimeter Protection					
Defending against Denial of Service Attack					
Inventory of Connections to External Networks					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Contact Numbers in Directories					
Isolating Sensitive Systems from Network					
Connecting Modems to Network Prohibited					
Modem Pools					
Highest Risk Elements on the Network					
Firewalls Rules					
Firewalls Required for all Dial Up Connections					
Firewalls Must Run on Dedicated Computers					
Changing Firewall Configurations					
Internet Connections Need Firewalls					
Remote User / Dial-in Rules					
Unsuccessful Logon Attempts					
Remote Systems Connecting to Production					
Issuing Laptops/ Portable Computers					
Controlling Remote Access					
Dial Up access needs Protection					
Using Modems/ ISDN, DSL Connections					
Connecting Networks to Third Party Networks					
Extended User Authentication Systems for Dial Up					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Use of Cable Modems					
Using Encryption Techniques					
Answering Incoming Calls					
Virus Handling Rules					
Virus Checking Programs on PCs and LAN Servers					
Testing for Viruses on a Stand-alone Computer					
Virus Checking at Firewalls, Servers, and Desktops					
Two Virus Screening Software Packages					
Floppy Virus Checking Decal					
Integrity Checking Programs					
Decrypting Before Checking for Virus					
Write Protection and Virus					
E-mail Rules					
E-mail Point of Entry					
Central E-mail Systems/ Anti-Virus					
Deleting and Destroying E-mail					
Using E-mail as a Database					
Recording and Retaining E-mail					
Internet Rules					
Setting up Internet Access					
Intrusion Detection Systems					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Public Servers on Internet					
Internet Commerce Servers - Demilitarized Zone					
Internet Commerce Servers - Encryption					
Downloading Internet Files / Anti-virus					
Firewalls and Internet Connections					
Internet Connections and Shared Directories					
Developing a Web Site					
Web Browsers					
Contact Information on Web Site					
E-commerce Rules					
Protecting E-commerce Web Sites					
Securing E-commerce Networks					
Hardware Rules					
Purchasing and Installing New Hardware					
Hardware Security - Down Time					
Moving / Relocating Hardware					
Disposal Rules					
Person Authorized to Destroy Sensitive Information					
Destruction of Records					
Object Reuse					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Using External Disposal Firms					
Zeroization of Password Materials					
Sensitive Information Destruction Before Servicing					
Sensitive Information Disposal					
Erasing before Giving to a Third Party					
Hardcopy Sensitive Information Disposal					
Using Removable Storage Media					
Building/ Room Access Rules					
Propped Open Doors to Computer Room					
Network Components Protection					
Physical Access to Sensitive Information					
Hard Drive Security					
Environment Rules					
Environment Controls					
Installing and Maintaining Network Cabling					
Supplying Continuous Power to Critical Equipment					
Managing and Maintaining Backup Power Generators					
Guards/ Outside Security Organizations / Equipment Rules					
Working with Guards / Guard Stations					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Outside Security Systems					
Security Equipment					
Systems Development / Programming Rules					
Software Development					
Development Security Requirements					
Developed Software Notice of Failure					
Test to Production - Removing Paths					
Test vs. Production Files Naming Conventions					
Separation of Development and Live Environments					
System Developers and Production					
Interfacing Applications Software/ Systems					
Special Labeling for Non-production Business					
System Interruption					
Systems Utilities Prohibited from Production Storage					
Development Using Licensed Software					
Managing Program Libraries					
Separating Duties - Systems Development					
Data Management Rules					
Managing Databases					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Maintaining Data Structures					
Setting up New Databases					
Confidential Data					
Software Maintenance / Upgrades Rules					
Applying Patches to Software					
Responding to Vendor Recommended Software Upgrades					
Operating System/ Utilities Upgrades					
Change Control Process					
Controlling old Versions of Programs					
System Testing Rules					
System Developers and Testing					
Restricted Use of Diagnostics					
Testing Third Party Software					
Software Testing with Sensitive Data					
Controlling Test Environments					
Using Live Data for Testing					
Testing Systems and Equipment					
Systems Documentation Rules					
Systems Documentation Security					
Maintaining a Hardware / Software Inventory					
Hardware Documentation					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Controlling Program Listings					
Documentation Version Control					
Required Documentation for Production					
Disaster Recovery Rules					
Doing a Business Impact Analysis					
Classification System					
Identifying Sensitive Information					
Safeguards and Mitigation Strategies					
Business Resumption					
Contingency Plans for Different Types of Disruption					
Implementing a Disaster Recovery Plan					
Escalating Responses					
Disaster Recovery Plan - Training, Testing, Practice					
Disaster Recovery Plan Annual Review and Revision					
Human Factor					
Off-Site Storage Rules					
Off Site Storage of Essential Information					
Physical Separation of Sites					
Multiple Site Storage of Backup Documents					

Rule	Description	Disposition: Keep (K); Delete (D); Modify (M)	Format: Full (F); Condensed (C)	Priority: Critical (1); Strongly suggested (2); Optional (3)	Parameter Value
Backup, Recovery and Archived Data Rules					
Managing Backup and Recovery Procedures					
Backup all New Software					
Frequency of Backing up Data					
Backup Scope					
Backing Up on Portable Computers					
Safeguarding your Backups					
Two Backup Copies					
Users Backing Up					
Automatic Backup to Network					
Users Notified of Backups					
Backup Information Retention					
Users Restoring Data					
Archiving Information					
Archival Storage					
Preserving Data in Archival Storage					
Archive Retention					
Regular Purging of Information					

Working Paper #4: Incident Reporting At-a-Glance Handout

Computer User Incident Response Quick Reference

Be Alert !

You can make a difference by being aware of your environment, noticing unusual activities, safeguarding vulnerabilities, and quickly reporting any incidents.

To Report…	Comments	
… an incident in process.		Call …
… sensitive information that has been or is being disclosed, lost, or damaged.		Call …
… a software/ system malfunction.	Do not attempt a recovery yourself.	1. Note (if time) any error messages, unusual system behavior (how is it behaving differently than before?) 2. Stop using the computer. 3. Disconnect from any attached networks. 4. Call …
… a virus.		1. Shut down the involved computer. 2. Disconnect from all networks. 3. Call …
… an offensive e-mail, call, etc.		Respond directly to the originator. If the originator does not promptly stop sending offensive messages, report it to …
… suspicious behavior.		Call …
… known systems security vulnerabilities, risks, alerts, and warnings.		Call …
… equipment damage or loss.		Call …
… a physical access violation.		Call …

Your Incident Response Team

_____	_____	_____
_____	_____	_____
_____	_____	_____

The most important thing to remember is to be PROMPT.

Working Paper #5: Awareness Program

Whom do you want to make aware of ISS?

Awareness Topics/ Curriculum	Audience		Campaign	Training	Materials Needed

Computer User Awareness Training: Sample Agenda

Topics	Duration (min.)	Supporting Visuals
Class Opening		Welcome Slide
Intros/Logistics/Class Overview	10	
Project Overview	10	
Management Support	10	
Subjects		
ISS Overview	30	Rule Guide Chapter 1
Incident Reporting	15	Incident Handout
Computer User Rules Overview	5	
Access Control Rules	10	Rule Guide Chapter 3
Network Security Rules	10	Rule Guide Chapter 4
Internet, E-mail Rules	15	Rule Guide Chapter 5
Workstation/Office Rules	5	Rule Guide Chapter 6
Physical/People Rules	5	Rule Guide Chapter 7
Copyright Rules	5	Rule Guide Chapter 8
Acceptable Use Rules	10	Rule Guide Chapter 9
Closing		Quiz
Summary Test	10	
Wrap Up/What's Expected	5	
Final Q&A	3	
Total Duration:	158 min. (2 hr, 38 min.)	