State of Nebraska

Information Systems Security (ISS)

Computer User's Security **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}

{Computer User's Security Handbook}

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

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

State of Nebraska
Information Security Guidelines

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

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

Computer User's Security Handbook

Version 1.0
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

Welcome to the age of technology, where information is readily available and easy to access. Information and your computer systems are critical assets that support your organization's current and future business practices. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, and employees.

In general, security is smart business practices. You, the employee, therefore are a key factor in protecting information, as you use it in your daily job. The intent of this guide is to educate you on information security by making you aware of threats and risks, giving you a good set of rules to incorporate into your own business practices, and to know what to do if you encounter a security violation.

Your ISS Program

Information Security Systems (ISS) refers to the programs and technology your organization puts in place to protect its information. This ISS program has been designed with the employee in mind. It focuses on the tools you require to do your job, your work habits, and even your work area.

ISS is multi-departmental, multi-disciplinary, and multi-organizational in nature. This means that information security cannot possibly be adequately addressed by a single department within your organization. Information can be found nearly everywhere in an organization and nearly every worker utilizes information in order to do their job. It is only natural that every worker should be specifically charged with responsibility for information security.

Computer users may be employees, temporaries, contractors, consultants, or third parties with whom special arrangements have been made. If you have been permitted to use information, you must also have the understanding that you must properly protect it.

It Takes a T.E.A.M.

It takes a T.E.A.M. and you are an important part of it. All employees, consultants, contractors, and temporaries must be provided with sufficient training and supporting reference materials to allow you to properly protect your organization's information resources. You should be allowed sufficient on-the-job time to acquaint yourself with the ISS rules and to know what to do in the event of an incident.

Together
Everyone
Achieves
More

Compliance

All computer users must be subject to the same rules and compliance of those rules. It is your responsibility, as a State of Nebraska employee, to comply with all rules of your organization.

Compliance Form

(… Explain the purpose of any compliance form(s) you choose to use. …)

Consequences of Non-Compliance or Violation

(…Explain what happens if an employee is found to be in violation of rules…)

Using this Guide

This **{Computer User Security Handbook}** is a reference tool for the employees and contractors of the State of Nebraska. It is written generically to all management and skill levels. It defines the general security areas, accompanying rules, and any procedures or "how to" steps for any security tasks you 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 you 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 / Office
- Physical/ People Security
- Copyright
- Acceptable Use

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:

- Glossary (Appendix)
- Summary list of Rules (Appendix)
- ISS Overview (Chapter 1)
- Incident Reporting Chart (Chapter 2)
- 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

ISS At-a-Glance

In order to fully understand the purpose of the rules in this Guide, it is important to know more about ISS Security. This section gives you a brief overview of the key areas and reasons why we need to protect your organization's information.

Understanding ISS Risks and Threats

One of the biggest concerns facing organizations today is to anticipate the type of security threats or intruders that could occur. In order to safeguard against any attack, it is necessary to understand how and what the intruder is after. Employee awareness of the potential dangers facing the organization is critical.

About Intruders

Intruders can come in from the outside or be an internal worker. There are amateur and professional intruders. Intruders can be very technical and persistent. Intruders are also adaptable. If you pick the top 10 risks to safeguard, they'll pick 11 or 26.

Types of Intruders to Beware Of

Hacker

A hacker is an individual whose primary aim is to penetrate the security defenses of large, sophisticated computer systems. A truly skilled hacker can penetrate a system right to the core and withdraw again without leaving a trace of the activity. Hackers are a threat to all computer systems which allow access from outside your organization's premises. The world's primary target, the pentagon, is attacked on an average of 1 every 3 minutes. A hacker is also called a black hat

Virus

Malicious software like a virus is a software program which replicates itself and spreads onto various data storage media (floppy disks, magnetic tapes, etc.) and/or across a network. The symptoms of virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.

Social Engineering

Social engineering is the process of convincing people to divulge information that they should not. Often built on false pretenses, and misidentification, social engineering is extremely effective. This is accomplished by name dropping, gaining your confidence, and sometimes through intimidation. Social engineering involves the manipulation of people rather than technology to successfully breach your organization's security.

ⓘ ***Important !*** Social engineering remains the single greatest security risk, despite our advances in technology, and many of the most damaging security penetrations are the result of social engineering.

Types of Incidents/ Attacks

- Steal information
- Disclosure of information
- Deface property (mutilate a web site)
- Change environment (redirect printers)
- Destroy and Ruin (change information, put garbage in information, delete information)
- Denial of Service (break the flow of information, cause excess information traffic to tie up all further processing)

What is Disclosure?

Revealing information to the public or media can be disastrous to an organization. The intent of many attackers is to reveal confidential information or disclose information prior to its release.

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

Chapter 2
Security Incidents & Reporting

About Security Incidents

The biggest role you can play in the ISS program is to be in tune to your surroundings so you will notice when something seems unusual. You, the employee, use the system day after day, so are often the one to spot unusual behavior or even incidents in actions.

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

Suspicions and Incidents

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

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

Be Alert !

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

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.

Preserving Evidence

If possible, do whatever you can to quickly gather evidence of what you are witnessing. 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, or other unusual behaviors prior to contacting your manager. Timing is critical and the evidence may no longer appear any more.

Gather Evidence … Report it… and Be Prompt!

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

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

Don’t Resolve it Yourself

Not under any circumstances should you, the employee, attempt to prove the existence of potential or current weaknesses, or try to solely resolve suspicions, or incidents, unless you have been specifically assigned this task.

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

Your Incident Response Team

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.

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

Anonymity and Protection

To encourage reporting, your organization may wish to publicize the fact that reports can be made anonymously. Using a voice messaging systems also encourages reporting if you know your will receive an answering machine instead of a person.

If you have reported security issues to your organization in good faith, your organization will protect you if you report what you believe to be a violation of laws or regulations, or conditions that could jeopardize the health or safety of other workers. You will not be terminated, threatened, or discriminated against because you report what you perceive to be a wrongdoing or dangerous situation.

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.

Reporting Types

Internal Reporting

This reporting structure is internal to your organization and may include one or all of the following:

- security department (officers, managers, and staff)
- IS Help desk
- your manager
- security guard(s)
- information owners
- user department managers
- IS system / network administrator(s)
- … and others.

You should initially report problems internally rather than externally, reducing any adverse publicity or loss announcements. External reporting should only be done in an extreme emergency.

Centralized Reporting

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

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

External Reporting

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

- law enforcement, police
- fire department
- FBI
- external auditors
- … and others.

Interfering with Incident Reporting

You should never attempt to interfere with, prevent, obstruct, or dissuade another employee from reporting a suspected information security problem or violation. Any form of retaliation against an individual reporting or investigating information security problems or violations is prohibited.

Not reporting an incident is prohibited. If a report of a known infestation is not promptly made, there could be great damage done. Some organizations add specific penalties for not reporting problems.

Incident Reporting At-a-Glance

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

Chapter 3
Access Control Rules

About Access Control

As a user of information systems in your organization, you will be given access to the applications and information you need to do your job. Access Control is the set up and maintenance of system access data that determines who you are, what you can access, what restrictions you have been given, and what tasks you can perform.

Sensitive Data

If your job requires that you use highly confidential or time sensitive information, you will be given a higher access level so you can get to the more sensitive applications and data. If this is the case, you must be even more aware of information security issues and should carefully review all the rules in this chapter.

Logging On and Off

Before you can access any information systems, you must first identify yourself to the computer via a logon process. Here you will enter your unique User ID that identifies you as the requesting user. You will always need to protect your access rights by supplying a confidential password along with your User ID. Your password is strictly confidential. Once you have successfully logged on, you will have access to all the authorities you have been granted in your Access Control authorization(s).

Depending on the configuration used by your organization, you may need to have several User IDs and passwords to access various applications and data.

Identification

When you initially log on to the system, you will need to enter the User ID (or sometimes called a Logon ID) given to you. This User ID is a unique identifier that tells the systems that you are requesting access. Any work performed on the system under your User ID is directly traceable back to you. This makes you accountable for all activities performed under your User ID. For this reason, it is important that you do not allow others to perform tasks under your Identification.

With the ever-increasing number of computers and networks found in organizations today, use of several User IDs for the same person is common and getting very complex. You may have multiple User IDs for access to different systems, however, each one still is issued uniquely to you.

Without unique User IDs, you cannot have privileges assigned just for you. If privileges cannot be restricted by user, then it will be very difficult to implement separation of duties, dual control, and other generally accepted security measures.

Many organizations are going to a single sign-on approach giving you one User ID for all environments.

Authentication

After you have been identified by the system, you will then enter a password to Authenticate that it is indeed you. Here, "password" could be replaced by other authentication methods like smart cards, PIN (personal identification numbers) numbers, dynamic password tokens, biometrics and other technologies.

Your password is a string of characters that only you know. Even the IS security administrator should not know your confidential code chosen for your password.

Upon being hired, you will be given a standard or “default” password to initially enter the system. It is important that you change it immediately to your confidential code.

Guessing passwords remains a popular and often successful attack method by which unauthorized persons gain system access. For this reason, we ask that you consider these rules in choosing and maintaining your password.

Authorization

When you have successfully logged on, that is, identified and authenticated yourself, you will be automatically given access to all the areas that apply to your job requirements. The areas you can access, or authorities, or privileges you are given are called your Authorization and are set up when you are hired or change job status. Once you have successfully logged on, you will have access to all the Authorities to which you have been granted by your User ID.

Access Control Rules

The rules pertaining to Access Control are critical to protect information systems by preventing unauthorized access. Since you are responsible for all activity under your identification, you can play a big part in preventing unauthorized persons from taking access of your User ID or finding out your confidential password.

The Access Control rules are grouped accordingly:

Logging On Rules

Rule - Unique User ID and Password

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

Rule - Unsuccessful Logging On

You will be allowed **{3}** failed attempts to try to log on. If you fail all attempts, your User ID may be revoked.

Explanation

Forcing the User ID to be reset prevents trial-and-error or brute force attempts at guessing passwords.

Troubleshooting

Problem: What should I do if … I failed all attempts to log on?

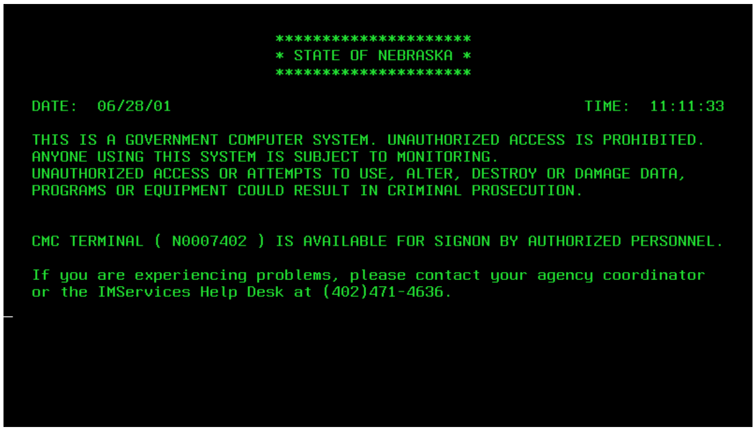
Action: You must call IS to have them manually reset your User ID. Your User ID has been revoked which disables it until it is reset.

Warning Banner Rules

A warning banner_is a security notice that displays on the screen when you have successfully accessed the system or application requested. This system message is displayed each time you log 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 you have accessed a government system or system that may contain government information.
- that use is restricted for authorized purposes.
- that your activities are subject to monitoring.
- that misuse can be reported to security and/ or law enforcement personnel and subject you 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

You must receive a warning banner for each environment you access.

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 Log on

The warning banner should display the date, time and device of the last successful and unsuccessful log on you performed. You should always think back to the last time you used the system and check to see if the time and device are correct.

Logging Off Rules

At end of day, be sure you log off from all systems you accessed that day. If you leave your workstation for an extended amount of time, you should also log off.

Rule - Automatic Log Off

You will automatically be logged off if there has been no activity on your workstation for **{10}** minutes. Your screen will become blank and your session will be suspended.

Explanation/ Key Points

This rule is most effective when it applies to all workstations. It could, however, be restricted to users accessing sensitive, critical, or valuable information.

Troubleshooting

Problem: What should I do if … I was automatically logged off?
Action: Re-establishment of the session must take place only after you have provided the proper password.

Problem: Will I loose the work I was doing, like a word processing file?
Action: No. After you have supplied the password, work can resume at the exact place you left it.

Rule - Leaving Your Workstation - Logging Off / Locking

You must log off / lock when you leave your workstation for an extended amount of time (lunch, breaks, meetings), in the event of an emergency (time permitting), or other instance that would cause you to leave your workstation. You should always log off at the end of the day.

Explanation/ Key Points

Particularly in open offices and cubicles, it is critical that you do not leave your workstation available for others to access your information.

Remember: You are responsible for the security of information in your possession.

Good practice:	Lock the terminal.
Better practice:	Log off the applications
Best practice:	Log off the network

Logging off applications and the network will cause files to be saved and applications to be closed in the event the system fails or there is a power failure during your absence.

ⓘ ***Important !*** There is no acceptable period during which systems with sensitive or valuable information may be unattended.

Chapter 3 - Access Control Rules

Identification (User ID) Rules

Rule - Unique User ID

You must have a unique User ID that makes you responsible for all activities involving your User ID.

Troubleshooting

Problem: What should I do if … I forgot my User ID?
Action: You must positively identify yourself to IS and they will give it to you.

Rule - Prohibit Group User IDs

You must never use one User ID for group(s) access. This prohibits Identification. Your User ID must be tied to an individual user and must never be generic.

Rule - Sharing your User ID is Prohibited

Your User IDs may not be utilized by anyone but you. You must not allow others to perform any activity with your User ID. Any IS logs will not reflect the true identity of the user.

Troubleshooting

Problem: What should I do if … I'm going on vacation and another user needs to do my job?
Action: As soon as you return from your vacation, change your password.

Rule - Using Another User ID is Prohibited

You should never perform any activity with another users User ID.

Troubleshooting

Problem: What should I do if … I have to do another users job?
Action: With proper authorization, you can use another User ID to perform the necessary tasks. The user that the User ID belongs to should change their password immediately after you have completed your tasks or they have returned to work.

Rule - Dormant User IDs

Your User ID will automatically have the associated privileges revoked after **{30}** days of inactivity. If you are a temporary employee, contractor, or consultant, it will be revoked in **{15}** days.

Troubleshooting

Problem:	What should I do if … my User ID has been revoked?
Action:	Your User ID will need to be re-activated when you return.

Rule - Internet User ID Expiration

Your User ID on internet accessible computers must be set to expire **{3}** months from the time they are established.

Authentication (Password) Rules

Rule - Changing Your Default Password

You must change your password when you are initially given the default password by your IS department. This default password should be valid for only your first log on session.

Explanation/ Key Points

You should be forced to change your default password issued to you by IS. 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.

Troubleshooting

Problem:	What should I do if … I forget my password?
Action:	Call IS and identify yourself so they can to reset your password.

Rule - Difficult to Guess Passwords

You should choose a password that is difficult to guess, yet easy to remember.

Explanation/ Key Points

The most frequently encountered problem with security systems is human error, and choosing an easily guessed password is one of the most common security-related mistakes.

Warning ! If a single sign-on password is guessed, an intruder then gains access to many systems.

Rule - Minimum/ maximum Password Length

Your password must have at least eight **{5}** characters, but no more than **{n}**. Passwords with only a few characters are much easier to guess.

Rule - Cyclical Previous Passwords

When you change your password, you should make it different each time, not a derivative from your previous one.

Explanation/ Key Points

You should not just partially change your 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

Your password allowable characters are {alpha, numeric, special, combination}. Your 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 you to choose a password that is difficult for unauthorized parties and system penetration software to guess.

Rule - Passwords Lower and Upper Case

Your password 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.

Example: "a" is not the same as "A"

Rule - Choosing Your Password

You must select a password that can provide reasonably good security to your information.

Explanation/ Key Points

Passwords - Good Choices

- Use a password with mixed-case alphabetic characters.
- Use a password with some non-alphabetic characters. i.e. digits or punctuation
- Use the standard English alphabet and numerals
- Join 2 small words with a special character.

- The longer the better. (no maximum limit)

Passwords - Bad Choices

- Do not use derivatives of your User ID (i.e. reversed, capitalized, doubled)
- Do not use common character sequences such as "123456"
- Do not use personal details such as your name, family member's name, pet's name, automobile license plate, social security number, address.
- Don't use a word (alone) contained in the dictionary (English or foreign language), spelling lists, or other lists of words.
- Do not use proper names, geographical locations, and common acronyms.
- Don't use important dates in your life - you and your family birthday , anniversary, hire date, etc.
- Do not use repeating characters or all digits or letters. This significantly reduces the amount of search time for a hacker.

Syntax Suggestions:

Good choice:	A mix of alpha and numeric characters. Ex: A3NY8T
Better choice:	A mix of alpha and numeric characters – more characters. Ex. Z9W34B2F
Best choice:	A mix of case sensitive alpha and numeric characters - more characters. Ex. Z9w34B2f
Do not use:	Jackie1 KatherineS 123456

Rule - Keeping Your Password Confidential

You should never give your password to anyone without approval.

Explanation/ Key Points

Passwords should be treated as private and highly confidential. Passwords should never be written down, typed into the system as a reminder or sent via e-mail.

Troubleshooting

Problem: What should I do if …I know someone else has my password?
Action: Immediately change your password.

Problem: What do I do if … I'm going to be gone for an extended time and want someone to have my password?
Action: Get the proper approvals and be sure to change your password as soon as you return.

Problem: What do I do if … someone gives me their password to perform a task?
Action: Make sure they change their password.

Rule - Reusing Passwords / History

You cannot reuse your password for **{15}** changes. OR You must not use the same password more than once in a **{12}** month period.

Explanation/ Key Points

You must not construct your password identically or substantially similar to passwords that you used previously. You must not recycle your passwords.

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 you use sensitive data and have a highly access authority, you must NEVER use the same password twice.

Rule - Display and Printing Passwords

You must never display or print your password.

Explanation/ Key Points

The display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. When you type your password into a system, it should not be displayed on a monitor or printed on a printer.

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

Rule - Forced Expiration of Passwords

You will be automatically forced to change your password every **{90}** days. If you access sensitive data, you will be forced to change your password every **{30}** days.

Explanation/ Key Points

You will need to change your password regularly in order to continue working. 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.

Rule - Unsuccessful Passwords Attempts

You will be allowed **{3}** failed attempts to successfully enter your password.

Explanation/ Key Points

To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. If you fail the number of attempts, your User ID must be revoked.

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 - Same Password on Different Systems

Do not use the same password on multiple systems if your job requires you to access multiple environments.

Rule - Disclosure Forces Password Change

You must change your password if you know someone has discovered it or it has been disclosed.

Rule - Writing Passwords Down

Your passwords should never be written down. Use a password that you are able to commit to memory, so you don’t forget it or have to write it down.

Explanation/ Key Points

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

With multiple systems and regular changes to passwords, you may have a lot of passwords to remember. Therefore, sometimes it is necessary to write it down. Discovering passwords written down and left in the top drawer, taped to a computer monitor, or in some other conspicuous spot is a surprisingly common way for penetration attackers to break into computers. This does not mean that you should never write down your password, only that you must not leave it in a spot where others could see it.

☝ ***Tip:*** You could use the "black night" method. With this method, passwords may be taped 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 - Written Passwords Left Near Devices

You must never write down or otherwise record a readable password and store it near the access device to which it pertains.

Explanation/ Key Points

For example, you should not leave passwords and telephone access numbers inside portable computers. PINs needed to initialize dynamic password tokens or smart cards should not be recorded on the devices themselves.

Rule - Proof Of Identify to Obtain a Password

You must appear in person to the IS department to obtain a new or changed password to positively identify yourself.

Troubleshooting

Problem: What should I do if … I forgot my password?

Action: You will need to have your password reset. The key is to positively identify you before resetting your password.

If the request is on the telephone, for example, you could use an employee code that only the employee knows, like employee number or mother’s maiden name. If it is through your Help desk / Security Administrator, they could create a questionnaire the covers both organization and employee information to positively identify you as an employee.

Authorization (Privileges) Rules

🕮 Rule - Authorized Privileges

You can only view, modify, print, transport, and mail information you have been authorized to access.

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

Chapter 4
Network Security Rules

About Network Security

Most organizations today process their business applications on or via a network. This network system may be internal or connected to an external communication environment. Organizations may have several networks, several mainframes and other peripheral computer systems that require a sophisticated configuration to connect it all together.

It is important that you, the employee, understand the importance of protecting the information on your network(s) in your organization. You play a large part in keeping the network safe from intruders, virus free and in good working order.

Remote Access

With the introduction of the laptop computers, e-mail messaging, fax machines, and the internet, it became less necessary for employee to report to an office. Many employees and contractors today work via telecommuting, that is, from a remote location. This may be due to logistics, business travel, having remote branches, or many other business purposes that best serve the function by having a portable office.

In addition to the precautions and safeguards we can all do to protect our network, we also need to be aware of connections with outside parties, over whose network environment you have no control. This openness of the internet is making organizations more vulnerable than years ago.

Network Security Rules

The rules pertaining to Network Security are critical to protect information systems on your network(s).

The Network Security rules are grouped accordingly:

Network Access Rules
Modems Rules
Remote Access Rules
Remote Sites Rules

Chapter 4 - Network Security Rules

Network Access Rules

Rule - Approval for Connections

You must not connect any devices to the state network, internal network, or any other equipment with a modem or communication system without prior approvals.

Explanation/ Key Points

You may be putting your organization's information in jeopardy if you create entry points in your own communication systems. You could create vulnerabilities that you are unaware of by bypassing the proper controls.

Rule - Gaining Unauthorized Access

You are not permitted to gain unauthorized access to any information systems on your network or connected to the network.

Explanation/ Key Points

You should not in any way damage, alter, or disrupt the operations of information systems with unauthorized access. You are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism, which could permit you to have unauthorized access.

Rule - Network Browsing Prohibited

You must not browse through your computer systems or networks searching for interesting files and/or programs. Steps taken to legitimately locate information needed to perform one's job is not considered browsing

Rule - Network Backups

To prevent accidental loss, all information on your organization's networks are routinely copied to tape, disk, and other storage media. This means that even if you specifically deleted a file, it is recoverable.

Rule - Overwhelming the Network

You must not send an overwhelming number of files across the network to cause interruption of processing. This is called denial of service attack, spamming or e-mail bombing.

Rule - Malicious Intent and the Network

You are prohibited from any form of malicious or disruptive use, including use of the organization's own resources, or any attached network in a manner that precludes or significantly hampers its use. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses, and use of the organization owned resources to make unauthorized entry to any other machine accessible via the network facilities.

Modem Rules

🕮 Rule - Modems Connections to Internal Networks Prohibited

You are prohibited from connecting dial-up modems to workstations, which are simultaneously connected to a local area network (LAN) or another internal communication network unless approved.

Explanation/ Key Points

This could establish a weak link in a system of network access controls.

🕮 Rule - Prohibit Modems in AutoAnswer Mode

You must not leave your approved modem connected to personal computers in autoanswer mode, such that it is able to receive in-coming dial-up calls. Be sure to turn off your modem at end of day.

Remote Access Rules

Rule - Dial-up Password Attempts

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

Troubleshooting

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

Rule - Remote Access Training

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

Remote Sites Rules

Rule - Telecommuting Permissible Equipment

If you are working on business at alternative work sites, you must use computer and network equipment provided by your organization. An exception will be made only if other equipment has been approved as compatible with your organization's information systems and controls.

Rule - Protection of Off-Site Property

The security of your organization's property at an alternative work site is just as important as it is at the central office. At alternative work sites, reasonable precautions must be taken to protect hardware, software, and information from theft, damage, and misuse.

Explanation/ Key Points

When required, you must abide by all remote system security policies, rules and procedures. This includes compliance with software license agreements, performance of regular backups, and use of shredders to dispose of sensitive information.

You must also not alter the configuration of hardware and software without prior approval.

Rule - Information to be Returned

You must return all property and information created in your portable computer provided by your organization. You may be given a portable computer so you can perform your job at remote locations including hotel rooms and personal residences.

Rule - Remote Working Environment

If you are a telecommuter, to retain the privilege of doing off-site work, you must structure your remote working environment so that it is in compliance with your organization's policies and standards.

Rule - Right to Conduct Inspections of Telecommute Office

Your organization maintains the right to conduct inspections of your telecommuter offices with **{1}** day advance notice. The information stored in your portable computer belongs to your organization and they can inspect or use the information in any manner, and at any time.

🕮 Rule - Sensitive Information on Portable Computers

If you are in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing sensitive information, you must not leave these computers unattended at any time unless the information has been encrypted.

🕮 Rule - Backing up Portables Computers

You must make periodic backups of all critical information and store it away from the portable device. These backups should be performed every **{1}** day. They should be stored elsewhere than the portable computer's carrying case.

🕮 Rule - Transportable Computers Hand Luggage on Airplanes

If you are in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing sensitive information, you must not check these computers in airline luggage systems. These computers must remain in your possession as hand luggage.

Explanation/ Key Points

The primary reason to not check your computer as baggage is to avoid theft or loss.

🕮 Rule - Portable Computer Security

You must keep your portable computers (i.e. laptop) in your possession at all times, or locked in a secure location (i.e. hotel safe). You must do your part to protect your equipment and information against theft, destruction, and loss.

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

Chapter 5

Individual Use/ E-mail, Internet, and E-commerce Rules

About E-mail, Internet and E-commerce

The use of e-mail, the internet, and e-commerce in the workplace has become an important critical function for many organizations. The key concern with information security and the cyber world is the connections and communications required to access it. This is a high-risk security area that without proper safeguards can leave the door open to intruders to access your organization's information.

In addition to security concerns, proper use of e-mail, the internet, and e-commerce is the responsibility of every employee. Improper use can detract from performance of duties and subject your organization to potential legal action. Careless use can subject you and other users to malicious software attacks.

Your IS department should implement a secure and managed environment for you to effectively and safely use e-mail, the internet and e-commerce to accomplish your jobs tasks. It is your responsibility to uphold the rules of proper usage.

E-mail, the Internet, and E-commerce Rules

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

E-mail Rules
Internet Rules
E-Commerce Rules

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

E-mail Rules

🕮 Rule - E-mail for Business Purposes Only

You should use e-mail for business purposes only.

🕮 Rule - E-mail and Confidential Information

E-mail that is not secure or encrypted (non-readable) should not be used to send sensitive information.

Explanation/ Key Points

Sensitive information may not be sent over an e-mail system unless it is encrypted at the source and decrypted at the destination.

🕮 Rule - Forwarding E-mail

You must not forward electronic mail to any address outside your organization's network unless the information owner/originator agrees in advance, or unless the information is clearly public in nature.

Warning ! Blanket (global) forwarding of electronic mail messages to any outside address is prohibited without written permission from the appropriate security resource.

🕮 Rule - Forwarding External E-mails

You must not create your own, or forward externally provided electronic mail messages which may be considered to be harassment or which may contribute to a hostile work environment. Among other things, a hostile work environment is created when derogatory comments about a certain sex, race, religion, or sexual preference are circulated.

🕮 Rule - Forwarding E-mail to Archival Records

All official organizational e-mail message, including those containing a formal management approval, authorization, delegation, or handing over of responsibility, or similar transaction, must be copied to a special archival account set up by your organization.

🕮 Rule - E-mail Retention

You can erase most e-mail messages after receipt. The only exception to this is if the e-mail message contains information required for future use.

🕮 Rule - E-mail Virus Protection Software

Your organization will use virus protection software on your workstation to prevent transmission of viruses in e-mail attachments and diskettes.

Explanation/ Key Points

A lack of user awareness about the risks of opening unsolicited e-mails may result in a virus infection spreading throughout the organization.

ⓘ ***Important !*** It is critical that you keep your anti-virus software and definitions (library of virus profiles) current with frequent updates / downloads.

🕮 Rule - Certainty of E-mail File Attachments Origin

You must be certain of the original of any file attachments you receive through e-mail. This is critical to protect your workstation and others against malicious software.

🕮 Rule - Using another Users E-mail Account

You must not use an e-mail account assigned to another individual to either send or receive messages.

Troubleshooting

Problem: What should I do if … I need to read another users e-mail messages while they are away on vacation?

Action: Use message forwarding or use your mail delegation features of your e-mail system.

🕮 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 - Deleting and Destroying E-mail

Internal correspondence must be disposed of when no longer needed.

Explanation/ Key Points

E-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.

ⓘ *Important !* Be aware of local rules, regulations, or pending legal actions that may restrict the deleting of your e-mail messages.

Rule - Privacy and E-mail

You must treat e-mail messages and files as private information. E-mail must be handled as a private and direct communication between the sender and the recipient.

Rule - E-mail is Public Communication

You should treat e-mail as public communications. Consider e-mail to be the electronic equivalent of a postcard. Unless the material is encrypted, you must refrain from sending credit card numbers, passwords, research and development information, and other sensitive data via e-mail.

Rule - E-mail as a Public Record (government)

Be aware of and follow local rules and regulations that define some or all e-mails as public records. Also observe rules governing archiving and deleting as well.

Rule - E-mail Profanity

You must not use profane, obscene or derogatory remarks in e-mail messages.

Explanation/ Key Points

Such remarks, even when made in jest, may create legal problems such as trade libel and defamation of character. Special caution is warranted because backup and archival copies of electronic mail may actually be more permanent and more readily accessed than traditional paper communications.

Rule - Responding to Junk (SPAM) E-mail

When you receive unwanted and unsolicited e-mail (also known as SPAM), you must refrain from responding directly to the sender unless you can “unsubscribe” thus sending out a “do not send” mail message.

Troubleshooting

Problem: What should I do if … I receive a SPAM e-mail?
Action: You should forward the message to the IS e-mail administrator who will take steps to prevent further transmissions.

Rule - Ownership of E-mail Messages and Attachments

All messages sent by e-mail are owned by your organization. Your organization reserves the right to access and disclose all messages sent over its E- mail system, for any purpose.

Rule - Disclosure of E-mail Messages and Attachments

Your organization management may review your e-mail communications to determine whether they have breached security, violated company policy, or taken other unauthorized actions. Your organization management may also disclose the contents of e-mail messages to law enforcement officials without prior notice to the your or whoever may have sent or received the message.

Rule - Authorization to Issue Broadcasts in E-mail

You must get the proper authorization to issue broadcasts through e-mail.

Rule - Scanned Signatures in E-mail

You must not use scanned versions of hand-rendered signatures to give the impression that an e-mail message or other electronic communications were signed by the sender.

Rule - Misrepresentation of Identity in E-mail

Misrepresenting, obscuring, suppressing, or replacing your identity on an e-mail communications system is forbidden. Your name, e-mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.

Internet Rules

All authorized state employees will be provided with an appropriate internet system.

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. All files down-loaded from the internet must be checked with an authorized virus detection package prior to being moved to any other computer.

Rule - Sending Sensitive Information Over the Internet

Your organization's sensitive information must never be sent over the internet unless it has first been encrypted by approved methods. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the internet.

Rule - Uploading via the Internet

You must not upload software, which has been licensed from a third party, or software, which has been developed by your organization to any computer via the internet unless authorization from the user's department manager has first been obtained.

Rule - Using the Internet for Personal Use

You should use the internet for business purposes only. If you use the internet for personal use, it must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not potentially embarrass or harm your organization.

ⓘ ***Important !*** Be aware that firewalls can create a detailed audit log reflecting transmissions, both in-bound and out-bound.

Rule - Approval for Internet Connections

You must not establish internet or any other external network connections, which could allow non-organization users to gain access to your organization's information. These connections include the establishment of multi-computer file systems (like Sun's NIS), internet home pages, internet FTP servers, and such.

Rule - Training for Internet Use

You must complete an approved ISS internet and e-mail training course prior to being granted privileges to use dial-up, internet, or any other remote access data communications system.

Rule - Internet User ID Expiration

Your User ID on internet accessible computers must be set to expire **{3}** months from the time they are established.

Rule - Personal Messages Disclaimer on Internet

If you post a message to an internet discussion group, an electronic bulletin board, or another public information system, this message must be accompanied by words clearly indicating that the comments do not necessarily represent the position of your organization.

Explanation/ Key Points

Such statements are required even when your organization's name does not appear in the text of the message and/or when an affiliation with your organization has not been explicitly stated.

When engaged in discussion groups, chat rooms, and other internet offerings, only those individuals authorized by management to provide official support for your organization's products and services may indicate their affiliation with your organization.

Example: If you disclose an affiliation with your organization, you must clearly indicate that "the opinions expressed are my own, and not necessarily those of my employer."

Rule - Internet Products and Services

You must not advertise, promote, present, or otherwise make statements about your organization's products and services in internet forums such as mailing lists, news groups, or chat sessions.

Rule - Public Area of Your Organization's Web Site

If you submit information to the public area on your organization's web site or electronic bulletin board system (BBS), you grant to your organization the right to edit, copy, republish, and distribute such information.

Rule - Unofficial Web Pages on the Internet

You cannot create or implement unofficial web pages dealing with your organization’s products or services.

Rule - Concealing your Identity on Internet is Prohibited

When using your organization’s information systems, or when conducting your organization’s business, you must not deliberately conceal or misrepresent your identity. This includes participating in discussion groups and chat rooms, as well as establishing accounts on other computers.

Rule - Exchanges of Information on the Internet

Your organization’s software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-organization party for any purposes other than the business purposes and only with the proper authorization.

Rule - Updating Organization Information on the Internet

If you are connected to your organization's systems via the internet, you are not permitted to directly modify any organization information.

E-commerce Rules

🕮 Rule - E-transactions

If your organization's transactions are sent and processed automatically on the internet, then a message must not be accepted or acted on unless: (a) the message has been shown to match a trading profile for the initiating organization, or (b) the message has been shown to deviate from a trading profile but additional steps have been taken to verify the accuracy and authenticity of the message.

🕮 Rule - Forming E-contracts

Unless specifically authorized to enter into contracts on behalf of your organization, or otherwise authorized to legally represent your organization, you must never respond to an e-mail message that binds your organization to any contract, position, or course of action.

🕮 Rule - Validating Identity of External Parties on Internet

It is relatively easy to spoof the identity of another user on public networks such as the internet. Before you release any internal organization information, enter into any contracts, or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed.

Explanation/ Key Points

Identity confirmation is ideally performed via digital certificates, but in cases where these are not yet available, other means such as letters of credit, third party references, and telephone conversations may be used.

🕮 Rule - Electronic Offers

All contracts formed through electronic offer and acceptance messages (fax, Electronic Data Interchange, e-mail, etc.) must be formalized and confirmed via paper documents within **{2}** weeks of acceptance.

🕮 Rule - Internet Customers

All customers using the internet to place orders with your organization must be presented with a summary of your organization important terms & conditions, and in order to complete their orders, they must specifically indicate that they agree to be bound by these terms & conditions

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

Chapter 6

Access Control/ Workstation / Office Rules

About Your Workstation / Office

One of the main ways that you, the employee, can contribute to your organization's ISS program is to be aware of your immediate surroundings, observe your working habits, and take the necessary precautions to safeguard your working area. Whether you have an office with a door, a cubicle or an open desk layout, you can be a major factor in the security of your information.

Workstation / Office Rules

The Workstation/ Office rules are grouped accordingly:

Chapter 6 - Workstation/ Office Rules

Workstation Rules

Rule - Workstation Protection Security

Reasonable efforts should be made to safeguard your individual workstations to protect against unauthorized access to your workstation, network or data.

Explanation/ Key Points

Workstations can be secured by securing the rooms where they are located and by physically attaching them to tables or work areas so that special tools are required to remove them from the premises.

Rule - Securing Unattended Workstations

You should log off your computer if you will be leaving your workstation for an extended amount of time. (i.e. meeting, lunch, break, end of day). If you leave your workstation unattended for **{10}** minutes, your screen will lock up.

Troubleshooting

Problem: What should I do if … I left for an extended period of time and my screen locked up?
Action: Call your designated contact to unlock the terminal.

Rule - Loading Personal Screen Savers

You should not install a personal screen saver on your workstation without prior approval. The screen saver software disk/ CD should be scanned for a virus or other malicious software that could potentially invade your workstation and your network.

Rule - Altering Computer Equipment

You cannot expand or alter computers supplied by your organization. This includes upgraded processors, expanded memory, extra circuit boards, and such, without proper approval and authorization.

Rule - Moving and Relocating Your Equipment

You must not move or relocate any office computer equipment (desktop computers, fax machines, LAN servers, network hubs, etc.) without the proper approval.

Rule - Sensitive Information While Working

You must cover sensitive information if another person enters your work area around your desk. If the information is in physical form, the information can be covered with other material. If the information is displayed on a computer screen, you may invoke a screen saver or log off.

Explanation/ Key Points

If you handle sensitive information and are in the immediate vicinity of a conference room, all meetings with third party visitors (vendors, customers, regulators, etc.) who are not authorized to have access to such sensitive information must take place in fully enclosed conference rooms.

Rule - Locking File Cabinets

If you handle sensitive information in the course of your regular business activities, you must be provided with locking file cabinets. You must lock all sensitive material in these file cabinets when away from your desk, and must provide a backup copy of the key(s) to the proper authorities.

Rule - Screen Positioning

If you handle sensitive information, you must position your computer display screen away from others view. This includes away from hallways, windows, doors, reception or public areas.

Rule - Clear Desk

You must not leave sensitive or other organization information in plain view on your desk or working area. Be sure all information is properly secured, especially during non-working hours.

Rule - Clear Screen

You must not leave sensitive or other organization information in plain view on your screen or terminal in your working area.

Rule - Office (with a door)

If your working area includes a door, it is important that you shut and/ or lock the door when you leave your working area for an extended period of time throughout the day and at the end of day.

Chapter 6 - Workstation/ Office Rules

Rule - Cubicle Security

If your working area is in a cubicle, you are in a more open environment with easier access to your information. You should take necessary precautions, don’t leave items exposed on your desk or terminal and lock up your personal property.

Rule - Bringing your personal PC/ laptop to Work

You must properly secure and protect your personally owned computer equipment (i.e. PCs, laptops, …) that you have brought to work. This non-organization owned equipment needs to follow the same safeguards.

Explanation/ Key Points

These PCs or laptops have been used as stand-alone machines, but they still contain your organization’s information.

Rule - Personal Equipment and Information Ownership

The information you create and develop on your personal equipment (at home or at the office) is owned by your organization.

Rule - Personal Equipment and Privacy

If you are using your personal equipment (at home or at work) containing organization information, you must follow your organization’s privacy issues and keep the information confidential.

Rule - Home Computers Security

You must incorporate the proper security safeguards if you generate information on your personal equipment at home and then transfer it to their work PC.

Disposal Rules

You must be very careful when throwing away obsolete equipment or media devices for they may contain organization information.

🕮 Rule - Information Disposal/ Wiping

You must properly dispose of devices containing organization information. PCs must be wiped clean of data and software.

Explanation/ Key Points

There are products available to wipe data from media, CDs, diskettes and hard drives. This will "sanitize" it for disposal.

ⓘ ***Important !*** Be aware of what information is on all devices that are being discarded or resold.

🕮 Rule - Discarding Hardcopy Information

You must not throw away sensitive hardcopy materials into hotel wastebaskets or other publicly accessible trash containers. All sensitive information must be retained until it can be shredded, incinerated, or destroyed with other approved methods.

Explanation/ Key Points

This rule applies to paper, microfiche, typewriter ribbons, carbon papers, stencils and templates, photographic negatives, thermal fax transfer films, computer hardcopy output, photocopies, and such.

🕮 Rule - Personal Equipment Disposal

If you use your personal equipment (PCs, laptops) for work purposes, you must dispose of information properly. This applies to all the information on your equipment, whether you are at the office or have transported the information out of your working environment.

🕮 Rule - Media Disposal/ Concealment

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. (i.e. degaussed, demagnetized, wiped, or zeroized)

🕮 Rule - Erase and Zeroize

When you erase sensitive information from a disk, tape, or other magnetic storage media, it must be followed by a repeated overwrite operation (zeroization) which prevents the data from later being scavenged.

💣 *Warning !* This is especially important if you are transferring information to a third party. Also check IRS rules for some applications.

🕮 Rule - Destruction Approval

You must not destroy or dispose of potentially important organization records or information without specific advance approval. Unauthorized destruction or disposal of your organization's records or information is prohibited.

Explanation/ Key Points

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).

Media Security Rules

Media, that is CDs, diskettes, jazz drives, and such, may be required in your job to transport, store, or back up your daily information. This media may be used day-to-day and reside near your workstation for ease and usability.

One of the main concerns in ISS security is the safekeeping and day-to-day protection of your media that you use every day.

Rule - Media Safety

You must protect and safely store all media devices that you use to do your daily job.

Explanation/ Key Points

When not being used by authorized workers, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information must be locked in file cabinets, desks, safes, or other furniture. Likewise, when not being used, or when not in a clearly visible and attended area, all computer media (floppy disks, CD-ROMs, etc.) containing sensitive information must be locked in similar enclosures.

Rule - Hard Drive Security

Sensitive information should not be on your workstation hard drive. Most workstations pose a risk of unauthorized access because the drives are accessible.

Rule - Sensitive and Non-sensitive on Same Media

You must not store sensitive information such that it is commingled with non-sensitive information on floppy diskettes or other removable data storage media.

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

Chapter 7

Physical / People Security Rules

About Physical / People Security

When you enter a building, room, or office and need to gain entry by using a card, fingerprint, or other means, then your organization has taken physical security measures. This type of security usually involves a device attached to a wall or door at the entry point. When you gain access to a secured area (i.e. computer operations room, cash handling room), you have been given prior access clearance or your identity has somehow been noted or recorded. Many organizations also require the same access methods to leave the building.

Typically organizations that house system operations will require physical security into the building and even the parking garage. Sometimes a security guard will be stationed at the entry point to further provide physical access security by observing employee traffic, handling deliveries and visitors.

Physical Security Rules

The Physical Security rules are grouped accordingly:

Physical / People Security Rules

Chapter 7 - Physical/ People Security Rules

Physical / People Security Rules

Rule - Tailgating and Piggybacking when Entering

If you are entering with someone else, you should still show your badge or show proof that you can enter. If someone else is entering with you, be sure to check them to see that they are authorized to enter.

Explanation/ Key Points

You must not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when you go through these entrances.

Rule - Lending Cards/ Keys, Tokens

You must never lend your access devices: cards, keys, token, etc, to a secured area to anyone.

Rule - Challenging Strangers

You should challenge any strangers you see on the premises that are not properly identified. (i.e. no badge). If you notice an unescorted visitor inside your organization's restricted areas, the visitor must be immediately questioned about the purpose for being in restricted areas. The visitor must then be directly accompanied to either a manager, a guard station, or the person they came to see. If they cannot promptly produce a valid badge, they must be escorted to the proper authorities.

Rule - Handling Visitors

All visitors must show proper identification and sign in prior to gaining access to restricted areas controlled by the organization. Visitors must be admitted only for specific authorized purposes.

Rule - Visitor Escorts

Visitors must be escorted at all times by an authorized employee, consultant, or contractor. This means that an escort is required as soon as a visitor enters a controlled area, and until this same visitor goes outside the controlled area.

Rule - Visitors Entrances

Visitors and other third parties must not be permitted to use the employee entrances or other uncontrolled pathways leading to areas containing sensitive information.

Rule - Social Engineering

Beware of people that ask a lot of questions about the organization and its security. They may be trying to gain knowledge to gain unauthorized access.

Explanation/ Key Points

It is called social engineering and is the process of convincing people to divulge information that they should not. Often built on false pretenses, and misidentification, social engineering is extremely effective. This is accomplished by name dropping, gaining your confidence, and sometimes through intimidation.

Rule - Sensitive Information and Physical Access Controls

Access to every office, computer room, and work area containing sensitive information must be physically restricted. Suggestions: receptionists, metal key locks, magnetic card door locks, etc.

Rule - Lock Office Doors

If you have a separate offices with a door, you must lock the doors you're your office is not in use. This practice will help to restrict unauthorized access to sensitive information.

Rule - Wearing ID Badges

When in your organization's buildings or facilities, you must wear any assigned identification badges on your outer garments so that both the picture and information on the badge are clearly visible.

Rule - Temporary ID Badges

If you forgot your badge, you must obtain a temporary badge by providing positive proof of identity. A temporary badge is valid for **{1}** day only.

Rule - Reporting Stolen/ lost Access Badges/ Cards/ Tokens

ID badges, physical access cards, tokens and such that have been lost or stolen or are suspected of being lost or stolen, must be reported to the proper authorities immediately.

Rule - Presenting Your ID Badge

You must present your badge to the badge reader / guard before entering every controlled door within your organization's premises. Before proceeding through every controlled door, you must wait until the badge reader indicates that you have permission to enter the area.

Rule - Propping Open Doors

When doors to a secured area are propped open (perhaps for moving computer equipment, furniture, supplies, or similar items), appropriate personnel must continuously monitor the entrance.

Rule - Stay away from Restricted Areas

You must not attempt to enter restricted areas in your organization for which you have not received access authorization.

Rule - Property Pass for Removing Equipment

PCs, cellular telephones, portable computers, modems, storage media and related information systems equipment must not leave the organization premises unless accompanied by an approved property pass. All such removals of storage media must be logged in some fashion.

Chapter 8

Individual Use/ Copyright Rules

About Copyright Information

All employees must comply with copyright laws for all software, written and on-line materials, and other information sources. Organizations should communicate this policy to you and designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

Courts have found organizations and their officers liable for copyright infringement where unauthorized copies were used to the organizations benefit. This has occurred even when the copying of software or other copyrighted material was done without management's knowledge.

Copyright Rules

The Copyright rules are grouped accordingly:

Copyright Rules

Copyright Rules

Rule - Copyright Laws for Software and Paper

You must comply with copyright laws for software and written materials.

Rule - Copyrighted Inquiries

You organization shall designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

Rule - Copying Copyright Materials

You may not copy documents or software protected by copyright without the written permission of the copyright holder. Any unauthorized reproduction of the copyrighted material may subject you to disciplinary action, civil liability, or both.

Rule - Protection of Software and Copyrighted Materials

The organization is not obligated to defend or indemnify employees in actions based on copyright violation.

Rule - Copyright Enforcement Statement

According to the U.S. Copyright Law: ".. illegal reproduction of software can be subject to civil damages of as much as $100,000, and criminal penalties, including fines and imprisonment." If you make, acquire or use unauthorized copies of computer software, you could be disciplined as appropriate under the circumstances. Such discipline may include termination. **{Organization Name/This}** organization does not condone the illegal duplication of software.

Rule - Making Excess Copies Prohibited

You must not make more copies of licensed software than are allowed.

Rule - Copying Vendor Software

You must never copy (called bootlegging) unlicensed software that has not been properly licensed by your organization with the vendor. If you copy software, you are doing so on your own behalf, since all such copying is strictly forbidden by your organization. You organization allows reproduction of copyrighted material only to the extent that it is legally considered "fair use" or with the permission of either the author or publisher.

Rule - Sending Copyrighted Information Electronically

You must never send your organization's copyright materials through e-mail or via the internet without proper approvals, encryption methods, and safeguards being put in place.

Rule - Violation of Copyright Laws

You must not violate the legal protection provided by copyright and licensing laws applied to programs and data.

Explanation/ Key Points

It is assumed that information and resources available via your network or state-owned resources are private to those individuals and organization's owning or holding rights to such information and resources, unless specifically stated otherwise by the owners or holders, or unless such information and resources clearly fall within the statutory definition of a public record. It is unacceptable for you to use the state-owned resources to gain access to information or resources not considered a public record without the granting of permission to do so by the owners or holders of rights to such information or resources.

Rule - Using Copyrighted Information from the Internet

Much of the material on the internet is copyrighted or otherwise protected by intellectual property law (for instance by license agreement). If you must use internet information for your business, be sure you have followed the proper copyright laws.

Rule - Ownership of Copyrighted Materials

While an employee of your organization, you grant to your organization exclusive rights to patents, copyrights, inventions, or other intellectual property you originate and/or develop for them.

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

Chapter 9

Individual Use/ Acceptable Use Rules

About Acceptable Use

This chapter is focused on you, the employee and how you use the tools available to you to do your job. This includes systems, paper materials and all other resources you are in touch with throughout your business day.

Your organization has established these rules governing the acceptable use of your resources for business. The rules concentrate on giving you guidelines to exercise good judgement in your daily business practices.

Acceptable Use Rules

The Acceptable Use rules are grouped accordingly:

Acceptable Use (of systems) Rules

Other Employees / Organization Rules

Public Records/ Privacy (of citizens) Rules

Paper Information Rules

Using Software and Data Rules

Using Files and Directory Rules

Telephone, Faxes, and Other Devices Rules

HR Related Rules

Chapter 9 - Acceptable Use Rules

Acceptable Use (of systems) Rules

Rule - Personal Use of your Computer

The computer you are given by your organization to do your job must be used for business purposes only.

Explanation/ Key Points

Incidental personal use is permissible if the use does not interfere with your job functions.

Rule - Other Business Activities

As a user of your organization's computing and communications services, you must not use these facilities for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by your organization.

Rule - Using State-Owned Resources Unrelated to Business

You must not use the state-owned resources for fund-raising or public relations activities unrelated to an your employment by the State of Nebraska. You must not use state-owned resources in conjunction with for-profit or activities, unless such activities are stated as a specifically acceptable use. You must not use the state-owned resources for unsolicited advertising, unless authorized by the governing body of the organization.

Rule - Using State Resources in an Acceptable Way

You must not use state resources that you are not authorized to be using. You must not use state resources for unauthorized or illegal purposes.

Rule - Transmitting State-Owned Resources in an Acceptable Way

You must use state-owned resources as consistent with laws, regulations or accepted community standards. Transmission of material in violation of any local, state or federal law or regulation is prohibited. It is not acceptable to transmit or knowingly receive threatening, obscene or harassing material.

Rule - Misrepresentation on State-Owned Resources

You must not misrepresent yourself, an agency, or the State of Nebraska when using the state-owned resources.

Rule - Using Others Users Data on the State-Owned Resources

You cannot access or attempt to access another individual's data or information without proper authorization.

Rule - Preventing Services to Others

You must not prevent others from accessing services they are entitled to in your organization.

Rule - Storing Games on your Computer

You may not store or use games on your organization's computer systems or state owned resources.

Rule - Giving Information to a Third Party

You must not sell or transfer your organization's software, documentation, and all other types of internal information to any outsider (third party) for any purposes, unless authorized to do so. You must not disclose co-worker information to a third party unless required by law, or unless permitted by clear and explicit consent of the subject.

Explanation/ Key Points

If you have the proper authority and disclose information to a third party, you must keep records of all such disclosures including specifically what information was disclosed, to whom it was disclosed, and the date of such disclosure. These records must be maintained for at least {5} years.

Rule - Handling Third Party Confidential Information

If you handle sensitive information entrusted to your organization by a third party, you must protect it as though it was your own organization's sensitive information.

Explanation/ Key Points

☝ ***Tip:*** If an outside agent, employee, consultant, or contractor is to receive sensitive information from a third party on behalf of your organization, this disclosure could be preceded by the third party's signature approval or release form.

Rule - Third Party Agreements and Approvals

You must not sign confidentiality agreements provided by third parties without the advance authorization of your organization's legal counsel designated to handle intellectual property matters.

🕮 Rule - Sensitive Disclosure Statement to Third Party

All disclosures of Highly Restricted, or Confidential information to third parties must be accompanied by an explicit statement describing exactly what information is restricted and how this information may and may not be used.

🕮 Rule - Exposure of Sensitive information Public Places

You must not be read, discuss, or otherwise exposed on airplanes, restaurants, public transportation, or in other public places any organization sensitive information.

🕮 Rule - Time Sensitive Information

You must not handle time sensitive information by e-mail, voice mail, telephone calls, or other computerized systems until the specifics have been publicly announced.

Explanation/ Key Points

This includes organization issues, like mergers and acquisitions, up-coming layoffs, and such.

Other Employees/ Organization Rules

Rule - Disclosing Co-worker(s) Contact Information

You must not disclose the names, titles, phone numbers, locations, or other contact particulars of your co-workers unless required for business purposes.

Rule - Disclosing Co-worker(s) Change in Status Information

You must not disclose the change of status of any co-worker. This includes: reason for terminations, retirement, resignation, leave of absence, leave of absence pending the results of an investigation, inter-departmental transfer, relocation, and changes to consultant/contractor status.

Explanation/ Key Points

Exceptions will be made when law requires such a disclosure or when the involved persons have previously clearly consented to the disclosure.

Rule - Personal Identifiers Prohibited

Any co-worker identifier, such as name or social security numbers, must not appear in any publicly accessible location managed by or controlled by your organization. This includes web pages, internet commerce sites, product manuals, and magazine advertisements.

Rule - Disclosing Organization Information

You must not disclose organization information to outsiders or internal departments, which do not require this information to do their jobs.

Explanation/ Key Points

This includes business plans, marketing strategies, new products, budgets and financial standings, executive meeting results, trade secrets, research results, corporate strategies, customer information, and any sensitive data or information that could harm, interrupt, or embarrass the organization.

Rule - Disclosing Organization Secured Areas

You should never disclose the location of your organization’s computer center, cash holding area, or other secured building, floor, or special room. The physical address should be confidential and must not be disclosed to those without a demonstrable need-to-know.

🕮 Rule - Disclosing Organization Future Plans Prohibited

You are forbidden from making any public representations about your organization's future earnings or the prospects for new products.

💣 ***Warning !*** This can avoid shareholder class-action lawsuits.

🕮 Rule - Organization Meetings and Sensitive information

If sensitive information is to be discussed orally in a meeting, seminar, lecture, or related presentation, the speaker must clearly communicate the sensitivity of the information. The speaker must also remind the audience to use discretion when disclosing it to others. Visual aids such as slides and overhead transparencies must include the appropriate confidentiality markings.

Explanation/ Key Points

Persons other than those specifically invited must not attend meetings where sensitive information will be discussed.

🕮 Rule - Sensitive Information and Meeting Rooms

You must erase black boards and white boards in conference rooms after meetings.

Explanation/ Key Points

When sensitive information has been recorded on black boards or white boards, it must be erased (with water or special cleaning fluids) before you leave the area.

🕮 Rule - Organization's Documentation

You must not take your organization's computer related documentation off-site or out of a secured area without proper permission.

Public Records/ Privacy (of citizens) Rules

Public records can also be private. If the information is a public record, yet you are not identified as the individual associated with the information, then it is considered to be private. However, if you are identified uniquely, such as by name, address, social security number, and such, then there is no longer privacy.

Rule - Privacy of Citizens

You must not reveal the privacy of citizens in any form from paper to software.

Rule - Privacy and E-mail

You must treat e-mail messages and files as private information. E-mail must be handled as a private and direct communication between a sender and a recipient.

Rule - Violating Others Privacy

You must not violate the privacy of other users and their data. For example, you shall not intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users, or represent themselves as another user unless explicitly authorized to do so by that user.

Rule - Public Records

Public records need to be accessible, yet protected against corruption, and loss.

Rule - Consent to Disclose Information to Law Enforcement

You must receive approval before allowing any information you use and store on your organization's systems to be divulged to law enforcement. The decision is at the discretion of the data owner or your organization's management.

Warning ! However, you must not allow police or other law enforcement to have access to your organization's information without a properly executed search warrant.

Rule - Collecting Private Information

You must not collect private information (race, religion, political opinions, sexual orientation, etc.) unless the collection effort has been approved in advance by your organization.

Rule - Children's Privacy

You cannot gather personal information about children without first obtaining clear and unambiguous consent from the involved parents or guardians.

Rule - Customers Privacy

You must only access customer information on a need-to-know basis and the information must be used only for internal business purposes. The collection of personal information about potential customers and others with whom your organization does business is customary and expected.

Explanation/ Key Points

Unless the clear and unambiguous consent of the party described by the information is first obtained, all third party sale, exchange, or other distribution is prohibited.

If you must get customers information (i.e. via a subpoena), the customer will be given {2} weeks advance notice prior to the release to provide the information.

All identifying information about customers such as credit card numbers, credit references, and social security numbers, must be accessible only to those personnel who need such access in order to perform their jobs.

ⓘ *Important !* You should never discuss customers private information in public places such as in building lobbies or on public transportation. This applies even when the identity of the customer is kept confidential.

Rule - Customers Disclosure to Third Party

You must not disclose information about your customers identity to third parties without proper permission from the customer.

Explanation/ Key Points

If given the proper approvals by the customer, you can provide the customer with the disclosure information, like contact names, telephone numbers and addresses of the third parties.

Rule - Explanation for Private Information

If you are requested to provide private information for business purposes, the full and complete reasons for collecting this information must be disclosed.

Explanation/ Key Points

You should report any refusal from any entity to provide private information if you have provided the proper identification and gathering reason.

Rule - Disclosure Notification / Blocking Privacy Request

If a third party requests information, the subject (citizen, customers, employee, etc.) must be given advance notice that their personal data held by your organization has been requested by a third party.

Explanation/ Key Points

Unless compelled to release the data by clear and authoritative law or regulation, a reasonable period of **{2}** weeks must be provided for the subject to block this disclosure. No response from the subject can within that period can be considered to be acquiescence to the disclosure.

Rule - Public Records Source Owner

Information generated by your organization and released to the public must be accompanied by the name of a designated employee acting as the single recognized official source and point-of-contact. All updates and corrections to this information that are released to the public must flow through this official source.

Rule - Materials Released to the Public

All information to be released to the public must have first have been reviewed and approved.

Explanation/ Key Points

Every speech, presentation, technical paper, book, or other communication to be delivered to the public must first have been approved for release by the proper authorities.

Paper Information Rules

Rule - Copying Sensitive Information

You must not photocopy or reprint sensitive information without proper authorization from the information owner.

Explanation/ Key Points

If additional copies of sensitive information are required, it must be recorded to include: number of copies, and recipients. Each of the recipients must be informed that distribution or copying is forbidden.

☝ ***Tip:*** You may want to number the copies of confidential documents individually with a sequence number to ensure that the persons responsible for the documents and the location of the documents can both be readily tracked.

Rule - Copying Sensitive Information and Special Paper

If you are releasing sensitive information to a third party, it can be distributed on special paper that cannot be copied using ordinary photocopy machines.

☝ ***Tip:*** You may also want to print sensitive information on special paper that will clearly show whether it is an original or a copy. This can achieved with color borders, watermarks, or other technology approved for such use.

Rule - Copier / Printer Malfunction

If you are making copies of sensitive information and the copy machine jams or malfunctions, you must not leave the copy machine / printer until all copies have been removed from the machine or are destroyed beyond recognition.

Rule - Attending to Printers

You must not leave the printers unattended if sensitive information is being printed or will soon be printed. You must be authorized to examine the information being printed.

Rule - Sensitive Information – Page Numbering

All sensitive organization information in paper form should indicate both the current and the last page.

Example: "page 6 of 51"

🕮 Rule - Third Party Copying Sensitive Information

Prior to sending any sensitive information to a third party for copying, printing, formatting, or other handling, the third party must sign an organization non-disclosure agreement.

🕮 Rule - Mailing Envelopes for Sensitive Information

If you are handling sensitive information by internal mail, external mail, or courier, it should be double wrapped.

Explanation/ Key Points

The outside envelope or container must be plain and not indicate the sensitivity of the contents contained therein.

The inside sealed envelope or container should be opaque and must be labeled Highly Restricted", "Confidential" or "To Be Opened by Addressee Only".

🕮 Rule - Tracking Mailed Sensitive Information

If you mail / deliver sensitive information, you must be able to track the information. For example, most couriers, UPS, Federal Express, and such offer a tracking process with a weigh bill number. It should always be marked for the recipient "signature required."

🕮 Rule - Delivering Sensitive Information

If you are responsible for delivering sensitive information, you must never leave it at an unattended desk, or left out in the open in an unoccupied office.

Even if you have given the information to a receptionist/ guard, it is recommended that you contact the intended recipient to acknowledgement receipt of the information.

🕮 Rule - Filing Sensitive Information

If you handle sensitive information in hard copy, you must file it in a locked file cabinets, closets, or desk drawer.

🕮 Rule - Destroying Unwanted Hard Copies

All waste copies of sensitive information that are generated in the course of copying, printing, or otherwise handling such information must be destroyed according to approved procedures.

It is suggested that if you need to discard unwanted hard copies of information, you need to shred it before it is thrown away.

Using Software and Data Rules

Rule - Malicious Intent is Prohibited

You must not intentionally develop programs that harass other users or infiltrate a computer system or damage or alter software components.

You are also prohibited from running or writing any computer program that can consume significant system resources or otherwise interfere with your organization’s business activities.

You must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any of your organization’s computer, network, or information.

Rule - Downloading Software

You must not download software from electronic bulletin board systems, the internet, or any other systems outside your organization. You must not use any externally provided software from a person or organization other than a known and trusted supplier. This is for protection against malicious software such as viruses, worms, Trojan horses, and other software which may damage your organization’s information and systems.

You also must not download software that is in violation of license agreements.

Rule - Protecting Software / Handling a Virus

Because viruses have become very complex, you must not attempt to eradicate it yourself if you have encountered a Suspicion or Incident.

If you suspect a virus, call the appropriate authorities immediately. *See Incident Reporting.*

Rule - Copying Software

You must not copy software provided by your organization to any storage media (floppy disk, magnetic tape, etc.), transfer such software to another computer, or disclose such software to outside parties.

Rule - Purchasing and Installing New / Upgraded Software

You must not install newly purchased software on you office PC, network servers, or other machines without first getting the proper approvals for set up and security.

Rule - Retaining Data

You must retain all financial accounting, tax accounting, and legal records for a period of at least {7} years. All other records must be retained for a period of at least {5} years.

Rule - Input Data Retention

Business source documents containing input data must be retained for at least **{90}** days beyond the date when this information was entered into your organization's computer system(s).

Using File and Directory Rules

Rule - Others User Directories and Files

You must never go into the directories and files of other users.

Rule - Unauthorized Access Prohibited

You should never have unauthorized access to software, data, or files even if your organization has not properly secured and protected them.

Rule - Receiving Files on Disks / CDs

The use of removable media (diskettes, CDs, …) is not permitted except where specifically authorized. They are the primary means of data distribution and a key area for security violations.

If you copy corrupt file(s) to your network, often their origin is not traceable.

ⓘ ***Important !*** Seemingly innocent files can contain a virus or other malicious code.

Rule - Setting up a New Directory

Data directories and structures should be set up by the owner of the files. They are the route map to the storage and access to files and data. Unauthorized access by others users to your directories should be prohibited.

ⓘ ***Important !*** Directories with files that contain sensitive information should be accessed with a password.

Rule - Amending Directory Structures

You should not change the existing directory structure set up by your organization without approval. Any unauthorized changes to the data paths may cause access rights to be circumvented.

Rule - Using Meaningful Directory and File Names

Your directory and file names should be meaningful to you. The naming is often arbitrary and can result in confusion in locating information. It should be intuitive for another authorized user to understand your structure in your absence. Poorly named files can result in accidental deletion or lost.

☝ ***Tip:*** Standards and naming conventions should be established.

Telephone, Faxes and Other Devices Rules

🕮 Rule - Telephone Disclosures

You must not disclose organization, customer, or other information by phone, unless the caller is positively identified and is authorized to have this information.

Telephone lines may be tapped or otherwise intercepted by unauthorized parties. For this reason, you should avoid discussing sensitive information regarding your organization when on the telephone.

ⓘ ***Important !*** Be especially careful when using speaker phones to discuss sensitive business issues.

🕮 Rule - Cellular Telephones

Sensitive information should NEVER be discussed on cordless or cellular telephones.

☝ ***Tip:*** You can use voice-line encryption if you need to discuss business on these telephones.

🕮 Rule - Answering Machines

You must not leave messages containing sensitive information on answering machines or voice mail systems.

🕮 Rule - Organization Credit Cards on Pay Phones

While using public pay telephones, you should swipe your organization's telephone card or other credit card rather than typing or speaking the billing information numbers.

🕮 Rule - Organization Telephone Book Security

Telephone books must not be distributed to outsiders or other third parties without specific authorization.

🕮 Rule - Consent to Record

In meetings or when using a telephone, you should not use speakerphones, microphones, loudspeakers, tape recorders, or similar technologies unless you have first obtained the consent of both the originator(s) and recipient(s) of the call.

Rule - Faxing Sensitive Information

If you need to fax sensitive information, the recipient must first have been notified of the time when it will be transmitted, and also have agreed that an authorized person will be present at the destination machine when the material is sent.

You must have the proper authority to fax the information. You should never fax sensitive information over unencrypted lines.

You must never allow a third party to perform the fax, that is, hotel staff, retail clerk, etc.

☝ ***Tip:*** You can have a password protected fax mailbox to restrict unauthorized release of the materials.

Rule - Fax Cover Sheet

If you are sending sensitive information via the fax, a cover sheet should first be sent and acknowledged by the recipient. After this is performed, the sensitive information may be sent via another call occurring immediately thereafter.

Rule - Taping Sensitive Information

You should not record sensitive information with dictation machines, tape recorders, or similar devices.

Explanation/ Key Points

If you must use these devices in your job, the proper sensitivity classification must be specified at the beginning and end of each segment of sensitive information. The recording media must also be marked with the most stringent data classification found on the media. It should be erased as soon as possible.

Rule - Video Conferencing

You must not record video-conferencing sessions must unless it is approved and communicated in advance to all videoconference participants.

Rule - Other Devices - Transmissions

You must never transmit confidential information via wireless microphones, walkie-talkies, radio local area networks (LANs), radio personal computer docking systems, and other unencrypted radio transmissions.

HR Related Rules

Rule - Personnel Records (privacy) and the Employee

You should have open access to your personnel records at your organization.

Explanation/ Key Points

Your personnel records must not be kept from you. You may be required to request you records in writing. You should be allowed to make a copy for yourself. Some HR departments require that files can only be reviewed at appointed times, during business hours, and in the presence of a Human Resources representative.

Your files are private and should not be accessed by anyone else. The only exception to this is for purposes of criminal investigation.

☝ ***Tip:*** Your organization could allow each employee a copy of your own personnel records to review and to ensure that it contains no errors every **{12}** months.

If employees object to the accuracy, relevance, or completeness of information appearing in their personnel file, they must be given an opportunity to add supplementary statements

Rule - Using Employee Information

The Human Resources Department must make reasonable efforts to ensure that all personal information is used only as intended, and that precautions preventing misuse are effective and appropriate.

Personal information about employees, consultants, or contractors, which has been gathered for one purpose, may not be used for another purpose without the clear and unambiguous consent of the parties to whom this information pertains.

Rule - Returning Organization Property

Employees, temporaries, contractors, and consultants should not receive their final compensation until they have first returned all hardware, software, working materials, confidential information, and other property belonging to the organization.

Rule - Help Wanted Ads and Disclosure

All public help wanted advertising or announcements must be approved in advance by the Human Resources Department or other designated area prior to being placed. This will ensure that labor law requirements are met, and that sensitive internal information is not inadvertently released.

Rule - Gathering Prospective Employee Information

Personal information about a prospective employee may not be gathered unless it is both necessary to make an employment decision and also relevant to the job in question. This includes marital status, family planning objectives, off-hours activities, political affiliations, performance on previous jobs, previous employers, credit history, education, and other personal details.

Rule - Employee Monitoring Notification

Your daily activities cannot be monitored without first securing your permission. Your organization cannot use computers to automatically collect information about your job performance unless you have first agreed.

Explanation/ Key Points

An exception may be those instances where advance permission is likely to change the behavior in question (e.g., suspected criminal activity).

This does not include the type of monitoring required to protect organization property, your safety, and your personal property. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no electronic monitoring will be performed.

Rule - Employee Job Performance Privacy

Individual employee job performance information must not be posted on bulletin boards or otherwise made available to others who do not have a legitimate business-related need-to-know.

Rule - Benefits Cannot be Denied

You cannot be denied benefits if you refuse to provide unnecessary private information. Disputes about the definition of "necessary private information" will be defined by your organization.

Rule - Employee Health and Safety Disclosure

Your organization must fully disclose to you, the results of toxic substance tests and other information relating to the health and safety of workers.

Chapter 10
Getting ISS Help

Getting ISS Help

You will probably receive this handbook 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

Appendix A - List of Rules

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

Logging On Rules (See Chapter 3)

- Rule - Unique User ID and Password
- Rule - Unsuccessful Logging On

Warning Banner Rules (See Chapter 3)

- Rule - Display a Warning Banner
- Rule - Warning Banner Keystroke Monitoring
- Rule - Warning Banner Last Log on

Logging Off Rules (See Chapter 3)

- Rule - Automatic Log Off
- Rule - Leaving Your Workstation - Logging Off / Locking

Identification (User ID) Rules (See Chapter 3)

- Rule - Unique User ID
- Rule - Prohibit Group User IDs
- Rule - Sharing your User ID is Prohibited
- Rule - Using Another User ID is Prohibited
- Rule - Dormant User IDs
- Rule - Internet User ID Expiration

Authentication (Password) Rules (See Chapter 3)

- Rule - Changing Your Default Password
- Rule - Difficult to Guess Passwords
- Rule - Minimum/ maximum Password Length
- Rule - Cyclical Previous Passwords
- Rule - Password Allowable Characters
- Rule - Passwords Lower and Upper Case
- Rule - Choosing Your Password
- Rule - Keeping Your Password Confidential
- Rule - Reusing Passwords / History
- Rule - Display and Printing Passwords
- Rule - Forced Expiration of Passwords
- Rule - Unsuccessful Passwords Attempts
- Rule - Same Password on Different Systems
- Rule - Disclosure Forces Password Change
- Rule - Writing Passwords Down
- Rule - Written Passwords Left Near Devices
- Rule - Proof Of Identify to Obtain a Password

Authorization (Privileges) Rules (See Chapter 3)

- Rule - Authorized Privileges

Network Access Rules (See Chapter 4)

- Rule - Approval for Connections
- Rule - Gaining Unauthorized Access
- Rule - Network Browsing Prohibited
- Rule - Network Backups
- Rule - Overwhelming the Network
- Rule - Malicious Intent and the Network

Modem Rules (See Chapter 4)

- Rule - Modems Connections to Internal Networks Prohibited
- Rule - Prohibit Modems in AutoAnswer Mode

Remote Access Rules (See Chapter 4)

- Rule - Dial-up Password Attempts
- Rule - Remote Access Training

Remote Sites Rules (See Chapter 4)

- Rule - Telecommuting Permissible Equipment
- Rule - Protection of Off-Site Property
- Rule - Information to be Returned
- Rule - Remote Working Environment
- Rule - Right to Conduct Inspections of Telecommute Office
- Rule - Sensitive Information on Portable Computers
- Rule - Backing up Portables Computers
- Rule - Transportable Computers Hand Luggage on Airplanes
- Rule - Portable Computer Security

E-mail Rules (See Chapter 5)

- Rule - E-mail for Business Purposes Only
- Rule - E-mail and Confidential Information
- Rule - Forwarding E-mail
- Rule - Forwarding External E-mails
- Rule - Forwarding E-mail to Archival Records
- Rule - E-mail Retention
- Rule - E-mail Virus Protection Software
- Rule - Certainty of E-mail File Attachments Origin
- Rule - Using another Users E-mail Account
- Rule - Using E-mail as a Database
- Rule - Deleting and Destroying E-mail
- Rule - Privacy and E-mail
- Rule - E-mail is Public Communication

- Rule - E-mail as a Public Record (government)
- Rule - E-mail Profanity
- Rule - Responding to Junk (SPAM) E-mail
- Rule - Ownership of E-mail Messages and Attachments
- Rule - Disclosure of E-mail Messages and Attachments
- Rule - Authorization to Issue Broadcasts in E-mail
- Rule - Scanned Signatures in E-mail
- Rule - Misrepresentation of Identity in E-mail

Internet Rules (See Chapter 5)

- Rule - Downloading Internet Files / Anti-Virus
- Rule - Sending Sensitive Information Over the Internet
- Rule - Uploading via the Internet
- Rule - Using the Internet for Personal Use
- Rule - Approval for Internet Connections
- Rule - Training for Internet Use
- Rule - Internet User ID Expiration
- Rule - Personal Messages Disclaimer on Internet
- Rule - Internet Products and Services
- Rule - Public Area of Your Organization’s Web Site
- Rule - Unofficial Web Pages on the Internet
- Rule - Concealing your Identity on Internet is Prohibited
- Rule - Exchanges of Information on the Internet
- Rule - Updating Organization Information on the Internet

E-commerce Rules (See Chapter 5)

- Rule - E-transactions
- Rule - Forming E-contracts
- Rule - Validating Identity of External Parties on Internet
- Rule - Electronic Offers
- Rule - Internet Customers

Workstation Rules (See Chapter 6)

- Rule - Workstation Protection Security
- Rule - Securing Unattended Workstations
- Rule - Loading Personal Screen Savers
- Rule - Altering Computer Equipment
- Rule - Moving and Relocating Your Equipment
- Rule - Sensitive Information While Working
- Rule - Locking File Cabinets
- Rule - Screen Positioning
- Rule - Clear Desk
- Rule - Clear Screen
- Rule - Office (with a door)
- Rule - Cubicle Security
- Rule - Bringing your personal PC/ laptop to Work
- Rule - Personal Equipment and Information Ownership

- Rule - Personal Equipment and Privacy
- Rule - Home Computers Security

Disposal Rules (See Chapter 6)

- Rule - Information Disposal/ Wiping
- Rule - Discarding Hardcopy Information
- Rule - Personal Equipment Disposal
- Rule - Media Disposal/ Concealment
- Rule - Erase and Zeroize
- Rule - Destruction Approval

Media Security Rules (See Chapter 6)

- Rule - Media Safety
- Rule - Hard Drive Security
- Rule - Sensitive and Non-sensitive on Same Media

Physical / People Security Rules (See Chapter 7)

- Rule - Tailgating and Piggybacking when Entering
- Rule - Lending Cards/ Keys, Tokens
- Rule - Challenging Strangers
- Rule - Handling Visitors
- Rule - Visitor Escorts
- Rule - Visitors Entrances
- Rule - Social Engineering
- Rule - Sensitive Information and Physical Access Controls
- Rule - Lock Office Doors
- Rule - Wearing ID Badges
- Rule - Temporary ID Badges
- Rule - Reporting Stolen/ lost Access Badges/ Cards/ Tokens
- Rule - Presenting Your Badge
- Rule - Propping Open Doors
- Rule - Stay away from Restricted Areas
- Rule - Property Pass for Removing Equipment

Copyright Rules (See Chapter 8)

- Rule - Copyright Laws for Software and Paper
- Rule - Copyrighted Inquiries
- Rule - Copying Copyright Materials
- Rule - Protection of Software and Copyrighted Materials
- Rule - Copyright Enforcement Statement
- Rule - Making Excess Copies Prohibited
- Rule - Copying Vendor Software
- Rule - Sending Copyrighted Information Electronically
- Rule - Violation of Copyright Laws
- Rule - Using Copyrighted Information from the Internet

- Rule - Ownership of Copyrighted Materials

Acceptable Use (of systems) Rules (See Chapter 9)

- Rule - Personal Use of your Computer
- Rule - Other Business Activities
- Rule - Using State-Owned Resources Unrelated to Business
- Rule - Using State Resources in an Acceptable Way
- Rule - Transmitting State-Owned Resources in an Acceptable Way
- Rule - Misrepresentation on State-Owned Resources
- Rule - Using Others Users Data on the State-Owned Resources
- Rule - Preventing Services to Others
- Rule - Storing Games on your Computer
- Rule - Giving Information to a Third Party
- Rule - Handling Third Party Confidential Information
- Rule - Third Party Agreements and Approvals
- Rule - Sensitive Disclosure Statement to Third Party
- Rule - Exposure of Sensitive information Public Places
- Rule - Time Sensitive Information

Other Employees/ Organization Rules (See Chapter 9)

- Rule - Disclosing Co-worker(s) Contact Information
- Rule - Disclosing Co-worker(s) Change in Status Information
- Rule - Personal Identifiers Prohibited
- Rule - Disclosing Organization Information
- Rule - Disclosing Organization Secured Areas
- Rule - Disclosing Organization Future Plans Prohibited
- Rule - Organization Meetings and Sensitive information
- Rule - Sensitive Information and Meeting Rooms
- Rule - Organization’s Documentation

Public Records/ Privacy (of citizens) Rules (See Chapter 9)

- Rule - Privacy of Citizens
- Rule - Privacy and E-mail
- Rule - Violating Others Privacy
- Rule - Public Records
- Rule - Consent to Disclose Information to Law Enforcement
- Rule - Collecting Private Information
- Rule - Children’s Privacy
- Rule - Customers Privacy
- Rule - Customers Disclosure to Third Party
- Rule - Explanation for Private Information
- Rule - Disclosure Notification / Blocking Privacy Request
- Rule - Public Records Source Owner
- Rule - Materials Released to the Public

Paper Information Rules (See Chapter 9)

- Rule - Copying Sensitive Information
- Rule - Copying Sensitive Information and Special Paper
- Rule - Copier / Printer Malfunction
- Rule - Attending to Printers
- Rule - Sensitive Information – Page Numbering
- Rule - Third Party Copying Sensitive Information
- Rule - Mailing Envelopes for Sensitive Information
- Rule - Tracking Mailed Sensitive Information
- Rule - Delivering Sensitive Information
- Rule - Filing Sensitive Information
- Rule - Destroying Unwanted Hard Copies

Using Software and Data Rules (See Chapter 9)

- Rule - Malicious Intent is Prohibited
- Rule - Downloading Software
- Rule - Protecting Software / Handling a Virus
- Rule - Copying Software
- Rule - Purchasing and Installing New / Upgraded Software
- Rule - Retaining Data
- Rule - Input Data Retention

Using File and Directory Rules (See Chapter 9)

- Rule - Others User Directories and Files
- Rule - Unauthorized Access Prohibited
- Rule - Receiving Files on Disks / CDs
- Rule - Setting up a New Directory
- Rule - Amending Directory Structures
- Rule - Using Meaningful Directory and File Names

Telephone, Faxes and Other Devices Rules (See Chapter 9)

- Rule - Telephone Disclosures
- Rule - Cellular Telephones
- Rule - Answering Machines
- Rule - Organization Credit Cards on Pay Phones
- Rule - Organization Telephone Book Security
- Rule - Consent to Record
- Rule - Faxing Sensitive Information
- Rule - Fax Cover Sheet
- Rule - Taping Sensitive Information
- Rule - Video Conferencing
- Rule - Other Devices - Transmissions

HR Related Rules (See Chapter 9)

- Rule - Personnel Records (privacy) and the Employee

Appendix

- Rule - Using Employee Information
- Rule - Returning Organization Property
- Rule - Help Wanted Ads and Disclosure
- Rule - Gathering Prospective Employee Information
- Rule - Employee Monitoring Notification
- Rule - Employee Job Performance Privacy
- Rule - Benefits Cannot be Denied
- Rule - Employee Health and Safety Disclosure

Index