Receivership Data Privacy and Security Procedures
For Property and Casualty Insurers in Liquidation

Drafting Note: The Receivership Data Privacy and Security Procedures for Property and Casualty Insurers in Liquidation are to be considered as guidance for state insurance departments, receivers and guaranty associations.

[*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

Administrative

Acceptable Use Procedures

[*Organization*]'s information systems and networks shall be used exclusively for the furtherance of [*Organization*]'s business.

Employees shall receive training on [*Organization*]'s data and security policy and their obligations regarding the protection of sensitive information, including procedures for protecting non-public personal information from unauthorized access, improper use, or destruction. Training shall be conducted upon employment, during orientation, at the commencement of a receivership with company employees and thereafter not less than annually. Employees are required to comply with these procedures as a condition of their employment. All employees or third parties who are granted access privileges shall sign a written acknowledgement of having received and read [*Organization*]'s security policy and procedures, and agreed to comply with its provisions or affirm in writing that he/she is bound and agrees to comply with a security policy and procedures substantially similar to those of [*Organization*].

General Use and Ownership

- All data created or residing on the [*Organization*]'s systems are subject to this policy.
- All data containing non-public personal information must be encrypted before it is electronically transmitted. In all other circumstances, non-public personal information and other sensitive information shall be encrypted in accordance with the Information Sensitivity Procedures starting on page 7.
- For purposes of this policy, ALL information and data residing on its systems and networks is considered the property of [*Organization*]. [*Organization*] may at any time monitor or audit any information, including data files, emails, and information stored on company issued computers or other electronic devices for any reason, at any time, with or without notice for the purpose of testing and monitoring compliance with these security procedures.

All sensitive information shall be kept confidential and shall not be distributed to or made available to any person without appropriate authorization.

Sensitive information shall be used solely and exclusively for the purpose of the administration of a receivership and shall not be utilized for any other purpose.

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.
- All computers, laptops and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 30 minutes or less, or by logging-off (Ctrl+Alt+Del for Windows 2000 or later users) when the host will be unattended.
- Sensitive information shall not be stored on any portable computer or portable electronic device unless the information is encrypted in accordance with the standards defined in these procedures.
- All equipment used by an authorized user connected to the [*Organization*]'s network, whether owned by the authorized user or [*Organization*], shall be continually protected and scanned for viruses and other malicious software at least [*insert time frame*] using approved virus-scanning software with a current virus database.
- Authorized users must use extreme caution when opening e-mail attachments, which may knowingly or unknowingly contain viruses, e-mail bombs, or Trojan horse code. All users shall receive instruction in recognizing potential hazards.

Unacceptable Use

The following activities are prohibited, provided however that nothing in this list shall be construed to prevent [*Organization*] authorized personnel from reviewing, monitoring, testing or improving applicable systems and 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 service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/Intranet/Extranet.
- Providing sensitive information to any third party without the appropriate authorization.
- Disabling or by-passing any security system, procedure or device installed or directed by [*Organization*].

Email and Communications Activities

- Sending unsolicited email messages not related to [*Organization*]'s business functions, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Unauthorized use, or forging, of email header information.

Technical

Information Sensitivity

All information owned, held, utilized or transmitted by or through [*Organization*] is subject to these procedures. Depending upon the nature of the information, higher levels of security shall be applied to secure information with greater sensitivity.

Public Information*

Public information is any information in the public realm that may be freely disseminated at the discretion of [*Organization*].

Sensitive Information*

Confidential Information

Confidential information is any information that in entitled to some level of protection either by law, contract, or custom, or where there is a need or expectation of privacy due to the potential financial or other harm arising out of the unauthorized access or release of such information. Examples may include budget information, matters subject to confidentiality agreements, financial data, strategic plans, and critical self analysis.

High Risk Information

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 information includes non-public personal information as defined in these procedures. Additional examples include such things as personnel and payroll records and employee health records.

*States should adopt definitions for public and sensitive information that are substantially similar to the definitions presented after review of applicable state laws.

Transmission Encryption Methodology
Information defined as sensitive and transmitted by or through [*Organization*] must be encrypted. Transmission of high risk information should follow proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA. These algorithms represent the actual cipher used for an approved application. Symmetric crypto-system key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Encryption standards and technologies will be reviewed at least annually and upgraded as technology improves.

All encryption technologies in use for data or data transmissions must be approved by the Information Security Officer and centrally managed by the organization’s designated technology department or approved provider.

Website access to High Risk Information
The [*Organization*] is committed to data security and the data quality of personally identifiable information that is either available from or collected by our website and will protect such information from loss, misuse or alteration. Website access to High Risk Information, as defined in this procedure, requires the use of secure socket layer (SSL) with a minimum of 128-bit encryption to protect the transmission of information. All information made available on the website is stored securely and is subject to legal disclosure requirements.

Browsers not supporting 128-bit encryption will not be allowed access to High Risk information.

Remote Access
Access to sensitive information housed in [*Organization*]’s network shall be made available to only to those individuals, including employees and third party vendors, etc., with a demonstrable need for access to that information. Authorizations will be made on a case by case basis by the Information Security Officer based upon established guidelines provided by management.

It is the responsibility of employees or third parties with access privileges to ensure a remote connection to the organization is not used by unauthorized persons to gain access to an organization’s information system resources.

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*] network to ensure that their access connection is subject to security procedures substantially similar to those of [*Organization*].

Requirements

- Secure remote access shall be strictly controlled and shall be available only to those individuals authorized by the Information Security Officer. Authorized access shall be established using one-time password authentication or public/private keys with strong pass-phrases.
- Authorized users shall not provide their login credentials to any other person, nor shall users write or make other written record of their login credentials.
- Authorized users shall access the network only with equipment provided by [*Organization*] unless otherwise approved by the Information Security Officer.
- Authorized users shall ensure that remote connections meet minimum authentication requirements such as CHAP or DLCI.
- Authorized users shall ensure that any remote host connecting to the organization's internal networks uses antivirus software with the most up-to-date virus definitions.
- Equipment with remote access to high risk information must meet the Transmission Encryption Methodology standards when working with the high risk information.
- Sensitive information shall not reside locally on a remote access computer or other information storage device unless the information is encrypted in accordance with the standards defined in these procedures.

Computer-to-Analog Line Connections

The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from personnel or contractors within the [*Organization*] will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to [*Organization*], and active penetrations have been launched against such lines by hackers. Waivers to the policy above will be granted on a case by case basis for a limited time period. Renewal of a waiver must be reviewed and approved in writing by the Security Officer.

Databases Storing Sensitive Information

The following procedures apply to any software programs and/or databases developed or maintained by [*Organization*]. To the greatest extent possible the [*Organization*] should seek to assure that any third party software meets the same standards.

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. Immediately following database authentication, the memory containing the user name and password shall be released or cleared.
- Database credentials shall be physically separated from other areas of the corresponding code, e.g., the credentials shall be in a separate source file. The file that contains the credentials shall contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file shall not reside in the same browseable or executable file directory tree in which the executing body of code resides.
- These requirements apply to any applications developed by [*Organization*]. To the greatest extent possible the [*Organization*] should seek to assure that any third party software meet the same standards.

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.

Application Development Standards

Applications shall contain the following security precautions:

- Authentication is applied to individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must provide for role based security, such that users with equal or greater security access can take over the functions of another without having to know the other's password.
- Applications must support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

Use of Passwords and Passphrases for Remote Access Users

Access to [*Organization*]'s network via insecure remote access methods such as computer-to-analog line connections, which have been approved for a limited time period, shall be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Anti-Virus Procedures

This procedure establishes requirements which must be met by all computers connected to [*Organization*] networks to ensure effective virus detection and prevention.

- All [*Organization*] servers and workstations shall have [*Organization*]'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files shall be kept up-to-date. Any virus-infected computer shall be isolated from the network until it is verified by the Information Security Officer or his designee as virus-free.
- All incoming and outgoing data and electronic mail must be scanned for viruses.
- As provided for in the Data Privacy Security Policy and Procedures, authorized users not part of the organization with a connection to the [*Organization*]'s network must be protected with an approved, licensed anti-virus software product that is kept updated in accordance with the vendor's recommendations.

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, or e-mail bombs.

Server Security

This procedure applies to server equipment which stores and/or transmits sensitive information and is owned and/or operated by [*Organization*] or a third party vendor.

Ownership and Responsibilities

Internal servers deployed at [*Organization*] shall be managed by an individual or operational group (Information Technology Department) or third party vendor that is responsible for system administration. Approved server configuration and security guides should be established and maintained by the individual or operational group. Such person or group shall monitor configuration and security compliance and implement an exception policy tailored to the organization's environment.

General Configuration Guidelines

- Follow the security best practices established in these procedures.
- Disable services and applications that are not currently in use or expected to be used.
- Utilize methods to control and log access to systems, for example, TCP Wrappers, whenever practical.
- Install the most recent security patches on the system as soon as practical, the only exception being when immediate application would interfere with business operations.
- Do not use a trust relationship between systems when some other method of communication will suffice.
- Always use standard security principles of granting a user the minimum security access necessary to perform a function.
- Do not use root or Administrator accounts when a non-privileged account will allow the required access.
- If a secure channel connection is available (i.e., technically feasible), privileged access must be performed over such secure channels, (e.g., encrypted network connections using SSH or IPSec).

Position servers in an access-controlled environment whenever possible. (See Physical section further in this document). End user access to servers storing sensitive information is permitted only from controlled work areas. System administrator access to servers storing sensitive information may be permitted by the information security officer on a case-by-case basis.

Monitoring

- Maintain and routinely review logs and audit trails on all security-related events.

- 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:

> "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission from the Information Security Officer to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

Wireless Communications Procedures

This procedure prohibits access to [*Organization*] networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of these procedures or have been granted an exclusive waiver by the Information Security Officer are approved for connectivity to [*Organization*]'s networks.

This procedure covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of [*Organization*]'s internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to [*Organization*]'s networks do not fall under the purview of this policy.

Register Access Points and Cards

All wireless Access Points / Base Stations connected to the network must be registered and approved by the Information Security Officer. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in laptops or desktop computers must be registered with the Information Security Officer. The Information Security Officer shall be responsible for keeping a registry of the devices.

Encryption and Authentication

Wireless implementations must maintain point to point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or similar technology.

Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier. Whenever possible the SSID should not be broadcast.

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 equipment are to be kept locked with access limited to authorized employees.
- All windows shall be kept locked unless an employee is in the room or in a position to monitor access to the room. It is very important to close and lock windows in rooms on lower floors.

- 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 the Information Technology department or vendor to have the hard drive wiped so that any sensitive data is unrecoverable in accordance with [*Organization*] Security Policy.
- Machines that are swapped internally between individuals or groups, which contained sensitive data (original or derived), must have the hard drive wiped before being utilized by the new user.
- Prior to the last day of employment, employees must return any mobile devices or equipment, any off-site equipment authorized for their use, and any portable media belonging to [*Organization*].

Server Room Security Guidelines and Recommendations

- Don't arouse unnecessary interest in secure areas -- minimize use of location signs.
- Minimize external access. Secure rooms should only have one or two solid, lockable doors. The doors should be observable by staff. Doors to secure areas should never be left open.
- Maintain appropriate locks. Keep doors and windows locked when room is not in use. Maintain secure system for keys and combinations. If there is a breach, each compromised lock should be changed.
- Maintain automatic fire suppression system, and provide appropriate staff training in its use.
- Maintain reasonable climate control in secured rooms, with temperature ranges between 50 and 80 degrees Fahrenheit, with a humidity range of 20% - 50%.
- Minimize nonessential materials that could jeopardize a secure room. Examples of nonessential items include: coffee, food, cigarettes, curtains, reams of paper, and other flammables.

Storage and Destruction of Sensitive Information

- Keep the hard copies and portable media (CDs, USB drives, DVDs, etc.) locked up in a secure area.
- Limit access to sensitive information to essential personnel.

Destruction of all sensitive information must be done in such manner to ensure the information is rendered completely and permanently destroyed.

Hard copies of sensitive information should be destroyed by pulping or shredding.

Sensitive information on portable media must be completely erased, or the media destroyed. Simply deleting a file is not sufficient to prevent a user from recovering the file later.

If a computer system is to be discarded, sold, transferred, etc, all files must first be erased from the hard drive by wiping the hard drive. An appropriate member of the technology department or approved provider must verify this process has been completed before the equipment leaves [*Organization*]'s premises or control.

Compliance

- Audits of the security procedures shall be performed not less than annually and upon the occurrence of any event in which a review of current procedures is appropriate. Such audit shall be performed by an authorized employee of the organization or by an outside individual or firm at the discretion of management.

Enforcement

This Information Security Policy is incorporated by reference into the [*Organization*] employee handbook. Violations of this policy by employees may result in disciplinary action up to and including termination.

Access to sensitive information by other authorized users is conditioned upon compliance with these procedures, or procedures that are substantially similar in nature and scope. Such persons who fail or refuse to comply with these policies will not be allowed access to [*Organization*]'s systems and may be liable for damages to third parties or subject to other penalties imposed by law.

Glossary

Term	**Definition**
Analog	Analog refers to electronic transmission accomplished by adding signals of varying frequency or amplitude to carrier waves of a given frequency of alternating electromagnetic current. Broadcast and phone transmission have conventionally used analog technology. A modem is used to convert analog to digital information to and from your computer.
Asymmetric encryption	Asymmetric encryption uses different keys for encryption and decryption. One key is used to encrypt the message and another key to decrypt it. The encryption key is normally called the public key in some algorithms because it can be made publicly available without compromising the secrecy of the message or the decryption key. The decryption key is normally called the private key or secret key. Systems that are used in this fashion are called public key systems. Sometimes, people call all asymmetric key systems "public key," but this is not correct—there is no requirement that one key be made public. Public and private keys are mathematically related. If you encrypt a message with your private key, the recipient of the message can decrypt it with your public key. Similarly, anyone can send anyone else an encrypted message, simply by encrypting the message with the recipient's public key; the sender doesn't need to know the recipient's private key. When you receive a message encrypted with your public key, you, and only you, can decrypt it with your private key. In addition to providing an encryption facility, some public key systems provide an authentication feature which ensures that when the recipient decrypts your

	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 Internet. They are extremely secure and relatively simple to use. One difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her. What's needed, therefore, is a global registry of public keys, which is one of the promises of the new LDAP technology.
Blowfish	A symmetric block cipher that was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms
CHAP	Challenge Handshake Authentication Protocol. A type of authentication protocol in which the authentication agent sends the client program a key to be used to encrypt the user name and password. CHAP doesn't only require the client to authenticate itself at startup time, but sends challenges at regular intervals to make sure the client hasn't been replaced by an intruder, for instance by switching phone lines
Denial of service	A denial-of-service attack (also, DoS attack) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.
DES	Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key. Although it was considered strong and there are over 72 quadrillion possible encryption keys that can be used, in 1997 the DES was cracked by a determined group of researchers and, independently in a cooperative effort on the Internet using over 14,000 computers. Since then many organizations use triple DES (3DES), which is essentially DES repeated three times but for material that has to be kept absolutely confidential, or kept confidential over the long term, DES is not the best choice. Look to its replacement, the Advanced Encryption System (AES) or one of its siblings. For many applications, however, including telecommunications and mobile radios, DES is enough.
DLCI	A data link connection identifier (DLCI) is a channel

	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
Private key	The portion of an encryption key pair that is kept secret by the owner of the key pair. Private keys sign or decrypt data.
Public key	The public portion of an encryption key pair.
RADIUS	RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.
RC5	RC5 [Riv95] is a fast block cipher designed by Ronald Rivest for RSA Data Security (now RSA Security) in

	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 monitors and controls network devices, and manages configurations, statistics collection, performance and security.
Source code	The form in which a computer program is originally written, usually in a language which other programmers can understand. In order to actually run, the source code is changed by the computer's compiler into an internal language which is much harder for humans (but easier for the computer) to understand.
Source routing	Source Routing is a technique whereby the sender of a packet can specify the route that a packet should take through the network.
SSH	Sometimes known as Secure Socket Shell, SSH is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are

	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: Echo: Echoes back whatever you type through the telnet x.x.x.x echo command. Chargen: Generates a stream of ASCII data Use the telnet x.x.x.x chargen command. Discard: Throws away whatever you type. Use the

	telnet x.x.x.x discard command. 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 the user. It 'sleeps' until something comes along which needs its help; most commonly found on Unix systems. The wrapper sits between the inbound connection and daemon on the system which controls access to the system. The wrapper reads the incoming traffic and originating site and compares the IP address to an access list which the Security Administrator configures. The access list contains sites which are authorized or not authorized to connect to the system. The wrapper records the time, date, and originating IP address of the inbound connection before it allows access to the system.
Trojan horse	A program that appears legitimate, but performs some illicit activity when run. It may be used to locate password information, to make the system more vulnerable to future entry, or to simply destroy programs and/or data on the hard disk. A Trojan horse is similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from a remote site to take control of the computer. Trojans often sneak in attached to a free game or other utility.
Trust relationships	A logical connection that is established between directory domains so that the rights and privileges of users and devices in one domain is shared with the other. For example, it allows users to log on once and have access to all associated resources without having to be authenticated again.
UDP small services	UDP small services consists of the following three router commands: Echo: Echoes the payload of the datagram you send. Discard: Silently pitches the datagram you send. Chargen: Pitches the datagram you send, and responds with a 72-character string of ASCII

	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