Computer Access and Usage Policy

The Salvation Army values excellence, cooperation, and integrity in the accomplishment of its mission. As part of accomplishing its mission, the Canada and Bermuda Territory has invested heavily in computer technology. That investment is intended to improve the efficiency and effectiveness of the employees, with the ultimate goal of better serving the spiritual and social needs of our clients and members.

The following policies have been established in order to help minimize the overall cost while maximizing the availability and security of the computing resources of the Territory. It should be readily apparent in the following why individual policies have been implemented, be it legal, security, or financial. The document is divided into two sections. The first section states the policies. The appendix provides rationales and information for each policy.

Note that the management of the organization requires access to data at any time even in an employee's absence. In addition, the IT Department must be able to assist in the recovery of lost or damaged data. In order for this to be possible, users cannot expect total privacy in the use of the organization's computer resources. Nevertheless, one should not and need not assume that an individual in the organizational will be intently, continuously monitoring the actions and communications within the organization.

Where possible, the policies consider the desires of the officers and employees while maintaining the overall intent of protecting the investment in technology and data. An example of this is in the area of e-mail where personal e-mail is allowed if it does not contain graphics since graphics have a negative impact by raising the cost of the network. It is expected that individuals will not abuse this type of privilege.

Table of contents:

APPENDIX

POLICIES

Following are the policies of the Canada & Bermuda Territory of the Salvation Army. An appendix is attached providing information and rationale for each of the policies.

1. Privacy

- **Salvation Army management reserves the right at any time and without prior notice, to examine e-mail, personal file directories, and other information stored on Salvation Army computers. This examination allows management access to information that may be informative to or part of its operations.**
- **Approved Systems Administrators may, in the normal execution of their job responsibilities, become privy to the content of computer data and e-mail files. This information will remain confidential as long as the data/information does not contravene municipal/provincial/federal laws or the Minutes/policies of the organization in which case the information will be brought to the attention of the individual's manager for further action.**
- **The Salvation Army will not tolerate any illegal activity on its computers. Management will take appropriate actions in situations where an illegal activity is discovered.**

2. Internet Browsing

- **Personal browsing of the Internet on Army owned equipment or using the Army's computer network is not allowed.**
- **Use of Army owned equipment and/or network resources for the following is not allowed:**
    - **Use of "Hotmail" or other personal e-mail sites except as approved by the IT Department for locations without Lotus Notes.**
    - **Access to radio stations on the Internet.**
    - **Receiving personal Internet site updates.**
- **Use of Army owned equipment or using the Army's computer network at any time to visit pornographic web sites is not allowed. Accessing or attempting to access pornographic Internet sites is just cause for termination of employment or appointment.**
    - **A check of computers is possible (and will be done) to identify if the computer has been used to visit pornographic web sites.**
    - **The Internet filter used by The Salvation Army allows the organization to monitor usage and identify users attempting to reach blocked Internet sites such as sites identified as pornographic.**
    - **Individuals accessing or attempting to access pornographic Internet sites will be reported by the Personnel Department to the individuals Department Head or Divisional Commander who will then interview the individual, discuss the access or attempted access, and take appropriate disciplinary action.**

3. Legal - Software Copyrights

- **A license must be acquired for each copy of software products. The license and media (i.e. CD, diskette, etc) must be held in a secure location and cannot be loaned or used on multiple computers unless explicitly allowed in the license agreement.**
- **When unlicensed software is found, the IT or Audit Department will immediately notify the user and the associated manager and purchase a license for the software. The location will be billed for the license. A copy of the license must be sent to the IT or Audit Department as follow up.**
    - **Note that simply removing the software is not sufficient. The Army must be covered for the use (past or present) of the software.**
    - **Where use of the software is deemed to have been personal, the cost of the software must be paid by the employee.**
    - **If the software was a trial version and was programmed to disallow usage once the trial period was ended, the software can be removed without buying a license.**
- **If unlicensed software is found on a computer owned or leased by The Salvation Army, it will be considered a breach of this policy and is just cause for termination of employment or appointment of the user.**

4. Security - Passwords

- **The system is set to automatically expire user passwords after 90 days of usage or less.**
- **Under no circumstances will sharing of passwords be condoned. Deviation will result in immediate cancellation of both users' accounts by the IT Department. The IT Department will re-instate the users' accounts only upon formal request by the users' Cabinet Member or Divisional Commander.**
- **Passwords must be made up of a combination of letters and numbers/symbols.**

5. Security - Unattended Computers

- **When leaving a computer unattended, users must take reasonable precautions to prevent unauthorized access to information. This may include:**
    - **Logging off the network;**
    - **Shutting down the computer;**
    - **Using a password-protected Microsoft Windows screen saver;**
    - **Locking the workstation (Windows 2000 feature); and/or**
    - **Locking the office door.**

6. Security – Internet Connections

- **All computers and networks with a connection to the Internet must be protected with a firewall.**
- **All computers (regardless of whether they are connected to the Internet or not) must have an Anti-virus program actively running at all times.**
  - **The virus definitions must be updated on a regular basis (preferable at least weekly) with the definitions from the company that developed the anti-virus software.**

7. Security - Confidentiality in E-Mails

- **All e-mail containing sensitive or confidential information should be encrypted if it is addressed to someone in the Salvation Army that is using Lotus Notes.**
- **Sensitive or confidential information should not be e-mailed outside the organization.**

8. Security - Scanned Signatures

- **Scanned signatures on electronic documents (e-mail or attachments to e-mail) are strictly forbidden.**
- **Scanned signatures for use on hard copy documents are strongly discouraged because of the risk to both the organization and the author.**
  - **Where a scanned signature is considered necessary for use on hard copy documents, pre-approval from the author and the associated Cabinet member or Divisional Commander is required.**
  - **Scanning a signature or using a scanned signature without the consent of the author is just cause for termination of employment or appointment.**
  - **The author is responsible for ensuring that their scanned signature is kept in a secure location and that it is only provided to individuals on an as required basis.**
  - **The Salvation Army will hold individuals accountable for misuse of scanned signatures.**
- **Where a scanned signature for cheque signing is used, an electronic signing machine with dual user password protection must be used.**
  - **Note that the purchase of an electronic signing machine should go through a full cost benefit analysis to ensure the expenditure is justified.**

9. Cost Reduction - Unapproved Software

- **Any location wishing to use software that is not expressly listed in the Official Minutes must receive approval from the IT Department prior to obtaining the software.**

10. Cost Reduction – Personal e-mail and documents

- **Personal e-mail that is created and sent outside of regular hours of duty and that does not contain graphics, audio clips, or programs may be sent on Army owned computer equipment. Graphic and audio content are not allowed.**
- **Personal e-mail received containing graphic, audio, or program attachments must be deleted as soon as possible the same day they are received. Such e-mail may not be forwarded within or outside of the organization.**
- **E-mail trying to sell things or to announce sales/events must not be broadcasted, sent or forwarded on Army owned computer equipment. This activity will be limited to the electronic Bulletin Board.**

11. Cost Reduction – Games, Entertainment, and Personal Software

- **Loading of game, entertainment, and personal software on Army owned equipment is not allowed.**
  - **The exception to this policy is where there is an approved rationale for the computers to be installed for the express purpose of entertaining the users or providing special training.**
- **Forwarding of game, entertainment, and personal software to others within or outside of the organization using the Army's computer network is not allowed.**
- **Where games (other than those games provided by Microsoft with the Windows operating system on new computers) are found on Army owned equipment, an IT representative will delete the games and notify the employee's supervisor.**
- **Playing of network based computer games on Army owned computers is not allowed (except the one exception noted above and if the computers are not part of the corporate WAN).**

12. Cost Reduction - Portable Computers

- **Users using notebook, palmtop, and other transportable computers must not leave these computers unattended (eg. on a desk or in an unlocked desk outside of regular office hours, in an unlocked car, or unsupervised in airports, malls, etc).**
- **Users travelling with transportable computers must not check these computers in airline luggage systems, with hotel porters, etc. These computers must remain in the possession of the traveler as hand luggage. The computer must be stored out of sight if it is left unsupervised in a hotel room.**

13. Cost Reduction - Data Backup

- **Users will be responsible for ensuring that the data on their PC is properly backed up or has been copied to or stored on the network drives.**
- **Network Administrators are responsible for ensuring that a regular daily backup is done of all data and programs on the servers, and that copies of the backup media are stored in a secure, off-site location.**

14. Cost Reduction - Graphics

- **Graphics will be used sparingly at the discretion of individual departments/divisions and under the scrutiny of the IT Department. Where a seeming excess of space is being used by a user, an IT representative will communicate first with the user and/or manager. Failing resolution, communication will be made with the associated Divisional Commander or Department Head to ensure that the graphic content is being used in an official capacity and is beneficial.**
- **Graphics may not be added to e-mail as part of a heading or signature plate.**
    - **Lotus Notes stationery templates and mood stamps are not transmitted as part of the message and thus may be used.**

15. Cost Reduction – File Space Quota

- **Storage quotas will be set for network drives and mail files. Users requiring more than the quota may obtain additional space by having their manager provide a rationale to the Information Technology Department.**
- **Retention periods for various types of information, persons responsible for archiving documents, and methods of retention is covered in a separate Minute.**

16. Cost Reduction - Screen Savers, etc

- **Only screen savers within the standard Windows operating system may be used.**
- **Programs to alter the cursor or to add active graphics for entertainment (eg. Felix) must not be loaded or used on Army owned computer equipment.**
- **Personalized Windows "wallpaper" created from static bitmap images are not programs, and therefore do not conflict with computer resources. Therefore, their use is permitted.**

17. Virus Warnings and Computer Tips

- **All types of advisories regarding computer viruses should be sent to the Help Desk for testing and verification. If there is a cause for alarm, the IT Department will notify users as quickly as possible.**
    - **Note that the intent of a virus hoax is to disrupt the work flow within an organization rather than to destroy data.**
- **All employees are encouraged to look on the Lotus Notes Bulletin Board on a regular basis for tips and information regarding computer use.**

I certify that I have read and understood the Salvation Army's Computer Usage and Access Policy. I have received a copy of this Policy for future reference.

Officer's/Employee's/Contractor's /Volunteer's Signature

Name (Please print clearly)

Date

Appendix – Rational & Additional Information

1. Privacy

The Salvation Army owns or leases all computer systems that are used by it for the purposes of carrying out its Mission. Data stored on Salvation Army owned computers is the property of The Salvation Army. The Salvation Army reserves the right to monitor all aspects of its networks and computer systems including, but not limited to, Internet sites visited by employees, chat groups, material downloaded from and uploaded to the Internet, incoming and outgoing e-mail and file directories. As such, individual users should not have any reasonable expectation of privacy in the use of these resources.

The Salvation Army will not tolerate any illegal activity on its computers.

2. Internet Browsing

An increasing number of individuals within the organization are using the Internet as a regular part of performing their responsibilities. Personal use of this tool, both during the day and the evening is causing serious delays to those individuals using it for business purposes.

We regret that the cost associated with increasing the speed of the Internet connection to allow for personal browsing is prohibitive. Prohibiting personal browsing on Salvation Army computer resources is thus an act of stewardship and fiscal responsibility.

In addition, it has become apparent that some individuals are not using discretion in the web sites that they visit. Each time an individual visits a web site from one of the organization's computers, our corporate identity is transmitted as part of the actual connection to the site. Thus the Army's reputation is compromised. A check of computers is possible (and will be done) to identify if the computer has been used to visit pornographic web sites. Also, the Internet filter used by The Salvation Army allows the organization to monitor usage and identify users attempting to reach blocked Internet sites such as sites identified as pornographic.

3. Legal – Software Copyrights

Using software without having a proper license for the software is illegal and can result in the individual or the organization being sued. Beyond the cost, this would harm the reputation of the Army.

There is often a misunderstanding about "Shareware". The license with the software sets out the rules of the particular package.

- Some can be shared with no fee.
- Some have limited functionality but are free to use. In this instance, you would need to buy the full product to get full functionality.
- Some is free for a short trial period.

Software vendors normally provide you with an "evaluation copy" of their software for a short test period. This can be distributed under the term shareware. Use of the software beyond the trial period constitutes a violation of copyright law.

Another area of confusion is whether a duplicate copy of the software can be run on a home computer without a separate license. Previously, some vendors allowed for a user to have licensed software on a computer at work and to load the same software on a home computer using the same license. **This is no longer the case.** Now the general rule is that the second copy of the software can only be loaded on a notebook provided by the organization to the same employee to qualify for this exemption.

Note:

- Licenses for upgrade versions of software are not legal without the license from the original product. Both licenses must be retained.
- The license for the operating system must remain with the computer even when the hardware is transferred or sold.

Once software has been used, it is not sufficient to simply delete the illegally used software. The software must be purchased once it has been used (outside of a specific vendor approved evaluation period). The IT Department Help Desk is available to assist in obtaining licenses and deleting software.

Downloading and using copyright protected content (including music) without appropriate permission is also illegal.

4. Security - Passwords

Lotus Notes provides each user and in turn the organization with a secure platform on which to communicate and operate. Just as a hand written signature provides proof of authenticity and origin on a paper copy, Notes provides an identification that indicates that the sender of a document is who they claim to be.

This functionality is further enhanced by providing a user with the ability to have someone else work within their mail file and send responses on their behalf while still retaining that sender's identity. Just as in paper copy a person writes "for" or "on behalf of " before signing a document for someone else, Notes identifies the sender as well as the person for whom they are sending the document.

This security allows someone receiving the document to appropriately act on the advice or commands within the document. It thus provides the organization with a tool for performing business quicker and more effectively.

However, when a user circumvents this security by failing to keep their password private (intentionally or unintentionally), or leaving themselves logged onto the computer when they are away from their desk, the entire organization suffers because the tool can no longer be trusted.

Using another person's password and sending a document under that ID and password is performing an act similar to forging that person's signature. This has varying degrees of severity depending on the importance of the document or the policies the organization places on signing authorities. In any case, it breaks down the organization's ability to function effectively using electronic media.

The best password is a long one made up of a combination of letters, numbers, and symbols (in mixed case) because they are much more difficult to guess or hack. The worst passwords are those made up of words in the dictionary or names (especially your child's or spouse's name).

5. Security – Unattended Computers

Once a computer has been turned on at the office and logged into the network, anyone can use that computer to access all of the particular user's data. When you leave your computer logged on when you leave your desk, your data is not secure. Thus it is essential that users secure the computer when they leave. When the organization migrates to the Windows 2000 operating system, tools will be available to securely lock the workstation in addition to requiring all users to log on even when not connected to the network.

6. Security – Internet Connections

The Internet is a very insecure environment. Transmitted data is susceptible to interception (Item 4 below will provide more information on this). There are also two significant security issues related to connectivity to the Internet: protection from hackers and protection from viruses.

Hackers are individuals that attempt to access the information on your computer without your knowledge. Access itself can be the motivating factor. In other instances, destruction of or access to data are the motivating factor(s). Hackers can enter the computer/network either through an Internet connection or through a dial-up account on the computer/network.

Protection from hackers requires a "firewall" to be properly in place and to be carefully monitored. A "firewall" is software that forces individuals to log on to the computer with an ID and password. An ID and password are only given to individuals that you want to allow into the computer.

Viruses are programs that are written to perform some damage to the data/programs stored on the computer/network. They are transmitted within other programs across the Internet or on diskettes. Trojans are a form of virus.

There are hundreds of viruses. Protection from viruses requires using an anti-virus program. The anti-virus program identifies viruses using a table of definitions (provided by the anti-virus program vendor). Sometimes, anti-virus programs can remove the virus and fix the original program. It is much more effective to identify and remove the virus before it is activated.

7. Security – Confidentiality in E-Mails

Lotus Notes provides a secure communications platform. It provides strong security controls through the use of encryption technology and Access Control Lists that permit data access to authorized users only.

Access to Lotus Notes databases can be limited/controlled by Notes User ID or by Notes User Group. Thus reading and/or updating of databases can be controlled. The IT Department sets the limits as per the database owner's request.

Users have the ability to manually set encryption on e-mail (in the delivery options dialogue box), making it possible for only the sender and intended recipient of the message to view the contents. There are however several difficulties in the use of encryption such as successors being unable to read business related material. Thus where possible, encryption should not be used. However, if sensitive/confidential information needs to be e-mailed, then encryption should be used.

In addition to encrypting e-mail, there is also a "prevent copy" feature (in the delivery options dialogue box) to provide additional security. If this feature is used, the recipient will be unable to print or forward the message. The combination of encryption and prevent copy provides a very secure environment.

Note the following:

- Individuals with access to your mailbox cannot read mail that has been encrypted.
- If your mailbox is renamed for use by a successor, the successor will be able to read encrypted mail.
- You can only encrypt mail to a person outside of the organization if you have a copy of their Public Encryption Key.

E-mail being sent to individuals outside of the organization must go through the Internet and the Internet is not a secure environment in which to send information.

8. Security – Scanned Signatures

For reasons similar to those outlined under passwords, use of scanned signatures breaks down the authenticity of documents unless a secure process that can withstand the scrutiny of an audit surrounds the use of the scanned signature. This normally entails the use of an electronic signing machine with dual user password protection.

A scanned signature is retained on an electronic document as a simple graphic. Thus it can be copied and pasted elsewhere with a simple copy and paste function. This could lead to embarrassing or costly situations.

Note that where an external party has reason to believe that the signature is a true representation of an individual whom they know to hold an appropriate decision making position, that external party is justified in executing the request(s) that are covered in documents with the scanned signature. Thus The Salvation Army must honor commitments made in such documents. However, The Salvation Army can hold individuals responsible for inappropriately using the scanned signature.

A scanned signature can be useful in a mass production of a letter with colour. However, the actual scanned signature file must be kept very secure.

9. Cost Reduction – Unapproved Software

The IT Department takes great effort to ensure that application software on the approved list is compatible with the hardware, operating system and other applications in use within the organization. This effort is to minimize computer system failure and the associated negative impact on the organization.

When users indiscriminately load software that is not approved, frequently seemingly "unrelated" compatibility problems start to occur. Diagnosing the problem(s) is time consuming, more difficult, and frustrating for the user and the Help Desk staff.

10. Cost Reduction – Personal E-mail and Documents

The costs associated with sending an e-mail that does not contain graphics (scanned pictures, games, animated cartoons/games, etc) or audio clips is very low. Thus personal e-mails that do not contain graphics or audio clips and that are created and transmitted outside of regular business hours create a minimal cost to the organization. In situations where friends/relatives are far away and the individual does not have his/her own personal computer with Internet access, that small cost to the organization can be offset by the employee satisfaction.

Employees using the company equipment for e-mail, business or personal, should be aware that e-mail that cannot be delivered by the Internet is returned to the sender and to the "postmaster". In an organization, the postmaster is a mailbox monitored by IT Department staff to ensure proper mail distribution. The sender is identified in the e-mail so redirecting requires opening the e-mail. To add to this, the Internet itself is not a secure means of communicating extremely confidential information. Thus, caution should be used where extremely sensitive information is being sent via the Internet.

Personal broadcast e-mail that tries to sell things is disruptive and unprofessional. An electronic Bulletin Board has been built within Notes for both personal and business related items.

11. Cost Reduction – Games, Entertainment, and Personal Software

Games, entertainment, and personal software generally consume large amounts of computer and network resources and are thus quite costly. In addition, they cause computer and network problems, thus hampering the ability of others within the organization to effectively perform their job.

12. Cost Reduction - Portable Computers

Portable computers are valuable assets. They require safeguarding because of their value and the fact that they are very easily stolen. Loss through theft has a direct financial impact on the organization, both for the hardware and data.

13. Cost Reduction – Data Backup

To protect the Army's investment in data, users are responsible for backing up the information on their PC's. Users with PC's connected to the network can store their data on the server or place a duplicate of the information on the server. Data on servers must be backed up daily as part of the network management.

14. Cost Reduction - Graphics

The use of graphics is becoming increasingly common. Graphics can be an effective way of communicating a message but they are often used simply to decorate a page, making it pleasing to view but not enhancing the message or the readers ability to comprehend the message (the reason for the document in the first place).

Unfortunately, there is a significant cost that must be paid by the organization to support graphics. Graphics generally require a lot of disk space. This means that more disk space is required along with increased backup system capacity. When the document is transmitted in or as an attachment to an e-mail, additional network traffic is created requiring the organization to spend more money on network facilities.

The organization is also increasing the number of documents created and stored. There are a number of factors that make this an effective way of operating. However, there is an associated cost. Using the newer office products has caused document sizes to increase because of the increased functionality and user friendly features. When there are graphics in the document the cost is much higher. The disk space requirements are beginning to increase exponentially.

15. Cost Reduction – File Space Quota

The number of documents created and communicated within the organization on a daily basis has been steadily increasing. Computers, the network, and e-mail have revolutionized the way we work. It has not reduced our tendency to accumulate large numbers of documents, many of which are useless or are duplicated in one or more locations on the network.

16. Cost Reduction – Screen Savers, etc

Using password protection with a screen saver provides limited security when you leave your desk for a short period. Historically, screen savers were meant to continuously change the image on a screen so that the image would not become "burnt" into the actual face of the screen. With new technology, this is no longer required.

The difficulty with screen savers is when they utilize animation and audio. Animation and audio take up considerable disk space. The problem is compounded with some screen savers that actually use computer resources even when they are not active on the screen. This means that the computer is less efficient from an operating perspective.

Other problems occur when users load programs for changing the cursor or adding active graphics for entertainment (eg. Felix). The performance of the computer is often negatively affected and sometimes the computer will develop unusual problems that the Help Desk staff must spend time diagnosing and correcting. Many of these downloaded programs contain viruses.

17. Virus Warning and Computer Tips

Many virus warnings are hoaxes (despite their claim for legitimacy by including supposed quotes from knowledgeable organizations like IBM, Microsoft, or the police). They are intended to disrupt the regular flow of business by getting staff to forward the hoax to other staff members and friends. There is a write-up on this on the THQ Notice Board under IT Tips.

In addition there are a number of other helpful tips for common computer problems on the Notice Board.

Computer Access Policy Acknowledgement

(Please fax completed forms to (416) 422-6160.)

First/Common Name:		Division:	
Initial(s):		Ministry Unit:	
Family Name:		Position/Title:	
Rank:		Telephone:	

My signature below indicates that:

1. *I understand that the user identification and password that will be assigned to me is for my use only and will not be shared with any other individual;*
2. *I have a copy of and have read the Territorial Computer Access Policy; and*
3. *I will notify the Information Technology Department immediately if my password has been compromised.*

Signature:

End User:	Name (Please Print)	Date: