Receivership Data Privacy and Security Procedures
For Life and Health Insurers in Liquidation

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 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. A third party that is granted access privileges shall submit a written acknowledgement that it has in place and is bound by security procedures that are adequate to protect sensitive information and shall provide a copy of such procedures to the Organization upon its request.

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, which may include sharing such information with affected guaranty associations and their representatives in connection with the 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.

- 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

As recommended by the Receivership Technol

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.

- 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 being 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+,

- 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

As recommended by the Receivership Technol 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 em

hfiT[d[ize( )e9 or cJ0.00s

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 the execution of a written acknowledgement that the user is bound by security procedures that are adequate to protect sensitive information and the submission of such procedures to the Organization upon its request. Such persons who fail or refuse to comply with policies and/or procedures submitted or represented to the [*Organization*] 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

	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 spoobhost.yivi p5r lea4p((spoobhost.y0.00s0.0002 T

geo T*8(puters, T*-5edr sec hal

Pinged floods

The act of using the ping utility or command to continuously ping a machine causing network traffic congestion.

	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 prot

	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