# [*Organization*] Information Security Procedures

## Purpose

The purpose of these Information Security Procedures is to establish the minimum administrative, technical, and physical safeguards that will be utilized by [*Organization*] to protect sensitive information from unauthorized access, disclosure, corruption, or destruction.

The intention of these procedures is to implement the data security policy enacted by [*Organization*] and to ensure that [*Organization*] is in compliance with all applicable state and federal laws and regulations regarding data privacy and security, and to protect sensitive information from foreseeable security threats.

## Scope

[*Organization*] will apply these procedures to all sensitive information that it owns or which is in its possession or control, or which it may disseminate to other authorized persons in the performance of [*Organization*]'s or other such person's business, statutory or regulatory functions.

## Procedures

**Security and Proprietary Information**

- The organization's official website should not contain any sensitive information.
- Information contained on the organization's systems including public or private websites should be classified as either public or sensitive, as defined by the information sensitivity procedures.
- Passwords shall be kept secure and shall not be shared with any other person. Authorized users are responsible for the security of their passwords and accounts.
- System level passwords must be changed on an [*insert time frame*] basis. System level accounts include, but are not limited to the following:
    - Root
    - Enable (Cisco Account)
    - Network Administration
    - Database accounts with access to sensitive information
    - Application Administration
- User level passwords must be changed in accordance with the organization's systems use policy, but in any case no less than semi-annually. User level accounts include, but are not limited to the following:
    - Email
    - Web
    - Network
    - Application Accounts with access to sensitive information.
-

procedures for securing sensitive data in furtherance of [*Organization*] data security policy.

Sending or receiving data, or in any manner utilizing [*Organization*]'s equipment, systems, or resources to engage in any activity in violation of local, state, or federal law.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

**System and Network Activities**
Prohibited activities include but are not limited to the following:

- Violations of copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by [*Organization*].
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which [*Organization*] or the end user does not have an active license.
- Exporting software, technical information, encryption software or technology, in violation of export control laws.
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done remotely.
- Using a [*Organization*] equipment or systems to procure or transmit material that is in violation of [*Organization*]'s workplace rules as defined in the [*Organization*] handbook.
- Making fraudulent offers of products, items, or services originating from any [*Organization*] account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning without the prior express authorization of management.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying serv

High risk information is information that is protected by state or federal law, or information which if accessed by unauthorized persons might foreseeable result in significant financial loss, embarrassment, or inconvenience to affected persons. High risk

**General**

- All employees, contractors, vendors, or other persons who are granted access to [*Organization*]'s network shall agree to maintain all access procedures and codes in strict confidence and shall not share such information with any unauthorized person. It is the responsibility of [*Organization*]'s employees, contractors, vendors and agents with access privileges to [*Organization*

In order to maintain the security of sensitive information on an internally stored database, access by software programs may be granted only after authentication with credentials. The credentials used for the authentication shall not reside in the main, executing body of the program's source code in clear text. Database credentials shall not be stored in a location that can be accessed through a web server.

**Storage of Database User Names and Passwords**

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file shall only be accessible by authorized users.
- Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials shall not reside in the documents tree of a web server.
- Pass through authentications (i.e., Oracle OPS$ authentication) shall not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database shall adhere to the [*Organization*]'s Password Procedures.

**Retrieval of Database User Names and Passwords**

- If stored in a file that is not source code, the database user names and passwords shall be read from the file immediately prior to use.

€
not alscode, hat thiThethat is not54.0.0013.67 0hal name3.tabuting 4.0.00ed foauthen(passwn)1(tiaer

### Database Credentials

- Every program or collection of programs implementing a single business function shall have unique database credentials. Sharing of credentials between programs is prohibited.
- Database passwords used by programs are system-level passwords and shall adhere to the [*Organization*]'s Password Procedures.
- Developer groups shall have a process in place to ensure that database passwords are controlled and changed in accordance with the [*Organization*]'s Policy and Procedures. This process shall include a method for restricting knowledge of database passwords on a need-to-know basis.

## Password Procedures

All authorized users are required to select and maintain passwords in accordance with the guidelines below.

### General

- All system-level passwords (e.g., root, enable, Administration, application administration accounts, etc.) must be changed on a [insert time frame] basis.
- All user-level passwords (e.g., email, web, network, etc.) must be changed in accordance with the organization's systems use policy, but in any case no less than semi-annually.
- Passwords shall not be transmitted in any form of non-encrypted electronic communication.
- Where SNMP is used, the community strings should be defined as something other than the standard defaults of "public," "private" and "system" and should be different from the passwords used to log in interactively. A keyed hash should be used where available (e.g., SNMPv2).
- All user-level and system-level passwords should conform to the guidelines described below.

### Password Rules

Password guidelines should be substantially similar to the following criteria:

- Be at least 8 characters in length
- Contain at least 3 of the 4 following password complexity requirements:
  - Lowercase letters (e.g., a – z)
  - Uppercase letters (e.g., A – Z)
  - Numbers (e.g., 1 – 9)
  - Characters (e.g., (!@#$%^&*)
- Not be based on personal information: names of family, pets, etc.
- Not be written down or stored on-line

**Password Protection Standards**

It is suggested that passwords chosen for [*Organization*]'s accounts shall not be the same as passwords chosen by the employee or third party for non-[*Organization*] accounts.

All passwords are to be treated as sensitive, confidential information. Passwords are not be shared with anyone, including administrative assistants or secretaries.

If an account or password is suspected to have been compromised, immediately report the incident to the employee's immediate supervisor and/or the Information Security Officer.

Users shall not knowingly or intentionally send or receive, or allow to be sent or received any programs or files they know or reasonably should know to contain any malicious content including but not limited to viruses, worms, Trojan horses

- Logs and audit trails must be saved as follows:
  - All security related logs must be kept online for a minimum of 1 week.
  - Weekly full tape backups of logs and audit trails must be retained for not less than 2 weeks.
  - Monthly full backups must be retained for not less than 6 months.
- Logs and audit trails must be reviewed as follows:
  - Event logging shall occur at the network, operating system, application and security levels.
  - Logs and audit trails should be reviewed weekly.
- Promptly report all security-related events to the Information Security Officer.
- The Information Security Officer shall promptly investigate and take appropriate remedial action with respect to any suspected or attempted attacks on the security system or attempts to gain unauthorized access to sensitive information.
- Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts or non-public personal information
  - Anomalous occurrences that are not related to specific applications on the host

**Router Security Procedures**

This procedure describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of [*Organization*].

Every router shall meet the following configuration standards:

- No local user accounts are configured on the router. Routers must use TACACS+, or comparable standard, for all user authentication.
- The enable account password on the router shall be stored in a secure encrypted form on the router. All [*Organization*]'s routers should have the same encrypted password for the enable account.
- Disallow the following
  - IP directed broadcasts
  - Incoming packets at the router sourced with invalid addresses such as RFC1918 address
  - TCP small services
  - UDP small services
  - All source routing
  - All web services running on the router
- Use corporate standardized SNMP community strings.
- Access rules are to be added as business needs arise and as approved by the Information Security Officer.
- Each router must have the following statement posted in clear view:

## Physical

All references to security in this section are related to physical security. Issues of electronic data security and intellectual property are covered elsewhere within this document. Physical security includes building and room security as well as physical security devices such as locks and physical restraints. Physical security is related to electronic data and intellectual property security. The ability to physically access a computer or paper files may compromise the security of electronic data. Physical security depends on many things. Building construction details such as the type of floors, walls, roof and especially windows are important.

Alarms and other security systems tend to increase building security. Some of the types of security systems in [*Organization*] buildings are door monitor systems and after-hours motion detection and alarm systems.

The type, quantity and value of equipment and information located in [*Organization*] buildings are important security factors. The more desirable or marketable these items are, the more likely it is that someone will attempt to breach [*Organization*] security.

### Physical Security Procedures

- All building exterior doors are to be kept locked at all times except where specific procedures have been established to leave a door unlocked. Doors shall be left unlocked or open only while a staff member is in a position to monitor access through the doorway. No one shall provide or allow access to any building or room to anyone who is not known to them to be an employee with authorization to work in that area, or an authorized visitor or vendor. Employees are encouraged to challenge in a non-offensive manner anyone in an [*Organization*] building or room whom they do not know. Any person who is suspicious or cannot provide identification must be reported to management. If you witness a building problem, such as a faulty lock or door, or something potentially dangerous, you must notify management.
- Individual workstations may be located in a single office or a larger room with multiple workstations. Users must control physical access to their office and thus their computer. All rooms shall be kept locked unless a staff member is in the room or within sight of the room (in a position to monitor access to the room) or specific procedures have been established to allow the room to be left unlocked. Employees may choose not to lock a room for brief periods during regular working hours if the room does not contain sensitive information. However, employees are advised to lock all rooms any time no one is there to monitor access.
- All rooms containing allocated systems, production servers and related

- Office and building keys are distributed to [*Organization*] employees and authorized users based on the individual employee's actual need for access to specific areas.
- Equipment assigned to the employee is the responsibility of the individual employee. If any equipment is moved, broken, or replaced, the Information Technology staff or vendors must be notified. In the event that any equipment is to be upgraded in accordance with the [*Organization*] policy, the Information Technology Staff must give prior approval to the upgrade and perform the upgrade. Any non-mobile [*Organization*] equipment taken off-site will require authorization in accordance with the [*Organization's*] written policies and procedures. Laptops, PDA's and other mobile devices specifically assigned to an employee may be taken off-site by that employee without such specific authorization. The employee is responsible for the physical security of any company equipment to which he or she is entrusted.
- All company equipment must be tracked through inventory control and audited not less than annually by the [*Department*].
- If [*Organization*]-issued equipment becomes lost or stolen, the individual with responsibility for the equipment must immediately report this to the Information Security Officer.
- Machines that are decommissioned (surplused/scrapped) are to be sent to

message he knows it comes from you and no one else.

Public-key systems, such as Pretty Good Privacy (PGP) and the RSA cryptographic algorithm, are becoming popular for transmitting information via the

| | |
|---|---|
| | number which is attached to data frames to tell the network how to route the data. A 13-bit field that defines the destination address of a packet. The address is local on a link-by-link basis. |
| E-mail bombs | A denial of service attack in which an excessive amount of e-mail data is sent to an e-mail address in an attempt to disrupt the e-mail service, or to prevent the recipient from receiving legitimate messages. |
| E-mail header | The text at the beginning of an Internet e-mail message. It is generated by the client mail program that first sends it and by all the mail servers en route to the destination. Each node adds more text, including from/to addresses, subject, content type, time stamp and identification data. You can trace the path of the message from source to destination by reviewing the e-mail header text. |
| Forged routing | The act of intercepting packets and changing the TCP/IP routing address |
| Hash number | Producing hash values for accessing data or for security. A hash value (or simply hash), also called a message digest, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value |
| IDEA | (International Data Encryption Algorithm) - A private key encryption-decryption algorithm that uses a key that is twice the length of a DES key. |
| IP directed broadcasts | A directed broadcast is a broadcast destined for networks other than the networks on which it originated. By enabling IP's directed-broadcast feature, you can forward IP packets whose destination is a nonlocal (for example, remote LAN) broadcast address. For example, the source host originates a unicast packet. IP then forwards the packet, as a unicast, to a destination subnet and explodes the packet into a broadcast. You can use this feature to locate network servers and to enable both the forwarding and exploding of directed broadcasts. |
| IPSec | A framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), IPSec ensures confidentiality, integrity, and authenticity of data communications across a public network. IPSec provides a necessary |

| | |
|---|---|
| | component of a standards-based, flexible solution for deploying a network wide security policy. |
| ISDN | Integrated Service Digital Network. A system that provides simultaneous voice and high speed data transmission through a single channel to the user's premises. ISDN is an international standard for end-to-end digital transmission of voice, data and signaling. |
| LDAP | Lightweight Directory Access Protocol is designed to provide access to directories supporting the X.500 models, while not incurring the resource requirements of the X.500 Directory Access Protocol (DAP). This protocol is specifically targeted at management applications and browser applications that provide read/write interactive access to directories. When used with a directory supporting the X.500 protocols, it is intended to be a complement to the X.500 DAP. |
| Network sniffing | Sniffing is the act of intercepting and inspecting data packets over a network. |
| Non-Public Personal Information | Non-Public personal information contains information on individuals including claimants and employees. Non-public personal information links an individual's name to one or more pieces of other information of a sensitive nature, for example, a social security number, financial account number, or health information. Because NPI placed in the hands of an unauthorized person could result in substantial financial harm or embarrassment to the individual, this type of information requires the highest level of security |
| One-time Password | The purpose of a one-time password (OTP) is to make it more difficult to gain unauthorized access to restricted resources, like a computer account. With OTP, the user creates a password, and the system creates a variation of the password each time a password is required. In this way, the same password is never used twice. With OTP, even if an attacker learns a password by snooping, he won't be able to use it again. |
| Packet spoofing | A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that |

| | |
|---|---|
| | the packets are coming from that host. Newer routers and firewall arrangements can offer protection against IP spoofing. |
| Passphrase | A secret string of words used to authenticate an individual's identity during system logon. Similar to a password, it can be made up of any number of characters. A passphrase is generally thought to be stronger than a password, although not many programs support its use. Passphrases are often used to control both access to, and operation of, cryptographic programs and systems. |
| Ping | A computer network tool used to test whether a computer network host Is reachable across an IP network. |
| Pinged floods | The act of using the ping utility or command to continuously ping a machine causing network traffic congestion. |
| Pirated software | Pirated software is software obtained without proper licensing. |
| Port scanning | An attempt by hackers to find the weaknesses of a computer or network by scanning or probing system ports via requests for information. It can be used by IT professionals as a legitimate tool to discover and correct security holes. But it can also be used maliciously to detect and exploit weaknesses IP spoofing. |

| | |
|---|---|
| | 1994. It is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. Allowable choices for the block size are 32 bits (for experimentation and evaluation purposes only), 64 bits (for use a drop-in replacement for DES), and 128 bits. The number of rounds can range from 0 to 255, while the key can range from 0 bits to 2040 bits in size. Such built-in variability provides flexibility at all levels of security and efficiency. |
| RFC1918 address | In Internet terminology, a private network is a network that uses RFC 1918 private IP address space. Computers may be allocated addresses from this address space when it's necessary for them to communicate with other computing devices on an internal (non-Internet) network but not directly with the Internet. |
| RSA | In cryptography, RSA is an algorithm for public-key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is still widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys. RSA is a public/private key system. |
| SNMP | Simple Network Management Protocol - Network management protocol used in TCP/IP networks. |

SNMP m neC42 140.or sig8y used in m neC4sse when itenc6Tw[(Rraph8

Soliev3(cketwShkey, [SH.TjETrithm known to be )TjT*-1-0.0001 3ers mUN
ab[SH.TjEctuirlgoa.6.48

| | |
|---|---|
| | secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted. SSH uses RSA public key cryptography for both connection and authentication. |
| SSID | SSID is an acronym for Service Set Identifier. The SSID is a sequence of up to 32 letters or numbers that is the ID, or name, of a wireless local area network. The SSID is set by a network administrator and for open wireless networks, the SSID is broadcast to all wireless devices within range of the network access point. A closed wireless network does not broadcast the SSID, requiring users to know the SSID to access the network. Most wireless base stations come with a default SSID that is easily found on the Internet and security experts recommend changing the default SSID to protect your network. |
| Symmetric encryption | Symmetric encryption (AKA private key, secret key, or single key systems) uses a single key. That key is used both to encrypt and to decrypt information. A separate key is needed for each pair of users who exchange messages, and both sides of the encryption transaction must keep the key secret. The security of the encryption method is completely dependent on how well the key is protected. The Data Encryption Standard (DES) algorithm is a Symmetric encryption algorithm. |
| TACACS+ | Terminal Access Controller Access Control System. Authentication protocol, which provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution. |
| TCP small services | TCP small services consist of the following four router commands:<br><br>Echo: Echoes back whatever you type through the telnet x.x.x.x echo command.<br><br>Chargen: Generates a stream of ASCII data Use the telnet x.x.x.x chargen command.<br><br>Discard: Throws away whatever you type. Use the |

| | |
|---|---|
| | telnet x.x.x.x discard command.<br><br>Daytime: Returns system date and time, if it is correct. It is correct if you run Network Time Protocol (NTP), or have set the date and time manually from the exec level. Use the telnet x.x.x.x daytime command. |
| TCP wrapper | Access control mechanism which allows/disallows and records access to TCP daemon. A daemon is a program that runs in the background whenever needed, carrying out tasks for t |

| | |
|---|---|
| | characters terminated with a CR+LF. |
| Worm | A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up a computer's resources and possibly shutting the system down. |
| X.509 | The X.509 directory service standard which, among many other things, defines specific formats for PKC (Public Key Certificates) and the algorithm that verifies a given certificate path is valid under a given PKI (called the certification path validation algorithm). X. 500 is relevant to public key infrastructures describing two authentication methods: simple authentication based on password usage and strong authentication based on public key cryptography. The current release, Version 3, added certificate extensions to the X.509 standard. |

## Revision History

| Version | Date | Comments |
|---|---|---|
| | | Initial Version – Approved by Receivership and Insolvency Task Force |
| | | |