



Information Security Policy Table of Contents

1. Introduction
2. Purpose
3. Scope of Policy
 1. Definition of Security
 2. Domains of Security
4. Security Roles & Responsibilities
 1. Policy Management
 2. Policy Implementation
 3. Security Custodians
 4. Individuals
 5. Company Services
5. Acceptable Use
 1. Overview
 2. General Use & Ownership
 3. Security and Proprietary Information
 4. Unacceptable Use
 - A. System and Network Activities
 - B. Email and Communications Activities
6. Passwords
 1. Overview
 2. General
 3. Guidelines
 - A. General Password Construction Guidelines
 - B. Password Protection Standards
 - C. Application Development Standards

**D. Use of Passwords and Passphrases for Remote
Access Users**

E. Passphrases

7. Virus Control

- 1. Overview**
- 2. General**
- 3. Accountability**
- 4. Installation Requirements**
- 5. Justification and Rationale**
- 6. Established Antiviral Procedures**

8. Intrusion Detection

- 1. Overview**
- 2. General**

9. Security Awareness and Training

- 1. Overview**
- 2. General**

10. Policy Review and Update

11. Security Policy Compliance and Enforcement

12. Revision History

1. Introduction

As a Christian technology and Information Security organization, Jesus Phreaks, Inc. bears an obligation to ensure appropriate security for all data, equipment, and processes in its domain of ownership and control. Since Jesus Phreaks is an employee-owned company, this obligation is shared, to varying degrees, by every member of the Company. The principles of free speech apply to this policy, and this policy is not intended to limit or restrict those principles.

These policies apply to all personnel within the Company. Each department will adapt this policy to meet their Information Security needs. The policy is written to incorporate current technological advances.

This document will:

1. Enumerate the elements that constitute Information Security (INFOSEC).
2. Explain the need for INFOSEC.
3. Specify the various categories of data, equipment, and processes subject to this policy.
4. Indicate, in broad terms, the INFOSEC responsibilities of the various roles in which each member of Jesus Phreaks, Inc. may function.
5. Indicate appropriate levels of security through standards and guidelines.

2. Purpose.

Confidentiality of information is mandated by common law, formal statute, explicit agreement, or convention. Different classes of information warrant different degrees of confidentiality.

The hardware and software components that constitute the Company's IT assets represent a sizable monetary investment that must be protected. The same is true for the information stored in its IT systems.

The use of Company IT assets in other than in a manner and for the purpose for which they were intended represents a misallocation of

valuable resources, and possibly a danger to its reputation or a violation of the law.

Finally, proper functionality of IT systems is required for the efficient operation of the Company. Some systems, such as the HR, Finance, Client Records, and Security systems are of paramount importance to the mission of Jesus Phreaks, Inc. Other systems (e.g. someone's PC) are of slightly less importance.

3. Scope of Policy.

1. Definition of Security.

Security can be defined as "the state of being free from unacceptable risk". The risk concerns the following categories of losses:

- Confidentiality of Information.
- Integrity of data.
- Assets.
- Efficient and Appropriate Use.
- System Availability.

Confidentiality refers to the privacy of personal or corporate information.

Integrity refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disc fails, or subtle, as when a character in a file is altered.

The *assets* that must be protected include:

- Computer and Peripheral Equipment.
- Communications Equipment.
- Computing and Communications Premises.
- Communications utilities.
- Supplies and Data Storage Media.
- System Computer Programs and Documentation.
- Application Computer Programs and Documentation.

Efficient and Appropriate Use ensures that Company resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.

Availability is concerned with the full functionality of a system (e.g. finance or payroll) and its components.

The potential causes of these losses are termed "threats". These threats may be human or non-human, natural, accidental, or deliberate.

2. Domains of Security.

This policy will deal with the following domains of security:

- Computer system security: CPU, Peripherals, OS. This includes data security.
- Physical security: The premises occupied by Company personnel and equipment.
- Operational security (OPSEC): Environment control, power equipment, and operation activities.
- Procedural security by IT, vendor, management personnel, as well as ordinary users.
- Communications security (COMSEC): Communications equipment, personnel, transmission paths, and adjacent areas.

4. Security Roles & Responsibilities.

1. Policy Management.

Approval of the Information Security Policy is vested with the Chief Information Officer (CIO), the Executive Technology Committee and the President of Jesus Phreaks, Inc.

Formulation and maintenance of the policy is the responsibility of the CIO.

2. Policy Implementation.

- Each member of the Company will be responsible for meeting published IT standards of behavior.

- The security of each system will be the responsibility of its custodian.

3. Security Custodians.

- IT will be the security custodian of all strategic system platforms.
- IT will be the security custodian of the strategic communications systems.
- IT will be the security custodian of all central computing facilities (e.g., server rooms, computer labs).
- Offices and departments will be the security custodian of strategic applications under their management control (e.g. Finance, HR).
- Individuals will be the security custodians of desktop systems under their control.

4. Individuals.

All ordinary users of Company IT resources:

1. Will operate within the guidelines set forth within the Technology Manual.
2. Are responsible for the proper care and use of IT resources under their direct control.

5. Company Services.

It is recognized that various departments of the Company provide services that relate to IT security, both directly and indirectly. It is expected that there will be collaboration between these departments and IT in generation of standards and implementation of the policy. Some of these departments and their services are:

- Human Resources: Personnel selection, induction, and exit processing.
- Campus Security: Physical security of the Jesus Phreaks Corporate Campus.

5. Acceptable Use.

1. Overview

Our intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Jesus Phreaks, Inc.'s established culture of openness, trust and integrity. We are committed to protecting Jesus Phreaks, Inc.'s members and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Jesus Phreaks, Inc. These systems are to be used for business purposes in serving the interests of the Company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Jesus Phreaks, Inc. member and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. General Use and Ownership

1. While Jesus Phreaks, Inc.'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Jesus Phreaks, Inc.

Because of the need to protect Jesus Phreaks, Inc.'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to Jesus Phreaks, Inc.

2. Members are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, members should be guided by departmental policies on personal use, and if there

is any uncertainty, members should consult their supervisor or manager.

3. We recommend that any information that users consider sensitive or vulnerable be encrypted.

4. For security and network maintenance purposes, authorized individuals within Jesus Phreaks, Inc. may monitor equipment, systems and network traffic at any time, per Audit Policy.

5. Jesus Phreaks, Inc. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3. Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: Company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Members should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed monthly, user-level passwords should be changed every 90 days.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.

4. Use encryption of information in compliance with Acceptable Encryption Use policy.

5. Because information contained on portable computers is especially vulnerable, special care should be exercised.

6. Postings by members from a Jesus Phreaks, Inc. email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Jesus Phreaks, Inc., unless posting is in the course of business duties.

7. All hosts used by the member that are connected to the Jesus Phreaks, Inc. Internet/Intranet/Extranet, whether owned by the member or Jesus Phreaks, Inc., shall be continually executing approved virus-scanning software with a current virus database.

8. Members must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Unacceptable Use

The following activities are, in general, prohibited. Members may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a member of Jesus Phreaks, Inc. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Jesus Phreaks, Inc.-owned resources.

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

A. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or Company protected by 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 Jesus Phreaks, Inc.

2. 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 Jesus Phreaks, Inc. or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. 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 at home.
6. Using a Jesus Phreaks, Inc. computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Jesus Phreaks, Inc. account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the member is not an intended recipient or logging into a server or account that the member 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.

10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.

11. Executing any form of network monitoring which will intercept data not intended for the member's host, unless this activity is a part of the member's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user other than the member's host (for example, denial of service attack).

14. 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.

B. Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within Jesus Phreaks, Inc.'s networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Jesus Phreaks, Inc. or connected via Jesus Phreaks, Inc.'s network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

6. Passwords.

1. Overview

Passwords are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Jesus Phreaks, Inc.'s entire corporate network. As such, all Jesus Phreaks, Inc. members (including contractors and vendors with access to Jesus Phreaks, Inc. systems) are responsible for taking the appropriate steps to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Jesus Phreaks, Inc. facility, has access to the Jesus Phreaks, Inc. network, or stores any non-public Jesus Phreaks, Inc. information.

2. General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.
- All production system-level passwords must be part of the IT administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

- All passwords must conform to the guidelines described below.

3. Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Jesus Phreaks, Inc.. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. All members should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "Jesus Phreaks, Inc.", "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#\$%^&*()_+|-=\`{}[]:;'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should *never* be written down or stored on-line in an unencrypted form.

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r" or some other variation.

NOTE: Do *not* use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for Jesus Phreaks, Inc. accounts as for other non-Jesus Phreaks, Inc. access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Jesus Phreaks, Inc. access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Jesus Phreaks, Inc. passwords with anyone, including administrative assistants or secretaries. No legitimate members of Jesus Phreaks, Inc. will *ever* ask you for your password.

All passwords are to be treated as sensitive, Confidential Jesus Phreaks, Inc. information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Outlook, Firefox).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including PDAs, cell phones or similar devices) without encryption.

Change passwords at least once every 90 days (except system-level passwords which must be changed monthly).

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates.

If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the Jesus Phreaks, Inc. Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a

mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

7. Virus Control

1. Overview

The purpose of this policy is to prevent infection of Jesus Phreaks, Inc. computers and networks by computer viruses and other malicious code. This policy is intended to prevent major and widespread damage to Company assets such as the network, user applications, files, and hardware.

The scope of this policy includes all personnel who use or are responsible for any computer system that resides at any Jesus Phreaks, Inc. facility, accesses the Jesus Phreaks, Inc. network, or stores any non-public Jesus Phreaks, Inc. information.

2. General

All Windows and Macintosh computers (clients and servers) connected physically or remotely to the Jesus Phreaks, Inc. network shall have antivirus software correctly installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network. If deemed necessary to prevent viral propagation to other networked devices or harmful effects to the network, computers infected with viruses, worms or other forms of malicious code (collectively referred to as

"virus" or "viruses") shall be disconnected from the network until the infection has been removed.

If feasible, all departmental servers providing email services shall direct all inbound email through the campus WebShields. This is done by creating a Mail Exchange (MX) record in the campus primary DNS. Once email is scanned, the WebShields will relay the email to the respective email server for delivery.

3. Accountability

Departmental Directors are responsible for monitoring compliance with this policy and associated standards by:

- Directing administrators of computers in their respective departments to install site-licensed or comparable anti-virus software on Company-owned desktops, laptops and servers.
- Directing reviews of, and action on, reports on compliance with this policy that are generated by Company InfoSec Services.
- Individual users (members, vendors and contractors) are responsible for compliance with this policy and its associated standards for departmental and personally owned machines (including laptops/notebooks) connected to the Jesus Phreaks, Inc. network.

4. Installation Requirements

If a computer does not have antivirus software installed, it shall be installed according to one of the two following methods:

- If the installation source is a Company-distributed CD-ROM, the antivirus software shall be installed before establishing any connection to the network. Upon establishing the initial network connection, the virus definitions shall be updated to the most current version immediately and before loading or installing any other software or data.
- If the installation source is a Company server, the computer shall be connected to the network for the sole purpose of installing antivirus software from that server. The installation shall be performed immediately

upon establishing the initial network connection and virus updates downloaded and installed before loading or installing any other software or data.

Under all other circumstances, any computers connected to the network shall have antivirus software properly installed, configured, and updated before being connected to the network.

At a minimum:

- Virus definitions shall be updated daily
- All files on all hard drives shall be scanned daily at a time convenient for the user.

When an enterprise-wide virus attack is in progress, IT Security shall notify the Company computing community via the best available method, and all files on all hard drives should be scanned immediately using the newest virus definitions available.

All operating systems shall have comparable protection, if available. In the event that no antivirus protection is available for a particular operating system or platform, anyone using or accessing these unprotected systems shall apply all prudent security practices to prevent infection, including the application of all security patches as soon as they become available. When antivirus software becomes available for an operating system or platform previously lacking antivirus software, it shall be installed on all applicable devices connected to the network.

The InfoSec Services department must explicitly approve any exceptions to this policy and respective workarounds.

5. Justification and Rationale

Availability, performance, and security of the network represent essential core assets to the daily operation of the Company. Viruses and other forms of malicious code (worms, Trojans, backdoors, VBS scripts, mass-mailers, etc.), represent a significant threat to these assets. In order to combat this threat, a comprehensive enterprise security policy must include antivirus provisions to detect, remove, and protect against viral infections.

Many virus infections threaten other computers sharing the infected computer's network. Files that can be cleaned should have the viral code removed -- returning them to pre-infected state. Files that cannot be cleaned must be quarantined until such time as they can be replaced with uninfected copies. If all efforts at removing viral infection fail, the computer's hard drive must be formatted and all software reinstalled using clean licensed copies. If an infected computer is deemed capable of infecting or affecting other computers or the network, the infected computer must be disconnected from the network until it is serviced by a IT representative or designee who will verify that the computer is virus-free.

Ideally, antivirus activities should be centrally managed. New viruses represent a continual threat, requiring continual research to plan proactive measures against them. Users must be educated about viral threats and best practices required to protect against infection. Whenever a new viral threat appears, the user community must be warned about the new threat. Up-to-date antivirus software must be distributed and its availability advertised to the Company computing community.

6. Established Antiviral Procedures

Jesus Phreaks, Inc. has taken a multi-tiered approach to address computer viruses. For the approved email servers on campus, all inbound email is scanned by a series of WebShield E500 network appliances. For the desktop and servers, the Company has a site license for McAfee VirusScan Enterprise. The site license permits UML faculty, staff, and students to have VirusScan on all Windows and Macintosh computers on the Company campus.

8. Intrusion Detection

1. Overview

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the

systems and network are secure. Intrusion detection systems can provide part of that assurance.

Intrusion detection provides two important functions in protecting information resources:

- Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

The scope of this policy includes all personnel who use or are responsible for any computer system that resides at any Jesus Phreaks, Inc. facility, accesses the Jesus Phreaks, Inc. network, or stores any non-public Jesus Phreaks, Inc. information.

2. General

Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.

Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.

Audit logging of any firewalls and other network perimeter access control system must be enabled.

Audit logs from the perimeter access control systems must be monitored/reviewed daily by the system administrator.

System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.

Audit logs for servers and hosts on the internal, protected, network must be reviewed on a weekly basis. The system administrator will furnish any audit logs as requested by the InfoSec Service department.

Host-based intrusion tools will be checked and documented on a routine.

All trouble reports should be reviewed for symptoms that might indicate intrusive activity.

All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the Incident Management Policy.

Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the Company Help Desk.

9. Security Awareness & Training

1. Overview

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

The purpose of the Security Training Policy is to describe the requirements for ensure each user at Jesus Phreaks, Inc. receives adequate training on computer security issues.

The scope of this policy includes all personnel who use or are responsible for any computer system that resides at any Jesus Phreaks, Inc. facility, accesses the Jesus Phreaks, Inc. network, or stores any non-public Jesus Phreaks, Inc. information.

2. General

All new users must attend an approved Security Awareness training class prior to, or at least within 30 days of, being granted access to any Company information resources.

All users must sign an acknowledgement stating they have read and understand Company requirements regarding computer security policies and procedures.

All users (members, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect Company information resources.

IT must prepare, maintain, and distribute one or more information security manuals that concisely describe Jesus Phreaks, Inc. information security policies and procedures. All users must attend an annual computer security compliance seminar and pass the associated examination.

IT must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

10. Policy Review and Update

This policy shall be reviewed on an annual basis by a committee consisting of a representative of the CEO, the CIO, the Director of Information Security, the Director of HR and a member chosen from the user community.

Policy updates will be made as warranted by advances in technology and circumstances.

11. Security Policy Compliance and Enforcement

Any member found to have violated this policy will be subject to disciplinary action, up to and including termination of employment and prosecution.

12. Revision History

Version 1 – 8 December, 2005