State of Nebraska

Information Systems Security (ISS)

IS Technical Staff **Template**

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

December 31, 2001

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

State of Nebraska

Information Security Systems (ISS)

{Your Organization's Name}

{IS Technical Staff Security Handbook}

"A complete security awareness guide and rules for the IS professional State of Nebraska employee."

State of Nebraska
Information Security Guidelines

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

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

IS Technical Staff Handbook

Version 1.0
December 31, 2001

Prepared by:

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

Table of Contents

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

Chapter 1
About Information Security

About Information Security

Information security has become the main focus of IS departments all over the world. With the Y2K efforts, came the realization that one of an organization's greatest assets is it's information systems. Information systems today are becoming more and more web-enabled and remotely accessible. With these technical trends come new security vulnerabilities and a constant effort to predict and safeguard against attack.

In general, IS security is smart business practices. The IS technical staff are key factors in protecting information, as IS has access to sensitive data, production data, and all critical operating systems. The intent of this guide is to educate the IS technical staff on information security issues, give IS a good set of rules to incorporate into their business practices, and to know what to do if IS encounters a security violation.

The Role of the IS Department

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

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

The IS Department and the Security Officer

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

Using this Guide

This **{IS Technical Staff Handbook}** is a reference tool for the IS technical staff in the organizations of the State of Nebraska. It is written generically to all technical levels, as well as all management levels, staff, programmers, administrators, and such other technical personnel. It is to be followed by all employees, contractors, etc. of the IS department. It defines the general security areas, accompanying rules, and any procedures or "how to" steps for any security tasks IS may need to perform. This guide can be used as a training tool, for reference support, or as part of an ISS awareness program.

About Rules

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

- Access Control
- Network Security
- E-mail , Internet, and E-commerce
- Workstation / Equipment
- Physical/ Premises Security
- Systems Development
- Disaster Recovery

Special Features of this Handbook

In addition to defining good practices and ISS rules for you to incorporate into your daily job tasks, this handbook also contains the following helpful features:

- Summary list of Rules (Appendix)
- Troubleshooting Chart (Chapter 10)

Handbook Structure - How Its Organized

To understand the layout of this handbook and to help you find a rule by chapter:

Table of Contents

Chapter 5	E-mail, Internet and E-commerce Rules
Chapter 6	Equipment / Hardware Rules
Chapter 7	Physical Security / Premises Rules
Chapter 8	Software Development
Chapter 9	Disaster Recovery Rules
Chapter 10	Getting ISS Help
Appendix	Appendix A - List of Rules
Index	

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

Chapter 2
Security Incidents and Reporting

About Security Incidents

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

Suspicions and Incidents

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

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

ⓘ ***Important !*** Reporting a suspicion, can prevent an incident.

Witnessing / Causing an Incident

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

ⓘ ***Important !*** The most important thing to remember is to be PROMPT.

ⓘ ***Important !*** Do not try to handle it yourself.

Your Incident Response Team

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

Incident Participation

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

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

They are:

____

____

____

Suspicion and Incident Reporting

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

Virus Reporting

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

Hardware Faults

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

Electronic Intrusion

For cases involving electronic intrusion, the goals of data integrity, data recovery, method of breach and intruder identification apply. Any daily activity 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, get immediate assistance.

Evidence

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

Collecting Evidence

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

Preserving Evidence

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

ⓘ ***Important !*** Do not try to restore the system until all evidence has been gathered.

Recording Evidence / Documenting Incident

Someone should be designated to document the incident/ suspicions key points: evidence, what occurred, timing, anticipated damage, and other such critical data to satisfy organization requirements.

Tracking Intrusions

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

Incident Patterns

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

Chapter 3
Access Control Rules

About Access Control

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

The Role of the IS Department

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

Access Control – Logging On

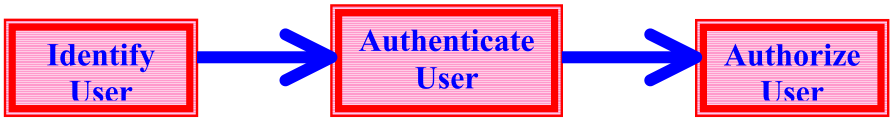
It is through a series of steps that the computer users can access, or log on to your organization's information.

Log On Types

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

- User ID
- Single signon
- Biometric
- Thumb print
- "Hamster"
- retina, iris, facial
- … and many more

The Log on Process



The Log On Process

Access Control Rules

The Access Control rules are grouped accordingly:

Technical Specialists Rules
Application Requirements Rules
Logging On Rules
Warning Banner Rules
Logging Off Rules
Identification (User ID) Rules
Authentication (Password) Rules
Authorization (Privileges) Rules
Sanctions Rules
Employment Status Change Rules

Technical Specialists Rules

The IS department is staffed with technical specialists that require having high level access to internal system functions. For this reason, it is important to carefully select and monitor IS activity as it relates to who is accessing what information.

Rule - Access by Technical Specialists

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

Explanation/ Key Points

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

Rule - Technical Specialists Security Check

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

Rule - Security Administration Activities

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

Application Requirements Rules

Rule - Application Controls

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

Logging On Rules

Rule - Unique User ID and Password

Every user must have a unique User ID and a confidential password. This User ID and password combination will be required for them to have access to your organization's information systems.

Rule - Unsuccessful Logon Attempts

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

Rule - Single Signon (Log On)

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

Rule - Disclosure of Incorrect Log on Information

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

This reduces the risk of intruders gaining knowledge of what they are doing wrong and being able to correct it.

Rule - Encrypted Log on Files

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

Rule - Logon Scripts

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

Rule - Third Party Logons

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

Rule - Giving Logon Information to the User

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

Rule - Limitation on Number of Daily Log Ons

To prevent unauthorized system usage, you should monitor excessive number of daily successful log ons.

Explanation/ Key Points

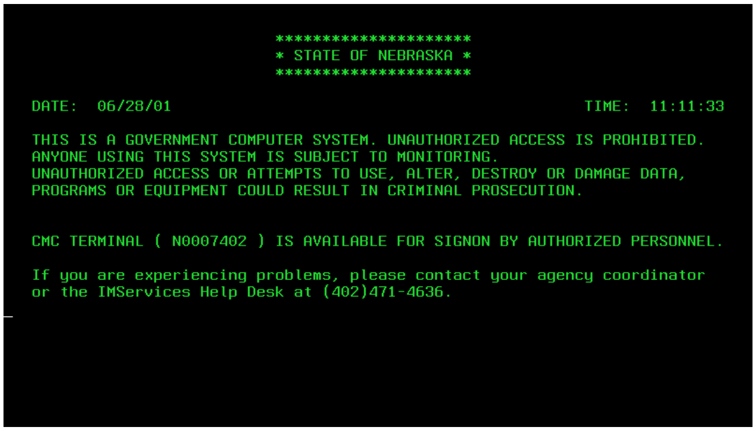
You may want to specify that the user is not permitted to log on more than **{10}** times a day. Any User ID that reaches this threshold is considered “high usage” and could be automatically blocked until the next day. Excessive log ons can help detect password sharing. If this high usage level continues, the User ID will be subject to immediate cancellation.

Warning Banner Rules

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

The warning banner should display:

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



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

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

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


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

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

Sample Warning Banner

Rule - Display a Warning Banner

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

Explanation/ Key Points

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

Rule - Warning Banner Keystroke Monitoring

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

Rule - Warning Banner Last Logon

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

Explanation/ Key Points

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

Rule - Warning Banner Information Disclosure

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

Explanation/ Key Points

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

Logging Off Rules

🕮 Rule - Automatic Log Off if No Activity

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

Explanation/ Key Points

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

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

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

🕮 Rule - Automatic Log Off at End of Day

All users should be automatically logged off at end of day. A procedure should be put in place to check all users at night to see if workstations have been left logged on.

Chapter 3 - Access Control Rules

Identification (User ID) Rules

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

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

Rule - Unique User ID

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

Rule - Prohibit Group User IDs

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

Rule - Dormant User IDs

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

Rule - Internet User ID Expiration

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

Rule - Granting Multiple User IDs

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

Explanation/ Key Points

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

Rule - Granting User IDs to Outsiders

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

Rule - Re-use of User IDs

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

Rule - Customer Privacy and User IDs

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

Rule - Distribution of User IDs

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

Rule - User ID Logs

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

Explanation/ Key Points

Suggested logs by User ID:

1. 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.

Authentication (Password) Rules

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

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

☝ ***Tip:*** Password management **-** Although the password is chosen by the user, it is up to IS to provide the guidelines to which they must comply.

Rule - Assign a Default Password

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

Explanation/ Key Points

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

Rule - Minimum/ Maximum Password Length

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

Explanation/ Key Points

Rule - Cyclical Previous Passwords

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

Explanation/ Key Points

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

Rule - Password Allowable Characters

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

Explanation/ Key Points

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

Rule - Passwords Lower and Upper Case

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

Explanation/ Key Points

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

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

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

Rule - Reusing Passwords / History

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

Explanation/ Key Points

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

ⓘ ***Important !*** If a user utilizes sensitive data and has a high access authority, they must NEVER use the same password twice.

Rule - Forced Expiration of Passwords

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

Explanation/ Key Points

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

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

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

Rule - Unsuccessful Passwords Attempts

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

Explanation/ Key Points

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

(a) revoked/ suspended until reset by the IS system administrator, Help desk, or security administrator.
(b) temporarily disabled for an extended period of time (no less than {3} minutes. (This is not the suggested choice.)
(c) disconnected, if using a dial-up or other external network connection.

Troubleshooting

Problem: What should I do if … I failed all attempts to log on?
Action: You must call IS to have them manually reset your password.

Rule - Proof Of Identify to Obtain a Password

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

Explanation/ Key Points

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

This can be automated by use of information known only to the user. This is acceptable for less secure systems. With more secure systems, it is best to go through a designated systems / network administrator, Help desk, or security administrator.

Troubleshooting

Problem: What should I do if … a user forgets their password?
Action: You must reset their password.

Rule - Distributing Passwords to Users

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

Explanation/ Key Points

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

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

Rule - Typing Passwords

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

Explanation/ Key Points

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

Rule - Resetting Passwords

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

Explanation/ Key Points

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

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

Rule - Dynamic Password Tokens

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

Rule - Seed for System Generated Passwords

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

Rule - Immediate Issue of System Generated Passwords

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

Rule - Storage of Passwords

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

Rule - Zeroization of Password Materials

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

Explanation/ Key Points

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

Rule - Password Based Boot Protection

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

Rule - Sending Passwords through the Mail

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

Rule - Password Encryption

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

Rule - Use of Duress Passwords

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

Rule - Changing Vendor Default Passwords

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

Rule - Passwords of Key Role Holders

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

Rule - Review Digital Certificates

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

Rule - Unauthorized Access to Passwords

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

Authorization (Privileges) Rules

Authorization, or privilege control is given at the User ID level and determines what the user can access. Once the user successfully logs on, they will have access to all the authorities, or privileges you have given to them. This allows for separation of duties, dual control, and other generally accepted security measures.

In order to define the user privileges, their roles need to be identified based on business functions. Then IS can determine what authorities are needed to perform these functions. The authorities to read, write, modify, update, or delete information from automated files or databases should be established by the owner(s) of the information.

Some users may be granted a specific combination of authorities. Users should not be given any authority beyond their needs. Access rules or profiles should be established in a manner that restricts users from performing incompatible functions or functions beyond their responsibility and enforces a separation of duties.

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

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

Explanation/ Key Points

☝ ***Tip:*** Menus should show only the options which that user can select.

Rule - Dual Access Controls

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

Rule - Privileges Granted by Groups

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

Rule - Users that Leave the Organization

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

📖 Rule - Systems Privileges

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

📖 Rule - Separation of Duties

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

Sanctions Rules

Rule - Revoking Access

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

Employment Status Change Rules

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

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

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**
Rule Date	**Rule Revision Date**	**Date Adopted**
Approval Name/ Code (signature)	**Rule Source**	**Audit Number/ Code**

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. …
5. Orientation …

Rule - Handling Terminations

Rule Statement

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

Policy Category Access Control	**Policy Standard** Employment Change	**Rule Number**
Rule Date	**Rule Revision Date**	**Date Adopted**
Approval Name/ Code (signature)	**Rule Source**	**Audit Number/ Code**

Explanation/ Key Points

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

Procedure

To handle employee terminations:

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

To handle employee resignations:

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

Chapter 4
Network Security Rules

About Network Security

Networks are common in most organizations to distribute processing and information to its internal and external employees, customers, and other business entities. Networks are also an access point to other systems, internet and other networks. Networks allow sharing of information, applications, and other computer resources. Dependence on networks requires availability 24 hours per day, every day of the year. Integrity and confidentiality are paramount.

Networks also represent major points of vulnerability to a large range of security problems. Public networks such as the internet compound the security threat. Remote access, connections between networks, internet access by workstations on the network, internet access to information and services, and other configurations make network security a complex problem. Networks can also enable a quicker spreading of problems, including computer viruses due to its accessibility of external and internal resources.

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

Internet and intranet sites must be protected from intrusion so that an unauthorized individual cannot alter data and information or compromise the integrity of state controlled networks. Intranet sites must be further protected by User IDs and passwords or other unique identifier so that access by unauthorized individuals is not allowed. Internet or intranet connections pose a risk of unauthorized access to state maintained data by compromising the integrity and privacy (where appropriate) of data. Potential consequences of unauthorized access include altering, erasing, or otherwise rendering the information invalid or unavailable by manipulating the data or the underlying programs.

The Role of the IS Department

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

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

The main IS network tasks are:

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

Network Security Rules

The Network Security rules are grouped accordingly:

Network/ Perimeter Security Rules
Firewalls Rules
Remote User / Dial-in Rules
Virus Handling Rules

Network / Perimeter Security Rules

Rule - Configuring Networks

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

Rule - Managing the Network

Only qualified IS technical staff should maintain the network.

Rule - Defending against Virus Attacks

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

Explanation/ Key Points

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

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

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

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

Rule - Handling Hoax Virus Warnings

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

Explanation/ Key Points

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

Rule - Installing Virus Scanning Software

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

Explanation/ Key Points

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

Rule - Modem Pool

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

Rule - Scanning for Modems

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

Rule - Dividing Large Networks

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

Rule - Network Connections with other Organizations

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

Rule - State-owned Resources

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

Rule - Network Controls

Network resources participating in the access of sensitive information or critical systems shall assume the security level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk. All network components must be identifiable and restricted to their intended use.

Rule - Unattended Network Terminals

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

Rule - Sensitive Information Prohibited from Network Printer

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

Rule - Controlling Network Analyzers

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

Rule - Setting up Intranet Access

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

Explanation/ Key Points

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

Rule - Setting up Extranet Access

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

Explanation/ Key Points

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

Chapter 4 - Network Security Rules

Rule - Network Diagrams

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

Rule - Default Passwords on Network Hardware

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

Rule - Keeping Track of Modems

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

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

Rule - Network Audit

An audit of network security should be conducted annually.

Rule - Perimeter Security

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

Explanation/ Key Points

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

Rule - Accessing Network Vulnerability

IS shall develop and use an on-going process to assess vulnerability of the network and risk in order to maintain adequate perimeter security controls.

Rule - Network Entry Controls

Appropriate access controls such as identification, authentication, certification, and authorization must be implemented to control entry to the network. *See Chapter 3 Access Control Rules.*

Rule - Monitoring Network Entry

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

Rule - Perimeter security 24/ 7

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

Rule - Implementing Perimeter Protection

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

Rule - Defending against Denial of Service Attack

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

Explanation/ Key Points

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

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

Rule - Inventory of Connections to External Networks

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

Rule - Contact Numbers in Directories

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

Rule - Isolating Sensitive Systems from Network

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

Rule - Connecting Modems to Network Prohibited

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

Rule - Modem Pools

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

Rule - Highest Risk Elements on the Network

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

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

Firewalls Rules

Rule - Firewalls Required for all Dial Up Connections

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

Rule - Firewalls Must Run on Dedicated Computers

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

Rule - Changing Firewall Configurations

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

Rule - Internet Connections Need Firewalls

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

Remote User / Dial-in Rules

Rule - Unsuccessful Logon Attempts

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

Rule - Remote Systems Connecting to Production

All computers which have remote dialogs with your organization's production systems must run an access control package approved by the proper authorities.

Rule - Issuing Laptops/ Portable Computers

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

Rule - Controlling Remote Access

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

Rule - Dial Up access needs Protection

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

Rule - Using Modems/ ISDN, DSL Connections

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

Explanation/ Key Points

There are dangers in using modems, ISDN links, and DSL connections to access public telephone networks to link diverse parts of your system.

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

Rule - Connecting Networks to Third Party Networks

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

Explanation/ Key Points

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

Rule - Extended User Authentication Systems for Dial Up

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

Rule - Use of Cable Modems

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

Rule - Using Encryption Techniques

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

Rule - Answering Incoming Calls

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

Virus Handling Rules

Rule - Virus Checking Programs on PCs and LAN Servers

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

Rule - Testing for Viruses on a Stand-alone Computer

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

Rule - Virus Checking at Firewalls, Servers, and Desktops

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

Rule - Two Virus Screening Software Packages

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

Rule - Floppy Virus Checking Decal

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

Rule - Integrity Checking Programs

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

Rule - Decrypting Before Checking for Virus

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

ⓘ ***Important !*** Many virus checking programs cannot detect viruses in encrypted files.

Rule - Write Protection and Virus

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

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

About E-mail, Internet, and E-commerce

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

The Role of the IS Department

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

E-mail, Internet, and E-commerce Rules

The E-mil, Internet, and E-commerce rules are grouped accordingly:

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

E-mail Rules

Rule - E-mail Point of Entry

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

Rule - Central E-mail Systems/ Anti-Virus

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

Rule - Deleting and Destroying E-mail

Internal correspondence must be disposed of when no longer needed.

Explanation/ Key Points

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

Rule - Using E-mail as a Database

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

Rule - Recording and Retaining E-mail

Your organization's systems administrators must establish and maintain a systematic process for the recording, retention, and destruction of electronic mail messages and accompanying logs. The destruction of both logs and the referenced electronic mail messages must be postponed whenever a subpoena, discovery motion, or other legal notice is received. Such destruction should also be postponed if the material might be needed for an imminent legal action.

Internet Rules

Rule - Setting up Internet Access

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

Explanation/ Key Points

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

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

Rule - Intrusion Detection Systems

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

Rule - Public Servers on Internet

Public internet servers must be placed on subnets separate from internal networks. Routers or firewalls must be employed to restrict traffic from the public servers to internal networks.

Rule - Internet Commerce Servers - Demilitarized Zone

All internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls in a demilitarized zone.

Rule - Internet Commerce Servers - Encryption

To prevent intruders from interfering with internet commerce activities, all internet commerce servers (web servers, database servers, payment servers, security servers, etc.) must employ unique digital certificates and must use encryption to transfer information in and out of these servers. An exception is made for web servers, FTP servers, and any other servers supporting communications with customers, prospects, or other members of the public.

Rule - Downloading Internet Files / Anti-virus

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

📖 Rule - Firewalls and Internet Connections

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

📖 Rule - Internet Connections and Shared Directories

Your organization’s computers that are internet-connected or directly reachable through the internet are prohibited from using shared directory systems, sometimes called shared file systems. These systems allow a user to obtain access to more than one computer's file system with only a single log-in process. Exceptions are made for internet commerce and other systems where a multiple machine architecture involves automatically passing users with severely restricted privileges from one computer to another.

📖 Rule - Developing a Web Site

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

📖 Rule - Web Browsers

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

Explanation/ Key Points

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

📖 Rule - Contact Information on Web Site

The opening pages of all your organization’s web sites must include information security contact information (e-mail address, phone number, etc.) for the Information Security Department or other such area.

E-commerce Rules

🕮 Rule - Protecting E-commerce Web Sites

E-commerce processing systems are to be designed with protection given the highest priority. It is not simply enough to safeguard the interaction between the customer and the web sites server. The software that performs the E-commerce function may be at risk.

🕮 Rule - Securing E-commerce Networks

E-commerce operates on and through communication networks. These network should be secured and protected against unauthorized access.

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

Chapter 6
Equipment / Hardware Rules

About Equipment and Hardware

Most organizations computer systems require a vast network of PCs and terminals and other supporting equipment like printers, UPS, and such. It is important to not only secure the physical hardware itself, but also to be aware of what information the equipment could contain.

The safeguards taken to secure hardware is dependent on its physical location and the sensitivity of its contents. Your organization may have a secured computer operations room with strict access limitations that houses most of the core equipment that runs the computer systems. However, each user area may not require a locked room, but the information may need to be protected that they use to do their jobs.

The Role of the IS Department

It is the responsibility of the IS department to install, maintain, test and secure the hardware at most organizations. If the equipment is old, they are required to dispose of the equipment in the proper fashion.

Equipment and Hardware Rules

The Equipment and Hardware rules are grouped accordingly:

Hardware Rules
Disposal Rules

Chapter 6 - Equipment / Hardware Rules

Hardware Rules

Rule - Purchasing and Installing New Hardware

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

Explanation/ Key Points

In addition to adequate capacity and performance reliability, new hardware systems must have proper safeguards. All major purchases should be evaluated and incorporated into existing security solutions.

Rule - Hardware Security - Down Time

All equipment in the process of being supported, that is, during any diagnostic testing, repair, or routine maintenance, should follow the same security safeguards as when it is operational. Should the safeguards be removed, the hardware and its contents will be at high risk for an incident. Removing safeguards can only be done with proper approval and with extreme caution.

Rule - Moving / Relocating Hardware

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

Disposal Rules

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

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

Rule - Person Authorized to Destroy Sensitive Information

Equipment owned by your organization may only be disposed of by authorized technical staff or a bonded destruction service who understand the information security risks.

Explanation/ Key Points

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

Rule - Destruction of Records

IS should not destroy or dispose of potentially important records or information without specific advance management approval. Unauthorized destruction or disposal of your organization's records is prohibited. Records and information must be retained if: (1) they are likely to be needed in the future, (2) regulation or statute requires their retention, or (3) they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts.

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

Rule - Object Reuse

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

Rule - Using External Disposal Firms

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

Rule - Zeroization of Password Materials

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

Explanation/ Key Points

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

Rule - Sensitive Information Destruction Before Servicing

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

Explanation/ Key Points

For example, if a hard disk drive were to crash, the drive might be sent to a computer repair service. The service company could examine the data on the drive, perhaps leading to unauthorized disclosure of sensitive information. To counter this risk, the drive could be degaussed prior to being sent to the service vendor. Such sensitive information destruction makes sense only if the information has been properly backed-up or if the consequences of disclosure are very severe. A more practical alternative would be to require that all hard drives storing sensitive data employ encryption, in which case there is no problem about sending the drive to an outside vendor. Another approach is to require confidentiality agreements (NDAs) from all third parties.

Rule - Sensitive Information Disposal

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

Explanation/ Key Points

Degaussing involves subjecting magnetic storage media such as floppy disks to a strong magnetic field which will then erase the information stored thereon.

Zeroization involves overwriting the storage media with repeated sequences of zeros and ones, thereby obliterating the data.

With most operating systems, standard disk file "delete" and "erase" commands simply delete the entry in a file allocation table (FAT) or directory;

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

Rule - Erasing before Giving to a Third Party

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

Rule - Hardcopy Sensitive Information Disposal

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

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

Rule - Using Removable Storage Media

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

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

Chapter 7
Physical Security/ Premises Rules

About Physical Security/ Premises

Good security practices are not only required for software, hardware and information, but also for the physical security of the facility, the people and the infrastructure of your organization.

All organizations must develop and implement rules which include at least the following:

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

The Role of the IS Department

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

Physical Security/ Premises Policy Statements

The Physical Security/ Premises rules are grouped accordingly:

Building/ Room Access Rules
Environmental Rules
Guards / Outside Security Organizations/ Equipment Rules

Chapter 7 - Physical Security/ Premises Rules

Building/ Room Access Rules

Rule - Propped Open Doors to Computer Room

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

Rule - Network Components Protection

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

Rule - Physical Access to Sensitive Information

Access to every office, computer room, and work area containing sensitive information must be physically restricted. All employees working in these areas must have the proper physical access authorities (receptionists keys, file cabinets / closet key locks, magnetic card door locks, etc.).

Rule - Hard Drive Security

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

Environment Rules

Rule - Environment Controls

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

Rule - Installing and Maintaining Network Cabling

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

Explanation/ Key Points

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

Rule - Supplying Continuous Power to Critical Equipment

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

Rule - Managing and Maintaining Backup Power Generators

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

Explanation/ Key Points

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

Guards/ Outside Security Organizations / Equipment Rules

Rule - Working with Guards / Guard Stations

All guards should be made aware of the policies, standards, and rules governing physical access. They need to know what and how to enforce any violators according to the published rules.

Rule - Outside Security Systems

If your organization uses vendor security software to control and support the physical access points, then it is important that user authorities assigned in IS match those in the security system regarding information access.

Rule - Security Equipment

Security equipment must follow the same technical security standards as any other hardware or equipment used at your organization. This applies to such devices as cameras, video surveillance, motion detectors, remote web viewing and such.

Chapter 8
Systems Development Rules

About Systems Development

Systems development is the main function of the IS department. This involves programming software or implementing purchased software for use with your organization's data. The purpose of this chapter is to provide guidance to the development team to control and maintain efficient practices to better protect data from exposure, unauthorized access, and possible corruption.

The Role of the IS Department

One of the main roles of the IS department is to develop and maintain software code that is designed to perform specific business and technical functions. The key tasks required to perform this software development is programming and debugging code, testing results and expected outcomes using test data, and finally incorporating the new code into the production systems for end-users to use with live data.

Systems Development Rules

The Systems Development rules are grouped accordingly:

Software Development/ Programming Rules
Data Management Rules
Software Maintenance / Upgrades Rules
Software Testing Rules
Systems Documentation Rules

Chapter 8 - System Development Rules

Systems Development / Programming Rules

Rule - Software Development

The IS programmers must always follow a formalized development process according to your organization's policies, standards, rules, and naming conventions.

Explanation/ Key Points

Controls are required to protect code and data integrity.

Rule - Development Security Requirements

IS must determine how each system of any new development should be accessed and protected within itself and as it interfaces with other systems. This should be build into the development process.

Rule - Developed Software Notice of Failure

When software fails to produce the expected results, it must always provide either an error message or some other indication of failure, that data integrity cannot be confirmed.

Rule - Test to Production - Removing Paths

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

Rule - Test vs. Production Files Naming Conventions

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

Rule - Separation of Development and Live Environments

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

Rule - System Developers and Production

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

Rule - Interfacing Applications Software/ Systems

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

Explanation/ Key Points

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

Rule - Special Labeling for Non-production Business

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

Rule - System Interruption

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

Rule - Systems Utilities Prohibited from Production Storage

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

Chapter 8 - System Development Rules

Rule - Development Using Licensed Software

In addition to in-house developed code, your organization might purchase a software package that may or may not require further customization. To comply with legislation and to receive continued vendor support, the terms and conditions of all vendor licensed software are to be strictly adhered to.

Explanation/ Key Points

Using unlicensed software can be a criminal offense.

Rule - Managing Program Libraries

IS should designate specific technical staff to have access to operational program libraries within your system where you keep the source code of your live systems. Live and development libraries should always be kept separate.

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

Rule - Separating Duties - Systems Development

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

Explanation/ Key Points

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

Data Management Rules

Rule - Managing Databases

The integrity of the organization's databases must be maintained at all times.

Rule - Maintaining Data Structures

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

Explanation/ Key Points

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

Rule - Setting up New Databases

Databases must be carefully stored, housed and tested according to the sensitivity of the data and its usage.

Rule - Confidential Data

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

Software Maintenance / Upgrades Rules

Rule - Applying Patches to Software

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

Explanation/ Key Points

Often intruders can penetrate old code forcing software vendors/ developers to produce code to deter future intrusions. Keeping up with the latest version of software also keeps up with the latest security measures.

Rule - Responding to Vendor Recommended Software Upgrades

IS should carefully weigh the risks of software upgrade with the anticipated benefits and necessity for such a change.

It is suggested that you always upgrade to have the latest functionality and also the latest security.

Rule - Operating System/ Utilities Upgrades

IS should keep all core systems, including all operating systems and utilities current. Necessary upgrades to the operating system must have the associated risks identified and be carefully planned, incorporating tested fall back procedures.

Explanation/ Key Points

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

Rule - Change Control Process

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

All systems must employ a change control process to control the access to data, to protect the integrity of the data, and to avoid accidental or intention corruption of data and programs. This process should account for who made the changes, be sure the changes are timely and secure.

Explanation/ Key Points

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

Rule - Controlling old Versions of Programs

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

System Testing Rules

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

Rule - System Developers and Testing

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

Rule - Restricted Use of Diagnostics

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

Rule - Testing Third Party Software

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

Rule - Software Testing with Sensitive Data

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

Rule - Controlling Test Environments

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

Rule - Using Live Data for Testing

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

Explanation/ Key Points

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

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

Rule - Testing Systems and Equipment

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

Explanation/ Key Points

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

Inadequate testing can threaten the integrity of your data.

Systems Documentation Rules

Rule - Systems Documentation Security

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

Explanation/ Key Points

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

Rule - Maintaining a Hardware / Software Inventory

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

Explanation/ Key Points

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

Rule - Hardware Documentation

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

Explanation/ Key Points

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

Keeping hardware maintenance is important to your organization’s infrastructure.

Rule - Controlling Program Listings

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

Rule - Documentation Version Control

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

Rule - Required Documentation for Production

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

Chapter 9
Disaster Recovery Rules

About Disaster Recovery

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

It is not the intent of this chapter to guide you through the process of designing and developing a disaster recovery plan. It does, however, give the IS department a set of Disaster Recovery Rules to follow to incorporate good business practices into the technical staffs daily tasks.

The Role of the IS Department

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

Contingency Planning

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

Disaster Recovery Plan

The reason for a disaster recovery plan is to rapidly recover your operations from a disaster. This will almost always involve restoring information from backups that have been stored in a safe place.

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

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

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

- Information resources must be available when needed. Continuity of information resources supporting critical services must be ensured in the event of a disruption to business or a disaster, which makes critical systems unavailable.

- Risks to information resources must be managed. The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected.

Testing the Plans/ Responding to Disaster

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

Your organization's Incident Response Team is trained to react in an emergency according to the disaster recovery plan. *See Chapter 2 Security Incidents and Reporting*.

Disaster Recovery Rules

The Disaster Recovery rules are grouped accordingly:

Disaster Recovery Rules

Rule - Doing a Business Impact Analysis

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

Rule - Classification System

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

Rule - Identifying Sensitive Information

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

Rule - Safeguards and Mitigation Strategies

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

Rule - Business Resumption

IS should bring all systems to full operation as soon as possible to resume business operations.

ⓘ ***Important !*** Be sure to gather and preserve all incident related evidence before hastily restoring the system.

Rule - Contingency Plans for Different Types of Disruption

IS should consider all types all disruption (natural, terrorist, accidental, etc.) and have a contingency plan for all possible causes.

Rule - Implementing a Disaster Recovery Plan

Each organization is responsible for implementing the disaster recovery plan.

Chapter 9 - Disaster Recovery Rules

Rule - Escalating Responses

Procedures should be put in place for reporting incidents and implementing the disaster recovery plan and escalating your organization’s response to a disaster.

Rule - Disaster Recovery Plan – Training, Testing, Practice

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

Rule - Disaster Recovery Plan Annual Review and Revision

Each organization should review and revise the disaster recovery plan yearly. This will include updating asset inventory, risk assessment tools, safeguards, contingency and resumption plans. The updates to the plans should then be re-tested and practiced.

Rule - Human Factor

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

Off-Site Storage Rules

Offsite storage of information is a basic rule of disaster survival. It is necessary to be able to conduct your business from an alternate location.

Rule - Off Site Storage of Essential Information

Backups of essential business information, software, applications, papers, and other media must be stored in an environmentally protected and access controlled site. All information systems, infrastructure, configuration of systems necessary to rebuild your organization's operations should also be kept off site.

Rule - Physical Separation of Sites

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

Rule - Multiple Site Storage of Backup Documents

Backup documents should be stored in multiple sites. This prevents losing the backup information should a disaster strike the backup facility.

Backup, Recovery and Archived Data Rules

Your organization should never lose more information than that which has changed since your last backup. Backups are fundamental to the installation of new systems and after the destruction of your existing systems. The storage process of the backup, number of generations and location are all factors making up the backup process.

Rule - Managing Backup and Recovery Procedures

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

Rule - Backup all New Software

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

Rule - Frequency of Backing up Data

The frequency of doing a backup depends on your organization's needs. It is usually done daily, and monthly.

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

Rule - Backup Scope

The scope of backups can be full, incremental, or differential. The scope of what gets backed can change from organization to organization.

Rule - Backing Up on Portable Computers

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

Rule - Safeguarding your Backups

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

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

Rule - Two Backup Copies

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

Rule - Users Backing Up

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

Rule - Automatic Backup to Network

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

Rule - Users Notified of Backups

All users should be made aware that their data and transactions are part of the backup process. This means that information stored on your organization's systems, even if a user has deleted it, is recoverable .

Rule - Backup Information Retention

Information must be retained for as long as necessary but for no longer. Information must be destroyed or sent to archives when no longer needed after **{2}** years.

Rule - Users Restoring Data

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

Rule - Archiving Information

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

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

Rule - Archival Storage

The computer data media used for storing sensitive, critical, or valuable information in archives must be high quality and must be periodically tested to ensure that it can properly respond to requests and that it is being reliably retained.

Rule - Preserving Data in Archival Storage

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

Rule - Archive Retention

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

Rule - Regular Purging of Information

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

Chapter 10
Getting ISS Help

Getting ISS Help

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

Call for ISS Support

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

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

Troubleshooting Chart

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

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

Appendix

The following documents are contained in this appendix:

Appendix A - List of Rules

The following list is a summary of all the rules in this handbook by category:

Technical Specialists Rules (See Chapter 3)

- Rule - Access by Technical Specialists
- Rule - Technical Specialists Security Check
- Rule - Security Administration Activities

Application Requirements Rules (See Chapter 3)

- Rule - Application Controls

Logging On Rules (See Chapter 3)

- Rule - Unique User ID and Password
- Rule - Unsuccessful Logon Attempts
- Rule - Single Sign On (Log On)
- Rule - Disclosure of Incorrect Logon Information
- Rule - Encrypted Logon Files
- Rule - Logon Scripts
- Rule - Third Party Logons
- Rule - Giving Logon Information to the User
- Rule - Limitation on Number of Daily Log Ons

Warning Banner Rules (See Chapter 3)

- Rule - Display a Warning Banner
- Rule - Warning Banner Keystroke Monitoring
- Rule - Warning Banner Last Logon
- Rule - Warning Banner Information Disclosure

Logging Off Rules (See Chapter 3)

- Rule - Automatic Log Off if No Activity
- Rule - Automatic Log Off at End of Day

Identification/ User ID Rules (See Chapter 3)

- Rule - Unique User ID
- Rule - Prohibit Group User IDs
- Rule - Dormant User IDs
- Rule - Internet User ID Expiration
- Rule - Granting Multiple User IDs
- Rule - Granting User IDs to Outsiders
- Rule - Re-use of User IDs
- Rule - Customer Privacy and User IDs

- Rule - Distribution of User IDs
- Rule - User ID Logs

Authentication (Password)Rules (See Chapter 3)

- Rule - Assign a Default Password
- Rule - Minimum/ Maximum Password Length
- Rule - Cyclical Previous Passwords
- Rule - Password Allowable Characters
- Rule - Passwords Lower and Upper Case
- Rule - Reusing Passwords / History
- Rule - Forced Expiration of Passwords
- Rule - Unsuccessful Passwords Attempts
- Rule - Proof Of Identify to Obtain a Password
- Rule - Distributing Passwords to Users
- Rule - Typing Passwords
- Rule - Resetting Passwords
- Rule - Dynamic Password Tokens
- Rule - Seed for System Generated Passwords
- Rule - Immediate Issue of System Generated Passwords
- Rule - Storage of Passwords
- Rule - Zeroization of Password Materials
- Rule - Password Based Boot Protection
- Rule - Sending Passwords through the Mail
- Rule - Password Encryption
- Rule - Use of Duress Passwords
- Rule - Changing Vendor Default Passwords
- Rule - Passwords of Key Role Holders
- Rule - Review Digital Certificates
- Rule - Unauthorized Access to Passwords

Authorization (Privileges) Rules (See Chapter 3)

- Rule - Privileges Granted on a Need-to-Know Basis
- Rule - Dual Access Controls
- Rule - Privileges Granted by Groups
- Rule - Users that Leave the Organization
- Rule - Systems Privileges
- Rule - Separation of Duties

Sanctions Rules (See Chapter 3)

- Rule - Revoking Access

Employment Status Change Rules (See Chapter 3)

- Rule - Setting Up a New User (New Hire)
- Rule - Handling Terminations

Appendix

Network / Perimeter Security Rules (See Chapter 4)

- Rule - Configuring Networks
- Rule - Managing the Network
- Rule - Defending against Virus Attacks
- Rule - Handling Hoax Virus Warnings
- Rule - Installing Virus Scanning Software
- Rule - Modem Pool
- Rule - Scanning for Modems
- Rule - Dividing Large Networks
- Rule - Network Connections with other Organizations
- Rule - State-owned Resources
- Rule - Network Controls
- Rule - Unattended Network Terminals
- Rule - Sensitive Information Prohibited from Network Printer
- Rule - Controlling Network Analyzers
- Rule - Setting up Intranet Access
- Rule - Setting up Extranet Access
- Rule - Network Diagrams
- Rule - Default Passwords on Network Hardware
- Rule - Keeping Track of Modems
- Rule - Network Audit
- Rule - Perimeter Security
- Rule - Accessing Network Vulnerability
- Rule - Network Entry Controls
- Rule - Monitoring Network Entry
- Rule - Perimeter security 24/ 7
- Rule - Implementing Perimeter Protection
- Rule - Defending against Denial of Service Attack
- Rule - Inventory of Connections to External Networks
- Rule - Contact Numbers in Directories
- Rule - Isolating Sensitive Systems from Network
- Rule - Connecting Modems to Network Prohibited
- Rule - Modem Pools
- Rule - Highest Risk Elements on the Network

Firewalls Rules (See Chapter 4)

- Rule - Firewalls Required for all Dial Up Connections
- Rule - Firewalls Must Run on Dedicated Computers
- Rule - Changing Firewall Configurations
- Rule - Internet Connections Need Firewalls

Remote User / Dial-in Rules (See Chapter 4)

- Rule - Unsuccessful Logon Attempts
- Rule - Remote Systems Connecting to Production
- Rule - Issuing Laptops/ Portable Computers
- Rule - Controlling Remote Access
- Rule - Dial Up access needs Protection

- Rule - Using Modems/ ISDN, DSL Connections
- Rule - Connecting Networks to Third Party Networks
- Rule - Extended User Authentication Systems for Dial Up
- Rule - Use of Cable Modems
- Rule - Using Encryption Techniques
- Rule - Answering Incoming Calls

Virus Handling Rules (See Chapter 4)

- Rule - Virus Checking Programs on PCs and LAN Servers
- Rule - Testing for Viruses on a Stand-alone Computer
- Rule - Virus Checking at Firewalls, Servers, and Desktops
- Rule - Two Virus Screening Software Packages
- Rule - Floppy Virus Checking Decal
- Rule - Integrity Checking Programs
- Rule - Decrypting Before Checking for Virus
- Rule - Write Protection and Virus

E-mail Rules (See Chapter 5)

- Rule - E-mail Point of Entry
- Rule - Central E-mail Systems/ Anti-Virus
- Rule - Deleting and Destroying E-mail
- Rule - Using E-mail as a Database
- Rule - Recording and Retaining E-mail

Internet Rules (See Chapter 5)

- Rule - Setting up Internet Access
- Rule - Intrusion Detection Systems
- Rule - Public Servers on Internet
- Rule - Internet Commerce Servers - Demilitarized Zone
- Rule - Internet Commerce Servers - Encryption
- Rule - Downloading Internet Files / Anti-virus
- Rule - Firewalls and Internet Connections
- Rule - Internet Connections and Shared Directories
- Rule - Developing a Web Site
- Rule - Web Browsers
- Rule - Contact Information on Web Site

E-commerce Rules (See Chapter 5)

- Rule - Protecting E-commerce Web Sites
- Rule - Securing E-commerce Networks

Hardware Rules (See Chapter 6)

- Rule - Purchasing and Installing New Hardware
- Rule - Hardware Security - Down Time

- Rule - Moving / Relocating Hardware

Disposal Rules (See Chapter 6)

- Rule - Person Authorized to Destroy Sensitive Information
- Rule - Destruction of Records
- Rule - Object Reuse
- Rule - Using External Disposal Firms
- Rule - Zeroization of Password Materials
- Rule - Sensitive Information Destruction Before Servicing
- Rule - Sensitive Information Disposal
- Rule - Erasing before Giving to a Third Party
- Rule - Hardcopy Sensitive Information Disposal
- Rule - Using Removable Storage Media

Building/ Room Access Rules (See Chapter 7)

- Rule - Propped Open Doors to Computer Room
- Rule - Network Components Protection
- Rule - Physical Access to Sensitive Information
- Rule - Hard Drive Security

Environment Rules (See Chapter 7

- Rule - Environment Controls
- Rule - Installing and Maintaining Network Cabling
- Rule - Supplying Continuous Power to Critical Equipment
- Rule - Managing and Maintaining Backup Power Generators

Guards/ Outside Security Organizations / Equipment Rules (See Chapter 7)

- Rule - Working with Guards / Guard Stations
- Rule - Outside Security Systems
- Rule - Security Equipment

Systems Development / Programming Rules (See Chapter 8)

- Rule - Software Development
- Rule - Development Security Requirements
- Rule - Developed Software Notice of Failure
- Rule - Test to Production - Removing Paths
- Rule - Test vs. Production Files Naming Conventions
- Rule - Separation of Development and Live Environments
- Rule - System Developers and Production
- Rule - Interfacing Applications Software/ Systems
- Rule - Special Labeling for Non-production Business
- Rule - System Interruption
- Rule - Systems Utilities Prohibited from Production Storage
- Rule - Development Using Licensed Software

- Rule - Managing Program Libraries
- Rule - Separating Duties - Systems Development

Data Management Rules (See Chapter 8)

- Rule - Managing Databases
- Rule - Maintaining Data Structures
- Rule - Setting up New Databases
- Rule - Confidential Data

Software Maintenance / Upgrades Rules (See Chapter 8)

- Rule - Applying Patches to Software
- Rule - Responding to Vendor Recommended Software Upgrades
- Rule - Operating System/ Utilities Upgrades
- Rule - Change Control Process
- Rule - Controlling old Versions of Programs

System Testing Rules (See Chapter 8)

- Rule - System Developers and Testing
- Rule - Restricted Use of Diagnostics
- Rule - Testing Third Party Software
- Rule - Software Testing with Sensitive Data
- Rule - Controlling Test Environments
- Rule - Using Live Data for Testing
- Rule - Testing Systems and Equipment

Systems Documentation Rules (See Chapter 8)

- Rule - Systems Documentation Security
- Rule - Maintaining a Hardware / Software Inventory
- Rule - Hardware Documentation
- Rule - Controlling Program Listings
- Rule - Documentation Version Control
- Rule - Required Documentation for Production

Disaster Recovery Rules (See Chapter 9)

- Rule - Doing a Business Impact Analysis
- Rule - Classification System
- Rule - Identifying Sensitive Information
- Rule - Safeguards and Mitigation Strategies
- Rule - Business Resumption
- Rule - Contingency Plans for Different Types of Disruption
- Rule - Implementing a Disaster Recovery Plan
- Rule - Escalating Responses
- Rule - Disaster Recovery Plan – Training, Testing, Practice
- Rule - Disaster Recovery Plan Annual Review and Revision

- Rule - Human Factor

Off-Site Storage Rules (See Chapter 9)

- Rule - Off Site Storage of Essential Information
- Rule - Physical Separation of Sites
- Rule - Multiple Site Storage of Backup Documents

Backup, Recovery and Archived Data Rules (See Chapter 9)

- Rule - Managing Backup and Recovery Procedures
- Rule - Backup all New Software
- Rule - Frequency of Backing up Data
- Rule - Backup Scope
- Rule - Backing Up on Portable Computers
- Rule - Safeguarding your Backups
- Rule - Two Backup Copies
- Rule - Users Backing Up
- Rule - Automatic Backup to Network
- Rule - Users Notified of Backups
- Rule - Backup Information Retention
- Rule - Users Restoring Data
- Rule - Archiving Information
- Rule - Archival Storage
- Rule - Preserving Data in Archival Storage
- Rule - Archive Retention
- Rule - Regular Purging of Information

Index