Policy Title	**IT Security Policy**
Author	Lai Kwok Chin MBA,
Owner	Dr Mohd Effendy, Executive Director
Endorsed by	IT Committee and Commissioner Council
Adopted by	Scout Council on 14 Feb 2015
Version	1.0
Effective Date	Mar 2015
Last Update	

Objectives:

The objectives of the Information Technology Security Policy are the preservation of confidentiality, integrity, and availability of systems and information used by members and staff of the Singapore Scout Association (SSA).

Confidentiality involves the protection of assets from unauthorized entities, integrity ensures the modification of assets is handled in a specified and authorized manner, and availability being a state of the system in which authorized users have continuous access to said assets.

The IT Security Policy is a collection of the following policies:

A. Acceptable Use Policy

1. Overview:

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the SSA's established culture of openness, trust and integrity.

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 the SSA. These systems are to be used for purposes in serving the interests of the SSA, and of our members and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every SSA's member and employee 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. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the SSA. These rules are in place to protect the SSA, its members and employees. Inappropriate use exposes the SSA to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct the SSA's business or interact with internal networks and business systems, whether owned or leased by the SSA, the member, employee, or a third party. All members, employees, contractors, consultants, temporary, and other workers of the SSA are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the SSA's policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to members, employees, contractors, consultants, temporaries, and other workers of the SSA, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the SSA.

4. Policy

4.1 General Use and Ownership

4.1.1 The SSA's proprietary information stored on electronic and computing devices whether owned or leased by the SSA, its member, employee, or a third party, remains the sole property of the SSA.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of the SSA's proprietary information.

4.1.3 You may access, use or share the SSA's proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Members and employees are responsible for exercising good judgment regarding the reasonableness of personal use, and if there is any uncertainty, members and employees should direct their queries to the Executive Director.

4.1.5 For security and network maintenance purposes, authorized individuals within the SSA may monitor equipment, systems and network traffic at any time.

4.1.6 The SSA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.2 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.3 Postings by employees from a SSA's email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the SSA, unless posting is in the course of business duties.

4.2.4 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Members and employees 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 or an employee of the SSA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the SSA owned resources.

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

4.3.1 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 the SSA.

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 the SSA or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting the SSA's business, even if you have authorized access, is prohibited.

4. 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.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. 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.

7. Using a SSA's computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any of the SSA's account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the member or employee is not an intended recipient or logging into a server or account that the member or 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.

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

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

13. 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.

14. Providing information about, or lists of, the SSA's members and employees to parties outside the SSA.

4.3.2 Email and Communication Activities

When using the SSA IT resources to access and use the Internet, users must realize they represent the SSA. Whenever members or employees state an affiliation to the SSA, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Singapore Scout Association". Questions may be addressed to the Executive Director.

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.

4.3.3 Blogging and Social Media

1. Blogging by members and employees, whether using the SSA's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Blogging has to be done in a professional and responsible manner; it does not otherwise violate the SSA's policy, and is not detrimental to the SSA's best interests. Blogging from the SSA's systems is also subject to monitoring.

2. Members and employees are prohibited from revealing any of the SSA's confidential or proprietary information when engaged in blogging or the use of social media.

3. Members and employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the SSA and/or any of its members and employees. Members and employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

4. Members and employees may also not attribute personal statements, opinions or beliefs to the SSA when engaged in blogging. If a member or an employee is expressing his or her beliefs and/or opinions in blogs, the member or employee may not, expressly or implicitly, represent himself or herself as a member, an employee or representative of the SSA.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the SSA's trademarks, logos and any other of the SSA's intellectual property may also not be used in connection with any blogging activity

5. Compliance

5.1 Compliance Measurement

The IT Manager will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Executive Director.

5.2 Exceptions

The Executive Director must approve any exception to the policy in advance.

5.3 Non-Compliance

A member or an employee found to have violated this policy might be subjected to disciplinary action, up to and including termination of membership or employment.

B. Email Policy

1. Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

2. Purpose

The purpose of this email policy is to ensure the proper use of the SSA's email system and make users aware of what the SSA deems as acceptable and unacceptable use of its email system. This policy outlines the requirements for use of email within the SSA network.

3. Scope

This policy covers appropriate use of any email sent from a SSA email address and applies to all members, employees, vendors, and agents operating on behalf of the SSA.

4. Policy

4.1 All use of email must be consistent with the SSA's policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

4.2 The SSA email account should be used primarily for the SSA business-related purposes; personal communication is permitted on a limited basis, but non-SSA related commercial uses are prohibited.

4.3 Email should be retained only if it qualifies as a SSA business record. Email is a SSA business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

4.4 The SSA email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Members or employees who receive any emails with this content from any SSA's member or employee should report the matter to the Executive Director immediately.

4.5 Users are prohibited from automatically forwarding SSA email to a third party email system. Individual messages that are forwarded by the user must not contain the SSA confidential information.

4.6 Using a reasonable amount of the SSA resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a SSA email account is prohibited.

4.7 Members or employees of the SSA shall have no expectation of privacy in anything they store, send or receive on the SSA's email system.

4.8 The SSA may monitor messages without prior notice. The SSA is not obliged to monitor email messages.

5. Compliance

5.1 Compliance Measurement

The IT Manager will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the Executive Director.

5.2 Exceptions

The Executive Director must approve any exception to the policy in advance.

5.3 Non-Compliance

A member or an employee found to have violated this policy might be subjected to disciplinary action, up to and including termination of membership or employment.

C. Internet Usage Policy

1. Overview

Internet connectivity presents the SSA with new risks that must be addressed to safeguard the association's vital information assets. These risks include:

Access to the Internet by employees that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the SSA may face loss of reputation and possible legal action through other types of misuse.

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

2. Purpose

The purpose of this policy is to define the appropriate uses of the Internet by the SSA's members and employees.

3. Scope

The Internet usage Policy applies to all Internet users (members, employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The SSA's Internet users are expected to be familiar with and to comply with this policy, and are also required to exercise their good judgment while using Internet services.

Capabilities for the following standard Internet services will be provided to users as needed:

- E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).

- Web browsing -- WWW services using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet.

The SSA reserves the right to add or delete services, as needs change or conditions warrant. All other services will be considered unauthorized access to/from the Internet and will not be allowed.

4. Policy

4.1 Prohibited Usage

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited. The SSA also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

- Accessing the SSA's information that is not within the scope of one's roles and responsibilities. This includes unauthorized reading of member account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.

- Misusing, disclosing without proper authorization, or altering member or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic member or personnel data with unauthorized personnel.

- Deliberate pointing or hyper-linking of the SSA Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the SSA.

- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law.

- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.

- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.

- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

- Any form of gambling.

Unless specifically authorized under the provisions of section 4.1, the following activities are also strictly prohibited:

- Unauthorized downloading of any shareware programs or files for use without authorization in advance from the Executive Director. Any ordering (shopping) of items or services on the Internet.
- Playing of any games.
- Forwarding of chain letters.
- Participation in any on-line contest or promotion.
- Acceptance of promotional gifts.

Bandwidth both within the SSA and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other users.

4.2 Software License

The SSA strongly supports strict adherence to software vendors' license agreements. When at work, or when the SSA computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the Executive Director for review.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

An employee using the SSA computer resources to access the Internet for personal purposes, without approval from the Executive Director, may be considered cause for disciplinary action up to and including termination.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk.

4.3 Expectation of Privacy

4.3.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.

The SSA reserves the right to examine E-mail, personal file directories, web access, and other information stored on the SSA owned or leased computers, at any time and without notice. This examination ensures

compliance with internal policies and assists with the management of the SSA's information systems.

4.3.2 Email Confidentiality

Users should be aware that clear text email is not a confidential means of communication. The SSA cannot guarantee that electronic communications will be private. Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once email is transmitted it might be altered. Deleting an email from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

4.4 Maintaining Corporate Image

4.4.1 Representation

When using the SSA resources to access and use the Internet, users must realize they represent the SSA. Whenever members or employees state an affiliation to the SSA, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Singapore Scout Association". Questions may be addressed to the Executive Director.

4.4.2 SSA Materials

Users must not place the SSA material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the Executive Director and will be placed by an authorized individual.

4.4.3 Creating Web Sites

All users wishing to establish a WWW home page or site must first develop business, implementation, and maintenance plans. Formal authorization must be obtained through the IT Manager. This will maintain publishing and content standards needed to ensure consistency and appropriateness.

In addition, contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted to the Executive Director for approval to continue.

All of the SSA pages are owned by, and are the ultimate responsibility of, the Executive Director. These web sites must be protected from unwanted intrusion through formal security measures.

5. Compliance

5.1 Compliance Measurement

The IT Manager will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

The Executive Director must approve any exception to the policy in advance.

5.3 Non-Compliance

A member or an employee found to have violated this policy might be subjected to disciplinary action, up to and including termination of membership or employment.

Additionally, the SSA may at its discretion seek legal remedies for damages incurred as a result of any violation. The SSA may also be required by law to report certain illegal activities to the proper enforcement agencies.

D. Password Protection Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of The SSA's resources. All users, including members, employees, contractors and vendors with access to the SSA systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

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.

3. Scope

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 the SSA premises, has access to the SSA's network, or stores any non-public SSA information.

4. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

4.1.2 Users must not use the same password for the SSA accounts as for other non-SSA access (for example, personal ISP account, option trading, benefits, and so on).

4.1.3 Where possible, users must not use the same password for various SSA access needs.

4.1.4 User accounts that have system-level privileges must have a unique password from all other accounts held by that user.

4.2 Password Change

4.2.1 All system-level passwords must be changed on at least a quarterly basis.

4.2.2 All user-level passwords must be changed at least every six months.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential SSA information.

4.3.2 Passwords must not be inserted into email messages or other forms of electronic communication.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not write passwords down or store them in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.3.6 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.7 Any user suspecting that his/her password may have been compromised must report the incident to the IT Manager and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must 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.

5. Password Construction Guidelines

All passwords should meet or exceed the following guidelines:

Strong passwords have the following characteristics:

- Contain at least eight alphanumeric characters.

- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

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

6. Compliance

6.1 Compliance Measurement

The IT Manager will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

6.2 Exceptions

The Executive Director must approve any exception to the policy in advance.

6.3 Non-Compliance

A member or an employee found to have violated this policy might be subjected to disciplinary action, up to and including termination of membership or employment.

E. Software Installation Policy

1. Overview

Allowing members and employees to install software on the SSA's computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when unauthorized software are installed on the SSA's computing equipment.

2. Purpose

The purpose of this policy is to outline the requirements around installation software on the SSA's computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within the SSA's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

3. Scope

This policy applies to SSA members, employees, contractors, vendors and agents with SSA-owned computing devices. This policy covers all computers, servers, smartphones, tablets and other computing devices owned and leased by the SSA.

4. Policy

- Employees may not install software on the SSA's computing devices operated within the SSA's network.
- The Executive Director must first approve software requests in writing or via email.
- The IT Manager will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

5. Compliance

5.1 Compliance Measurement

The IT Manager will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

The Executive Director must approve any exception to the policy in advance.

5.3 Non-Compliance

A member or an employee found to have violated this policy might be subjected to disciplinary action, up to and including termination of membership or employment.

F. Technology Equipment Disposal Policy

1. Overview

Technology equipment often contains parts that cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of the SSA data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

2. Purpose

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by the SSA.

3. Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within the SSA including, but not limited to the following: personal computers, servers, hard drives, laptops, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All the SSA's members, employees and affiliates must comply with this policy.

4. Policy

4.1 Technology Equipment Disposal

4.1.1 When Technology assets have reached the end of their useful life they should be sent to the IT Manager for proper disposal.

4.1.2 The IT Manager will securely erase all storage mediums in accordance with current industry best practices.

4.1.3 All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks.

4.1.4 No computer or technology equipment may be sold to any individual other than through the processes identified in this policy (Section 4.2 below).

4.1.5 No computer equipment should be disposed of via skips, dumps, landfill etc.

4.1.6 All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

4.1.7 Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

4.1.8 Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

4.2 Employee Purchase of Disposed Equipment

4.2.1 Equipment that is working, but reached the end of its useful life to the SSA, will be made available for purchase by employees.

4.2.2 Finance will determine an appropriate cost for each item.

4.2.3 All purchases are final. No warranty or support will be provided with any equipment sold.

4.2.4 Prior to leaving the SSA premises, all equipment must be removed from the IT inventory.

5. Compliance

5.1 Compliance Measurement

The IT Manager will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

The Executive Director must approve any exception to the policy in advance.

5.3 Non-Compliance

A member or an employee found to have violated this policy might be subjected to disciplinary action, up to and including termination of membership or employment.