The Archbishop’s Seminary

Information Security Policy

Contents

Information Security Policy

Purpose

The Information Systems of the Seminary contain a vast amount of data which plays a crucial part in the administration of the institution as well as in the support of its academic and administration work. Loss of, or damage to this data could have potentially very serious consequences for both individuals and the organisation as a whole.

All of these areas present potential hazards to the security of the information. This document sets out the policy of the Seminary with regard to the security of information. They also contain a number of policies and procedures which form subsets of the main policy and which detail the practical ways in which the main policy will operate.

There is a responsibility on every member and user of the Seminary to safeguard information. To be aware of the extent of that responsibility it is essential that every member of staff, and student, should read, understand and implement these policies.

The work of the Seminary in relation to information security is still developing. Therefore the policies and procedures will be revised, and further procedures documented and developed, as time progresses.

These policies and procedures have been developed by the school's Information Systems Security Working Committee that included Mr Roger Xuereb Archer from Alliance Ltd. They have been approved by the Headmaster and the Master Copy of each one is held by the Administration Department of the Seminary.

Scope

This policy applies to all authorized users of the School's computer resources including, but *not* limited to, Archbishop's Seminary personnel, teachers, students, contractors and temporary staff members (collectively known as 'personnel'). It covers all computer resources, including hardware, software, and proprietary information located in Archbishop's Seminary offices and school premises and at any off-site locations if these resources are under Archbishop's Seminary management and/or ownership.

Policy Statements

Information Security Policy

Unique problems exist in the protection of the School's computer resources and the information that they create, store, and/or exchange. Therefore, Archbishop's Seminary Security Management has established and will continue to establish specific information security policies, controls, and procedures to adequately safeguard the School's computer resources and proprietary information. Toward this end, the essence of these information security policies, controls, and procedures is the School's right to:

- Establish policy on privacy, confidentiality, and security in electronic communications;
- Ensure that Seminary electronic communications resources are used for purposes appropriate to the Seminary's mission;
- Inform the Seminary community about the applicability of Seminary policies to electronic communications;
- Ensure that electronic communications resources are used in compliance with the Seminary policies;
- Prevent disruptions to and misuse of Seminary electronic communications resources, services, and activities;
- Access its property; and
- Protect its property.

The School's Right to Access its Property

At any time, the Archbishop's Seminary management reserves the right to examine e-mail, personal file directories, and any other information stored on or transmitted through Archbishop's Seminary computer resources. This examination ensures compliance with internal information security policies, supports the performance of internal investigations, and assists with the management of Archbishop's Seminary information systems.

The School, in connection with its information security responsibilities, has the right to access any Archbishop's Seminary computer system, computer file, or computer network at any time for any reason. Electronic communications systems, and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of Archbishop's Seminary, and are not the property of users of the electronic communications services.

It is the aim of the School to access its property in such a way as to protect the privacy of its staff and students. Were possible, access to specific user facilities, such as e-mails, will be carried out with the presence of the individual.

However, access may be required as part of the normal administration of the School's computers and systems. Therefore the school retains the right to access to all areas and contents, which access may occur from time to time without prior notice.

The School's Right to Protect its Property

To ensure that the School's computer resources and the information that they create, store, and/or exchange are safe from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft:

- All authorized users of the School's computer resources are required to protect these assets against unauthorized usage, access, modification, destruction, disclosure, loss or transfer of data, whether accidental or intentional.
- All Archbishop's Seminary personnel who have authorized access to the School's computers and the information that they create, store, and/or exchange are responsible for complying with the policies, controls, and procedures.
- Teachers and administrative staff are responsible for ensuring that Archbishop's Seminary Information Security policies are observed in their area and are also responsible for ensuring that all users are aware of Archbishop's Seminary information security policies.
- Each individual joining Archbishop's Seminary must be assigned a unique login to access services, such as e-mail, Intranet, and file sharing via the School's computer network.
- Access to the School's numerous computer applications (e.g., Payroll and HR) requires additional management approval.
- Archbishop's Seminary personnel may access only the systems and data to which they have been authorized.
- Archbishop's Seminary personnel who are assigned any computer items (e.g., computing hardware, printer etc.) that are required to perform their jobs must surrender these items upon separation (i.e., resignation, termination, and/or leave of absence) from Archbishop's Seminary. All such items are and remain the property of Archbishop's Seminary at all times.
- Archbishop's Seminary personnel upon separation from the School must have all access to the School's computers, networks, files, and programs disabled.

Information Security Policies

In addition to the general Information Security Policy and the School's right to access and protect its property, the School has information security policies and guidelines that provide requirements for the use and protection of the School's computer resources and the information they create, store, and/or exchange. Toward this end, the following information security topics are addressed in this handbook.

Computer System Usage

Archbishop's Seminary computer systems must be used only for academic activities. Incidental personal use is permissible so long as it does not:

a) Consume more than a trivial amount of resources;

b) Interfere with school productivity; and

c) Preempt any business activity.

Personnel are reminded that the use of the School's resources, including electronic communications, should never create either the appearance or the reality of inappropriate use. Users must exercise good judgment at all times when using Internet services. Archbishop's Seminary monitors the use of its computing and Internet resources for performance reasons as well as for compliance to Archbishop's Seminary usage policies.

User Accountability

Authorized users are responsible for actions resulting from the use of their password/account. Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to Archbishop's Seminary computers and networks, users must choose passwords that are difficult to guess.

Computer and Network Access

Users must be authorized by the Archbishop's Seminary to have and use a valid login ID and password to gain access to a School's computer system. When a computer is used as the primary machine supporting one or more production business applications, this machine must run an approved access control system that provides privilege control as well as change control.

Authorized users of a computer system must *not* provide unauthorized access to a computer system and/or unauthorized access to the data files that reside on that computer system. Examples include:

- Leaving a terminal that has an active logon session still connected to it unattended and unprotected.
- Leaving computer system files unprotected.
- Sharing one's user-ID and password with another.

Access Control

Access to Internal Resources

Access to internal computer and information resources must be controlled and access should be given solely on a minimum needs basis. Access to the schools resources may only be given following the appropriate authorization by the Headmaster.

A central log of authorized users and the areas that they are allowed to access must be maintained. A copy of this log should be forwarded immediately to the Headmaster following any updates.

Access to all computer systems and networks must be protected. The School's current authentication standard is the use of unique user name and password combination.

Usernames & Passwords

Each member of staff should have a unique username for all accounts. Passwords are to be kept private, should not be easily guessed and should be changed periodically or if it is suspected that it became known. Student passwords must expire at least at the end of the scholastic year.

External Access

The Headmaster must authorize all connections to internal Archbishop's Seminary computers via the Internet. Such connections must authenticate themselves at a firewall before gaining access to Archbishop's Seminary's internal network. This authentication must meet, at a minimum, the internal access control standards and must be done via a system approved by the Headmaster.

Public System Access

Designated "public" systems (such as Internet web Server) do not need these authentication processes because anonymous interactions are expected.

Access Testing

Users must *not* "test the doors" (probe) security mechanisms at either Archbishop's Seminary or other Internet sites unless they have first obtained written permission from the Headmaster. If a user does probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity.

Electronic Mail Security

Users must provide the same level of protection to School and personal information in electronic format as that afforded to the same information in verbal or hardcopy format. Commonly, users tend to assume that electronic mail is secure, or legally binding as normal printed correspondence. This is not necessarily the case with electronic communications, particularly e-mails.

The Archbishop's Seminary *cannot* guarantee that electronic communications will be private. Personnel should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy. Due to technical problems that may arise (e.g. power failure) and other circumstances not under the control of the Archbishop's Seminary the school does not take responsibility for any delay, or delivery failure, or for any damages suffered as a consequence.

Content

The following actions and uses of the School's e-mail system are **expressly forbidden**:

- Transmitting of any message, information or material that is unlawful, obscene, pornographic, malicious, threatening, abusive, libelous, defamatory or hateful, or encourages conduct that would constitute a criminal act or give rise to liability or a breach of the School's policies. Among those which are considered offensive is any information, images, files and any messages which contain sexual implications, racial slurs, gender specific comments, defamatory statements or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
- Sending of unsolicited bulk mail messages, repetitive mail messages to a recipient without the relevant consent, propagation of chain letters, hoax viruses or virus alerts.
- Communicating pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material. Users are prohibited from being involved in any way with the exchange of the material described here.
- Political material, content or comments.
- Advertising of personal items or any other advertisement that is not in line with the School's academic or administrative policies.
- Frivolous usage of the e-mail system.
- Use of private e-mail accounts for business related e-mails;
- Users are not authorized to retrieve or read any e-mail messages that are not addressed to them.
- Usage of any external connection (e.g. dial-out) whilst connected to a School network.

Sensitive Information

Discretion and good judgment must be exercised when sending sensitive information through electronic mail. Sensitive information must *not* be transmitted electronically over an un-trusted network (e.g., Internet) unless it has first been encrypted.

Personal Use

Personal use of the School's e-mail facilities should be kept to a minimum and must be consistent with the School's image and policies. Incidental, occasional personal use is permissible so long as:

- It does not consume more than a trivial amount of system resources;
- It does not interfere with the productivity of the individual;
- Any School signature and disclaimer are removed.

Disclaimer

Users may not transmit personal opinions as those of the Archbishop's Seminary, nor make any statement that may be construed to be a statement made by the Archbishop's Seminary. The following disclaimer should be included as a suffix to all e-mail messages to addresses external to the Archbishop's Seminary:

E-Mail Disclaimer.

> *The information in this email, and any of its attachments is strictly confidential and intended solely for the person or organisation to whom it is addressed. The opinions expressed in this email are not necessarily those of the Archbishop's Seminary. Access to this email by anyone else is unauthorized. If you are not the intended recipient, you must not copy or distribute it or take action in reliance on it. If you have received this email in error, please notify us as soon as possible. Please note that communication via email over the Internet is insecure because third parties may have the possibility to access and manipulate emails. The Archbishop's Seminary does not accept any responsibility in this eventuality.*

NOTE: This text is automatically added to all e-mails sent via the Archbishop's Seminary Mail system to non- Archbishop's Seminary addresses. Therefore users should not include this text in emails when sent from the School network as this would result in a double disclaimer text.

Message Forwarding

Recognizing that some information is intended for specific individuals and may *not* be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Archbishop's Seminary sensitive information must *not* be forwarded to any party outside the Archbishop's Seminary without the prior written approval of the Headmaster. Blanket forwarding of messages (e.g., email accounts or pagers) to parties outside Archbishop's Seminary is prohibited unless the prior written permission of the Headmaster has been obtained.

Message Monitoring

It is the policy of Archbishop's Seminary ***not*** to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that Archbishop's Seminary may from time to time examine the content of electronic communications.

Respecting Privacy Rights

Except, as otherwise specifically provided, personnel may *not* intercept, disclose, or assist in intercepting or disclosing, electronic communications. The Archbishop's Seminary is committed to respecting the rights of its personnel, including their reasonable expectation of privacy. The Archbishop's Seminary also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary for the Archbishop's Seminary technical support staff to review the content of an individual personnel's communications during the course of problem resolution. Technical support personnel may not review the content of an individual personnel's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels.

Purging Electronic Messages

Users must, on a regular basis, purge messages from their personal electronic message storage areas no longer needed for School purposes. This will increase storage space and simplify maintenance, management and related activities.

If users exceed their allotted storage allocation, then the system may block further receipt or transmission of messages. In addition, School technical staff may delete old information to bring the message storage area back in line with the authorized allocation levels.

Disciplinary Action

Failure to comply with the policy regarding email use, will immediately result in the temporary or permanent blocking of the user's email account.

Internet Security

The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. This policy describes the Archbishop's Seminary's official policy regarding Internet security. It applies to all personnel who use the Internet facilities within the Archbishop's Seminary network environment. Users must exercise good judgment at all times when using Internet services. Accessing inappropriate, non-academic related Internet sites is generally prohibited. Questions should be directed to the Headmaster.

Browsing & Content

The following actions and uses of the School's Internet system are **expressly forbidden**:

- Retrieval or Transmitting of any information or material that is unlawful, obscene, pornographic, malicious, threatening, abusive, libelous, or hateful, or encourages conduct that would constitute a criminal act or give rise to liability or unrest or a breach of the School's policies. Among those which are considered offensive is any information, images, files and any messages which contain sexual implications, racial slurs, gender specific comments, defamatory statements or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
- Retrieval or transmission of information relating to the carrying on of any form of private business activity.
- Advertising of personal items or any other advertisement that is not in line with the School's academic or administrative policies.
- Frivolous usage of the Internet system, particularly if this is of a private nature;
- Use of private Internet accounts for business related activities;
- Use of third party connections (such as personal Internet accounts) using the School's resources equipment unless authorized by the Headmaster.
- Employees are not authorized to access, retrieve or read any messages, information, databases that are not in the Public Domain or to which they have not been duly authorized to access by the Headmaster.
- Employees are not authorized to access any site, computer system etc. (resource) which is not in the Public Domain or to which they have not been duly authorized to access by the School or the respective owner or administrator of that resource. Hacking, Spoofing and any other similar unauthorized activity is forbidden and severe disciplinary actions will be taken.
- Usage of any external connection (e.g. dial-out) whilst connected to a School network.

Information Movement

All information taken off the Internet must be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate. It is also relatively easy to spoof another user on the Internet. Likewise, contacts made over the Internet should *not* be trusted with the Archbishop's Seminary information.

Downloading

Downloading of any material from the Internet is prohibited as it could pose a threat to the School's resources or services. This include such material as:

- Applications;
- Executables;
- Scripts;
- Applets;
- Macros;
- Screen savers;
- ActiveX components;
- Multimedia Files (such MP3, MPEG, AVI, MOV);
- Browser plug-ins; and
- Application plug-ins, add-ons, patches and extensions.

If a user requires such material, then a written request should be forwarded to the Computer Systems Administrator. If the School requires this material, then the System Administrator will download it and subsequently forward/install the material for the requestor.

All material downloaded from non-Archbishop's Seminary sources via the Internet must be screened with virus detection software prior to being invoked. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone, non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage would then be restricted to the involved machine.

Sensitive Information

Users must *not* place the Archbishop's Seminary material (software, internal memos, etc.) on any publicly accessible computer that supports anonymous file transfer (FTP) or similar services, unless the Headmaster has first approved the posting of this material. In more general terms, the Archbishop's Seminary internal information must *not* be placed in any location, on machines connected to the Archbishop's Seminary internal networks or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.

Credit card numbers, login ID and passwords, and other parameters that can be used to gain access to goods or services, must *not* be sent over the Internet in readable form. An encryption algorithm approved by the Archbishop's Seminary Information Systems Administrator must be used to protect these parameters as they traverse the Internet.

Information Protection

Exchanges of software and/or data between the Archbishop's Seminary and any third party may *not* proceed unless this is authorized by the School. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

The Archbishop's Seminary strongly supports strict adherence to software vendors' license agreements. Copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Likewise, participation in pirate software bulletin boards and similar activities represent a conflict of interest with the Archbishop's Seminary policies, and are therefore prohibited.

Expectation of Privacy

Users of the Archbishop's Seminary information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, workers should not send information over the Internet if they consider it to be private.

Resource Usage

The Archbishop's Seminary provides Internet connectivity for a number of academic reasons. These include e-mail, World Wide Web services, file transfer, and remote access to e-mail mailboxes as well as other services. Users must exercise good judgment at all times when using Internet services. Accessing inappropriate, non-academic related Internet sites is prohibited.

Internet usage for personal purposes, should be done on personal, not School time. Use of the Archbishop's Seminary computing resources for these personal purposes is permissible so long as:

- The incremental cost of the usage is negligible;
- It does not interfere with the academic activities of the individual; and
- This is not a business activity.

Internet usage is subject to review and monitoring by authorized Archbishop's Seminary personnel. Personnel wishing to use Internet resources for more extensive personal activities should acquire their own, personal account from an independent Internet service provider so that the Archbishop's Seminary's name is not associated with the activity.

Computer and Server Security

Computers are today compact machines accessible to various users thus requiring several levels of protection. Both physical and logical security measures must be taken to ensure the safekeeping of these computers and the proprietary data they contain. Personnel must exercise good judgment to safeguard computers and the information contained therein. Personnel are also responsible for protecting the information stored on the computer.

Hardware Security Policy

- Each computer, server or other computer resource (e.g. printer) must be marked for identification and inventory control. Inventory records of computer resources must be kept current.
- Computer resources should be treated with due care and used in line with the School's needs.
- Food and drink should not be taken next to computer resources to minimize the risk of spillage and the resultant damage to the equipment.
- To prevent unauthorized access, users who are assigned a personal computer must configure their screen savers to blank the screen and require a password to resume whenever their workstations are unattended for more than 15 minutes.
- If sensitive data resides on microcomputers, screen savers must be manually invoked whenever users leave these microcomputers.
- Anyone seeking to remove any computer resource from an Archbishop's Seminary premises must first request authorization from the Headmaster.
- The loss or theft of any computer hardware and/or software must be reported immediately, in writing, to the Computer Systems Administrator who will inform the Headmaster of all thefts/losses.
- Computer File Servers, Networking Equipment and any other resource that contains sensitive information must be located in a secure area where physical access can be controlled.
- Physical and Logical access to the file servers should normally be limited to the Computer Systems Administrator. Contractors may be given access for normal support purposes whilst under supervision of the Systems Administrator.
- Laptop computers should be physically protected to lessen the risks of theft, destruction, and/or misuse. Suggested techniques include housing the equipment in a locked room, physically locking the equipment, or using a security cable with a locking mechanism.

Software Security

- Unless they receive information to the contrary, users should assume that all software on the Archbishop's Seminary computers is protected by copyright. In most cases, copyright protection will be evident based on a notice affixed to the media (for packaged software) or displayed on the screen. Software purchased for use by the School must be used in accordance with contractual agreements and copyright laws;
- Computer software purchased by the Archbishop's Seminary is authorized for School use only. Making copies of School purchased software for personal use is illegal and prohibited, unless specifically authorized within the license agreement.
- Software authorized for use on the Archbishop's Seminary computers is that which has been purchased through the normal purchasing procedures, or has been developed by the Archbishop's Seminary personnel or contractors. Use of unauthorized software, including that which has been borrowed or purchased by the user, is strictly prohibited;
- Freeware, shareware, and other software obtained without cost is considered unauthorized unless specifically approved in writing for use by the Headmaster or the Computer Systems Administrator.

Anti-Virus Protection

The Archbishop's Seminary resources need to be protected against the threat of computer viruses. Such viruses can cause damage and lose to information as well as possible expose School information to third parties. In addition, the School's image may be damaged if a virus is propagated via its resources and effects external computer systems. To minimize the possibility of virus infection the following must be adhered to:

- Approved virus screening programs must be installed and enabled on all computers, laptops, and file servers at all times;
- E-mail should be automatically scanned on receipt at the central e-mail system;
- If a virus detection program indicates that a virus has been discovered, the involved users must immediately notify the Computer System Administrator and desist from taking any further use of the system until the System Administrator has cleared this system; and
- Externally supplied floppy disks or other storage media may not be used on any Archbishop's Seminary personal computer unless these disks have first been checked for viruses.

Network Security

All external network connections to Archbishop's Seminary must be reviewed and approved by the Computer Systems Administrator and approved by the Headmaster prior to ordering and/or implementing the connection.

Unless the prior approval of the Headmaster has been obtained, external network connections that could allow non-Archbishop's Seminary users to gain access to Archbishop's Seminary systems and information may *not* be established. These connections include but are *not* limited to the establishment of new office connections, the establishment of connections to external sites, and the establishment of new Internet connections.

All physical and logical access to the School's network resources has to be managed and controlled. All Sensitive network equipment is to be in a secure environment where it may not be tampered with by unauthorized personnel.

Firewalls

All School external network connections (connections to non-Archbishop's Seminary networks) must have network level authentication using the School standard. Direct IP connection (e.g., Internet) must use a School approved firewall to protect the Archbishop's Seminary from unauthorized access. The School standard for firewall configurations is to deny all services unless explicitly permitted based on a compelling School need. The School's Computer Systems Administrator is responsible for configuring, administering, standardizing, and ensuring the integrity of all School firewalls.

Data Recovery

Main Systems

Backups preserve School information assets and should be made on a regular basis for audit logs and for files that are irreplaceable, have a high replacement cost, or are considered critical to the School's business.

Backups can be made using either a full or incremental approach. In either case, a multiple generation set approach should be used for the back-up media employed.

The backup media should be stored in a secure, geographically separate location from the original and isolated from environmental hazards.

Certain essential information, such as financial, payroll etc. should have separate back-up copies made at the end of each respective period.

Copies of back-up media should be kept off-site so as to ensure availability of the critical information in the event of a major disaster (such as an extended fire in the School premises).

This off-site storage should be secure and access to this material should only be given to personnel duly authorized by the Headmaster.

End-User

The Computer Systems Administrator must ensure that users have adequate facilities to back-up School's essential information on a School file server. Individuals are responsible for backing up the data on their desktop/laptop systems to the appropriate area a School file server.

The Computer System Administrator should back up essential end-user information that has been stored on file servers as part of the Main Systems back-up procedures.

Third Parties

Organizations/individuals who provide computing services for School applications are responsible for ensuring an adequate backup and recovery plan.

External Communications

Public Disclosure

Personnel must not publicly disclose internal Archbishop's Seminary information via any means that may adversely affect the Archbishop's Seminary relations with any party or public image. Written approval from the Headmaster has first been obtained before any such disclosures. Such information includes school administration or financial information, systems configuration, software bugs, software product performance, and the like. Responses to specific systems support e-mail messages are exempted from this policy.

Public Representations

Whenever users provide an affiliation, either by explicitly adding certain words, or by implication, for instance via an e-mail address, they must also clearly indicate the opinions expressed are their own, and not necessarily those of the Archbishop's Seminary. All external representations on behalf of the School must first be cleared with the Headmaster.

Modems

Modems directly connected to users' computers, which generally provide a weak, if any, authentication requirement, pose a significant threat to the security of the Archbishop's Seminary's networks and computer systems. Therefore, modems must *not* be configured in auto-answer mode. Personnel are also reminded that such connections do not receive firewall protection from protocols known to present security problems.

The Archbishop's Seminary provides its Personnel with central access to e-mail and Internet facilities. So please use these facilities wherever possible. If you still need to use a modem to dial out, then the procedure for Third Party Connections must be followed.

Third Party Connections

Personnel should not use dial-up facilities, such as personal Internet accounts, Seminary Remote Access or Electronic Banking Facilities, whilst concurrently connected to the School network.

When establishing a connection to any external network or facility, called a Third Party Connections (TPC) not via the School network (such a dial-up third party connection to an ISP) they must physically disconnect their computers from all School networks - simply logging-off the network is not adequate. It should also be noted that the use of a TPC requires authorization by the Headmaster.

Incident Handling

Contact Point

All information security incidents or potential security breaches be it to the School’s computer resources or to the information that they create, store, and/or exchange, must be reported to the Headmaster or, if applicable, to the appropriate Computer Systems Administrator.

Incident Log

Any suspected or actual incident must be recorded in an appropriate register that is held at the Headmaster's office. It is the responsibility of the Systems Administrator to update the log following such incident (or suspected incident) with the relevant details as laid out in the register.

Sanctions of Law

The Maltese law prohibits the theft or abuse of computers and other electronic resources such as electronic communications resources, systems, and services. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of electronic communications resources, systems, and services. The law classifies certain types of offenses as being a serious offence punishable with hefty fines and or imprisonment.

School Disciplinary Actions

Seminary policy prohibits the use of Seminary property for illegal purposes and for purposes not in support of the mission of the Seminary. In addition to any possible legal sanctions, violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion, as relevant, pursuant to Seminary scholastic and administrative policies.

Disciplinary Process

The School's administration will seek to understand the reasons for any violation of these policies. Where reasonable, parties who can be involved in any disciplinary action will be suitably advised and the matter discussed openly so as to arrive at a mutually acceptable resolution of the violation. However the School retains the right to use the approach that it deems most appropriate and to subsequently take appropriate actions.

Any Archbishop's Seminary personnel who violates the Archbishop's Seminary Information Security Policy or commits any security violation may be subject to disciplinary action up to and including termination.

Any member of the contractor work force who violates the Archbishop's Seminary Information Security Policy or commits any security violation will be subject to removal from the Archbishop's Seminary location and termination of the contract covering the assignment.

Additionally, any individual who violates the Archbishop's Seminary Information Security Policy or commits any security violation may also be subject to criminal prosecution and/or civil litigation under Maltese law. The decision to initiate litigation will be made upon review by the Archbishop's Seminary Legal Counsel and the School's Headmaster.

Effective Date

01/03/2002

Appendix A - Definitions

Definitions

Computer System — A functional unit consisting of:

- computer hardware (e.g., mainframe, minicomputer, laptop, workstations, file server)
- computer software (e.g., operating systems, applications)
- data processed and/or stored (e.g., on hard disk, floppy disk, tape, cartridge, CD -ROM, DVD, in memory)
- supporting documentation for data and software
- circuits and devices associated with system access, data storage, retrieval, transmission and display

Control — A security measure implemented to meet or exceed a specific policy.

Data Security Classification — Archbishop's Seminary data is classified into two basic categories:

1. Non-sensitive: Data is classified as "non-sensitive" if unauthorized modification, destruction, loss, disclosure, or unavailability of the data is not expected to cause interruption, setback, or damage to Archbishop's Seminary's business goals, competitive position, or reputation.
2. Sensitive: Data is classified as "sensitive" if unauthorized modification, destruction, loss, disclosure, or unavailability of the data would cause an interruption, setback, or damage to Archbishop's Seminary's business goals, competitive position, or reputation including, but not limited to personnel data (e.g., Social Security Numbers). All data that falls under the Data Protection Act is also considered "sensitive" data.

Direct IP Connection — Any short to long term connection established between a network (LAN or WAN) not connected to the Archbishop's Seminary network and the Archbishop's Seminary network. NOTE: This type of connection is intended to support only the TCP/IP protocol suite.

Downloading — The transfer of data from a host computer (mainframe, minicomputer, network server, etc.) to a connected workstation, such as a personal computer.

Encryption — The process of transforming computer-based readable data into an unintelligible form called "ciphertext." Reversing the encryption process and transforming the ciphertext back into its original "plaintext" form is called decryption. The encryption and decryption methods are designed so that only the desired recipient, with the appropriate key, may decrypt the ciphertext.

External Network Connection — Any temporary connection established between a device that is not on the Archbishop's Seminary network, to the Archbishop's Seminary network. In most cases, this is a manually originated modem or ISDN connection.

Login-ID — The term login-ID (also known as a user-ID) is used to refer to the unique name that identifies a user to a computer system.

Microcomputer — A general-purpose or portable (including laptop) computer consisting of one or more microprocessors assembled in a unit that will fit on top of a desk. The unit typically consists of a central processing unit (CPU), video display, keyboard, disk drive, and a number of peripheral devices such as a printer and CD-ROM drive. The terms "microcomputer" and "personal computer" (PC) are considered synonymous and may be used interchangeably in this document.

Owner — The principal user representative who has been charged with responsibility for a particular application system or data collection (for example a database). The Owner is the focal point for all user activity with respect to the application or data collection in question, including the specification of security requirements and related access control restrictions.

Policy — Management instructions indicating how an organization is to be run. A policy is a high-level statement intended to provide mandatory instructions to those who must make present and future decisions.

Procedure — A series of specific operational steps to execute a control.

Security Administrator — Specific individuals, assigned by management, who provide or coordinate the administration of computer system security and/or network security for those computer systems and/or networks for which they are responsible.

Uploading — The transfer of data from a connected device, such as a personal computer, to a host computer (mainframe, minicomputer, network server, etc.).

Virus — A parasitic software program equipped with the means of reproducing itself, that spreads throughout a computer or network by attaching itself or infecting other software or diskettes. A worm is a similar program that propagates across a network by making copies of itself.