

# SCSU INFORMATION SECURITY USAGE POLICIES AND PROCEDURES

## 1. INTRODUCTION

Information and information system resources are essential assets of Southern Connecticut State University (SCSU). The entire University community (students, faculty, and staff) is responsible for ensuring that computing and communication facilities are used in an effective, efficient, ethical and lawful manner. This Security Policy is provided to all members of university community to provide proper guidelines on each individual's responsibility to protect SCSU information through the appropriate usage of and application of security measures to individual computers, university accounts (Windows, Banner, MySCSU, etc.) and other technology services available on campus. Every individual should understand their obligations relating to the policy statements described herein.

SCSU staff responsible for planning, acquisition, configuration, deployment, management, and auditing of information systems should apply sound risk management practices when selecting security controls. This would include identifying what information is intended to be protected, what are the threats to that information or information system resource and the proper cost-effective safeguards that need to be applied to adequately protect the information. This resource acts as a guide for such practices. Questions should be addressed to the appropriate IT personnel should they arise.

## 2. PURPOSE

This Information security policy provides a set of comprehensive security guidelines to ensure that SCSU information and information system resources are properly and consistently protected. This Information Security Policy outlines student, faculty, and staff responsibilities in supporting the SCSU security program and compliance with this security policy.

The objectives of this policy are:

- i) Provide for uninterrupted services to the University community.
- ii) Safeguard the integrity and availability of the campus data network through appropriate controls
- iii) Protect the University's computing and communication assets including data, software and hardware.

- iv) Reduce the likelihood that computers on campus are used to attack other organizations, bringing liability and disrepute to the University.
- v) Protect SCSU against the loss or misuse of any information.
- vi) Define responsibility and accountability to maintain protection of SCSU information.
- vii) Preserve and support audit and legal compliance.

### **3. COVERAGE OF POLICY**

This policy applies to all information assets of Southern Connecticut State University. The term University Community includes students, faculty, staff, trainees, vendors, volunteers, contractors, consultants and other affiliates of the University. Each member of the University Community with access to institutional information is subject to and has responsibilities under this policy. The term information refers to any intelligible representation of data, including, but not limited to, such things as handwritten notes, software designs, databases, program listings, files, training material, risk assessment documents, business continuity plans, magnetic media (such as hard drive, tapes and floppy disks), printer output, telephone conversations, video tapes, and fax output. The term information system resources refers to information resources consisting of software and hardware designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit electronic data for a specific business process, including workstations, laptops, phones, fax machines, servers, and network devices.

## **4. SECURITY ROLES & RESPONSIBILITIES**

**4.1** The University believes that information security is the responsibility of all students, faculty, and staff. Every person handling information or using University information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the University.

**4.2** This Policy is the responsibility of the CIO, Information Technology; supervision of the policy will be undertaken by the Senior Management of the University and the CIO from Information Technology. Implementation of the information security policy is managed through the Information Security Officer and other designated personnel with security responsibilities in specified areas of the University.

**4.3** The responsibility for the security of computing and communication systems rests with the systems administrators who manage those systems. Information Technology (IT) will help systems administrators carry out these responsibilities to the extent possible with available resources.

**4.4** Heads of departments with computing or communication devices connected to the campus network managing their devices will:

i) Designate an individual with the responsibility to create and maintain a current contact list of individuals who are responsible for the computer(s) for each location in the department.

**4.5** Information Technology (IT) will:

i) Prepare and publish security alerts, notices, recommendations and guidelines for network and system administrators.

ii) Monitor backbone network traffic, as necessary and appropriate, for the detection of unauthorized activity and intrusion attempts.

iii) When a security problem (or potential security problem) is identified, IT will seek the cooperation of the appropriate contacts for the systems and networks involved in order to resolve such problems, but in the absence or unavailability of such individuals may need to act unilaterally to contain the problem, up to and including temporary isolation of systems or devices from the network, and notify the responsible system administrator when this is done.

iv) Carry out and review the results of automated network-based security scans of the systems and devices on University networks in order to detect known vulnerabilities or compromised hosts.

v) When appropriate, IT will inform the system administrators and department managers of planned scan activity providing detailed information about the scans, including time of

scan, originating machine, and test and vulnerabilities tested for. The security, operation or functionality of the scanned machines should not be endangered by the scan.

vi) Report the results of scans that identify security vulnerabilities only to the system administrator contact responsible for those systems.

vii) Report recurring vulnerabilities over multiple scans to the Departmental Head, and or appropriate manager.

viii) If identified security vulnerabilities, deemed to be a significant risk to others and which have been reported to the relevant system administrators, are not addressed in a timely manner, IT will take steps to disable network access to those systems and/or devices until the problems have been rectified.

ix) Provide assistance and advice to system administrators to the extent possible with available resources.

x) Co-ordinate investigations into any alleged computer or network security compromises, incidents and/or problems.

xi) Co-operate in the identification and prosecution of activities contrary to University policies and/or the law. Actions will be taken in accordance with relevant University Policies, Codes and Procedures with, as appropriate, the involvement of the University Police and law enforcement agencies.

**4.6** "System Administrator" refers to the individual who is responsible for system and network support for computing devices in a local computing group. In some instances, this may be a single person while in other instances the responsibility may be shared by several individuals, some of whom may be at different organizational levels. If an administrator is not designated, the owner of a computer is considered the System Administrator. System Administrators will:

i) Endeavor to protect the communication networks and computer systems for which they are responsible.

ii) Endeavour to employ IT recommended practices and guidelines where appropriate and practical.

iii) Co-operate with IT in addressing security problems identified by network monitoring.

iv) Address security vulnerabilities identified by IT scans deemed to be a significant risk to others.

v) Report significant computer security compromises to Information Security Officer.

vi) All computer resources must provide a notice before logon stating that the computer and network are solely for use of users authorized by Information Technology and that any unauthorized access is prohibited and may result in prosecution.

vii) Information, which by law is confidential, must be protected from unauthorized access or modification. Data, which is essential to critical functions, must be protected from loss, contamination, or destruction.

## 5. ACCEPTABLE USE

SCSU provides information system resources for support of SCSU academic and business operations. Users authorized to use SCSU information system resources, with supervisor's permission, may make incidental and occasional personal use of these facilities when it does not generate any additional costs to SCSU or does not reduce the staff or employee's productivity or student academic performance. With supervisor's permission, incidental and occasional personal use is permissible if the use meets all of the following conditions:

- i) Personal use does not consume or commit resources that could otherwise be used for SCSU academic/ business purposes -- such use parallels the generally accepted practice of allowing users to make local telephone calls of a personal nature, as long as the other conditions outlined below are met.
- ii) Personal use does not interfere with employee productivity or preempt any SCSU academic activity or violate SCSU policies and CSU policies.
- iii) Personal use is not for the purpose of solicitation of a personal business or for personal gain.
- iv) Personal use does not involve sending, forwarding, redistributing or replying to communications promoting lotteries, or "pools" based on chance, or chain letters.
- v) Personal use is not for the purpose of accessing, downloading, storing, or otherwise processing information of a non-professional manner, that which is sexually explicit, violent, vulgar, criminal in nature, or otherwise offensive material addressing age, gender, sexual orientation, race, religion, political beliefs, national origin, or disability.
- vi) Personal use should not be excessive as determined by the supervisor and the Information Technology.
- vii) Student/ patrons of the University may use University resources such as the Internet for SCSU academic purposes as needed to work on a specific assignment.
- viii) Each individual of the University Community is responsible for all actions performed on SCSU information resources under their User-ID/password. Disclosure of User-ID/password combinations except under emergency conditions is prohibited. If a User-ID/password is disclosed under emergency conditions, the password should be changed as soon as possible.
- ix) Students may not set up servers in their residence hall rooms. Exceptions to this policy must be approved by the CIO, Information Technology (e.g. computer science majors may be required to do this as part of their academic requirements). Exceptions will be approved on a case-by-case basis.

x) Employees may not use SCSU computer resources to set up services or accounts for the purpose of which is not in accordance with the non-profit, educational mission of the university. Individuals with questions concerning the appropriate use of a university computer should contact the CIO or the Information Security Officer.

### **5.1 Electronic Mail (E-mail) Acceptable Use**

This section provides additional guidelines on the proper use of, access to, and disclosure of electronic mail (email) messages sent or received by the SCSU Community (students, faculty, staff, authorized contractors, and consultants) using the University's electronic mail system.

i) The email system and the contents of all email messages sent, received or stored in the email system are the property of SCSU. University email is provided and intended to be used for University business only. Electronic mail is intended to be a convenient way for the students, faculty, and staff to communicate with one another and with colleagues at other locations. It is not the practice of SCSU to monitor the contents of electronic mail messages. However, the information in electronic mail files should not be considered "private," as it may be subject to disclosure under certain circumstances; for example, during audit or legal investigations. SCSU does not routinely monitor (e.g. via cookies) the Internet browsing habits of its students, faculty and staff.

ii) Users must not send email so that it appears to be anonymous or to have come from someone else.

iii) Users should not send unsolicited advertising via email.

iv) Users must not use SCSU computer systems to send or reply to "chain letters" or to distribute or obtain offensive or inappropriate material.

v) Users must not access personal email accounts or ISP's through a modem while simultaneously connected to the SCSU network.

vi) If SCSU information system resources are used to access a personal email account, the guidelines in this security policy also apply to that usage.

vii) SCSU users must be aware that legal restrictions on sending or receiving copyrighted, obscene, and/or objectionable material may apply and use discretion when forwarding messages to others.

viii) SCSU users should not execute email attachments for non-official/non-academic business such as music, video or animation files unless scanned for viruses.

## **5.2 Internet Acceptable Use**

The SCSU network provides Internet access to assist the university community in fulfilling their academic and professional requirements and in carrying out job related functions. With the exception of the personal incidental use outlined above, Internet access should be used for business related purposes. This section covers guidelines for Internet usage.

- i) Information Technology will review all SCSU Internet connections (all data communications with remote locations or devices using shared computing resources, e.g. local area network, attached PCs, etc.). The SCSU community can only access the Internet with connections established by Information Technology.
- ii) When using the Internet from the SCSU network, you are presenting yourself as a SCSU representative and must conduct yourself in accordance with all aspects of this security policy.
- iii) Information posted to discussion groups or mailing lists bearing a SCSU address must reflect the official position of the individual and must state that it is not the position of SCSU.
- iv) Users must not download material from the Internet that is subject to copyright or other intellectual property right protections unless express permission to do so is granted by the material owner.
- v) Information Technology can disallow the use of harmful software if a user downloads a file that adversely affects their system or other systems in the SCSU network.
- vi) All downloaded materials must be scanned for viruses before file execution.

## **6. LOGICAL & PHYSICAL ACCESS CONTROLS**

The SCSU network is provided to meet the academic needs of the University. The network connects all information system resources to facilitate communication among them. It is necessary to identify individuals who are permitted to access SCSU information system resources physically and logically connected to the SCSU network. Logical and physical controls prevent or discourage unauthorized access to SCSU information system resources. Information Technology controls access to the SCSU production network, internal network, systems and applications. Users control access to their individual computer; the files and applications that are installed on their individual computer. All files and applications are "owned" by key users; the owner is responsible for determining who has access to the file application and the appropriate level of access.

### **6.1 LOGICAL CONTROLS**

#### **6.1.1 User ID's and Passwords**

SCSU assigns unique user ID's and passwords for each authorized user. Users are responsible for all actions performed on SCSU information system resources under their User ID and password. Disclosure of User ID's and passwords, except under emergency conditions, is prohibited.

Passwords are the first line of defense for the protection of SCSU information and information systems resources. Using strong passwords will help reduce the possibility of unauthorized access to the university's network infrastructure.

##### **6.1.1.2 Password Length and Complexity**

Unless a specific University system or program requires otherwise, all passwords should be at least eight characters in length. All passwords must include at least one upper case letter, at least one lower case letter, at least one number, and at least one non-alphanumeric character. Simpler passwords are less secure than complex passwords. Passwords should not be, or be in any way derived from, dictionary words (or slang, jargon, and foreign language words), names, user IDs, or identifiable personal information. Passwords should not include words or terms associated with Southern Connecticut State University.

Those in charge of University systems, services, and programs are permitted to set additional password requirements beyond those listed above.

##### **6.1.1.3 Password Expiration**

SCSU forces password expiration every 60 days on most systems within the network infrastructure. SCSU users must change their password when prompted by the system or risk being locked out, thus requiring assistance to reset the account. When setting new passwords, the same passwords may not be used within one year of initial use.

#### **6.1.1.4 Password Protection**

Passwords used to connect to the SCSU network are SCSU proprietary information and should not be disclosed to anyone other than the authorized user, including system administrators and technical support staff. If for whatever reason a password is disclosed to an individual other than the authorized user, the password should be promptly changed. Individuals can be held accountable for any misuse if their passwords are guessed, disclosed, or compromised.

The University retains responsibility for the electronic security of passwords as stored within the University system; all members of the University community are otherwise responsible for maintaining the security of their passwords.

Any paperwork including user ID and password information should be destroyed or filed securely; passwords should not be written down and left in insecure environments. Passwords should not be stored within web browsers or other computer applications. When independent web sites or software programs require a user to provide a user ID, email address, and password, University passwords should not be re-used. Using the same password outside of the University system jeopardizes the security of personal and University systems and data.

#### **6.1.1.5 Passwords Do's and Don'ts**

Below are some simple pointers for proper management of passwords:

##### **Do's:**

Do use a password with a mixture of alphanumeric and non-alphanumeric characters, e.g., punctuation, special characters.

Do use a password consisting of 8 or more characters.

Do use a password that is easy to remember, so you don't have to write it down.

Do use a password that you can type quickly, without having to look at the keyboard. This makes it more difficult for someone to steal your password by watching over your shoulder.

Do change your password at least every 60 days.

Do change all vendor-supplied or default passwords on a computer prior to connecting to the SCSU network infrastructure.

Do change your password if it has been disclosed or suspected of being disclosed.

Do control all software and files containing formulas and algorithms used for the generation of passwords or Personal Identification Numbers (PINs).

**Don'ts:**

Don't use your login name in any form (as-is, reversed, capitalized, doubled etc.) as a password.

Don't use your first or last name in any form.

Don't use your spouse, or children's names.

Don't use any other personal information that can be easily obtained. This includes license plate numbers, spouse, children or pet names, telephone numbers, social security numbers, the brand of your automobile, zip code, the name of the street you live on, etc.

Don't use a password of all digits or all the same letters. This significantly decreases the search time for an intruder.

Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.

Don't use the same password on multiple systems.

Don't write down your password and leave in a location where other personnel may have access to it.

Don't share your password with anyone, except in response to your request to Network Operations for internal service or maintenance. Change the password as soon as possible after sharing it with Network support personnel.

**6.1.2 Access Requests**

User access should be requested by the Departmental Head and reviewed by the CIO, Information Technology or designee. SCSU departmental heads will determine the access required for individual and request appropriate access for those individuals. Department managers must ensure that their representatives maintain only those access privileges required to perform their academic/ official job functions.

**6.1.3 Access Termination**

When an employee terminates employment and a future contract has not been issued, their access to computer resources will be terminated. Retired employees may be permitted access to electronic mail systems. Similarly, students who are not enrolled for two consecutive semesters will have their access to computer resources terminated. Department heads and HR must ensure access to information systems is removed for

terminated employees. Information Technology is responsible for performing access termination prior to the individual's departure.

## **6.2 PHYSICAL CONTROLS**

Physical controls are often viewed as involving only physical access to a facility. However, physical controls actually include facility access, access to controlled areas within a facility, access to terminals or systems, handling of laptops, and location and handling of printers. This policy addresses the protection of and physical access to SCSU facilities, computer equipped rooms, computer labs, network equipment, PCs and other related equipment. All SCSU facilities will also adhere to all local, state and national electrical, fire, and other appropriate codes and insurance requirements.

### **6.2.1 Facility Access**

Access to SCSU facilities must be controlled in a manner that provides security to the SCSU community, and assets and provides for the detection of perimeter breaches. Recognizing that no physical security measure will withstand all intrusions, SCSU facilities should always be provided with a degree of physical protection commensurate with the value of the assets in, around, or accessible from that facility.

### **6.2.2 Workstations**

SCSU users must protect their workstations in a manner that precludes unauthorized access to SCSU information and information system resources. This would include logging out of workstations or terminals when left unattended or invoking a password protected screen saver to deter unauthorized users. Encryption of files that contain protected information must be used for the storage of protected information.

### **6.2.3 Laptop Systems**

In addition to those concerns regarding workstations addressed above, the following should also be considered regarding the use of laptop systems:

- a) It is the responsibility of the individual to update and maintain accurate information on the Equipment on Loan Form (CO-1079 REV 9/98).
- b) When not in use, the laptop should be stored in a locked cabinet or desk drawer or with some type of physical locking device.
- c) When traveling, the traveler must maintain physical control of the system at all times.
- d) Consider the use of removable media for storage of protected information while on travel.

## **7. COMPLIANCE WITH LEGAL & CONTRACTUAL REQUIREMENTS**

### **7.1 Authorized Use**

SCSU computing facilities must only be used for authorized purposes. The University may from time to time monitor or investigate usage of computing facilities and any person found using computing facilities or systems for unauthorized purposes, or without authorized access, may be subject to disciplinary, and where appropriate, legal proceedings.

### **7.2 Monitoring of Operational Logs**

The University shall only permit the inspection and monitoring of operational logs by computer operations personnel and system administrators. Disclosure of information from such logs, to officers of the law or to support disciplinary proceedings, shall only occur:

- i) when required by and consistent with law;
- ii) when there is reason to believe that a violation of law or of a University policy has taken place;
- iii) when there are compelling circumstances.

### **7.3 Access to University Records**

In general, the privacy of users' files will be respected but the University reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with University policies and regulations, and to determine which records are essential for the University to function administratively or to meet its teaching obligations. Except in emergency circumstances, authorization for access must be obtained from the Office of Information Technology, and shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

### **7.4 Protection of Software**

Software installed on any of the SCSU systems must be legally licensed. To ensure that all software and licensed products used within the University comply with the Copyright, Designs and Patents Act 1988, Digital Millennium Copyright Act, and subsequent Acts, the University will carry out checks from time to time to ensure that only authorized products are being used, and will keep a record of the results of those audits. Unauthorized copying of software or use of unauthorized products by students, faculty, or staff may be grounds for disciplinary, and where appropriate, legal proceedings. This includes illegally downloading software from the Internet. Users should not copy

software applications from one PC to another PC. SCSU departmental heads are responsible for ensuring that no software license usage in their department exceeds purchased levels, and arrange for additional licensed copies when needed to support academic activities. Information Technology will install all software and maintain an inventory of all applications.

## **7.5 Virus Control**

Computers infected with viruses or malicious code could jeopardize information security by contaminating, damaging, and destroying data. This policy provides controls to protect against such attacks.

The University will maintain detection and prevention controls to protect against malicious software and unauthorized external access to networks and systems. All users of University computers, including laptops, shall comply with best practice, when defined by Information Technology in order to ensure that up-to-date virus protection is maintained on their machines.

Users must be alert to and report any abnormal behavior exhibited by their computers or software applications since this may indicate the existence of a virus or other malicious logic undetected by resident anti-virus software.

It is the responsibility of Information Technology personnel to ensure that current anti-virus software is installed on servers and all other applicable equipment within the network.

### **7.5.1 Virus Containment and Removal**

Resident anti-virus software will be used to remove a virus from an infected file or program. If anti-virus software fails to remove the virus, the system must be disconnected from the network.

If subsequent attempts to remove the virus using updated anti-virus software resident on floppy disks fail, all software on the computer will be deleted including boot records, if necessary, and must be reinstalled using an uninfected, trusted source.

## **7.6 Host and Network Security**

Hosts and Network must be protected by available tools and security measures. These include use of special software such as Firewalls, Intrusion Detection Systems, Network Scanners and Network Monitors. All network firewalls policy and rules must be documented and must adhere to the University Security Policy.

## **8. INCIDENT DETECTION & REPORTING**

Properly and efficiently detecting and responding to suspicious network activities and unauthorized system use requires that users report unusual and suspicious activity surrounding the use of information system resources. Users should report possible incidents to the Office of Information Technology by email or by calling the help desk.

### **8.1 SECURITY BREACH NOTIFICATION & REPORTING**

#### **8.1.1 Security Breaches**

A security breach is defined as any action or event in contravention to the provisions of this Information Security Policy; and/or actions or events deemed a security breach by State or Federal law enforcement organizations.

The guidelines listed under "notification" below, should be applied during the course of an actual or potential security breach.

#### **8.1.2 Notification of a Security Breach**

The following steps are listed in the order that they should be taken. Once a breach is confirmed, the responsible officer should take these steps as urgently as possible. If a particular step is not appropriate to the breach, then the officer should ignore it and move to the next step.

- a) The CIO, Information Technology should be notified immediately.
- b) If the security breach involves a possible breach of State, Federal or International law, then the CIO, Information Technology or delegate will notify SCSU Police or state law enforcement agency (as appropriate), as soon as is practicable.
- c) If a University element is involved, then that element should be notified as soon as possible, preferably via the Head of Element or approved element representative.
- d) If an organization or person external to the University is involved in any capacity, then the Federal Computer Incident Response Center (FedCIRC) should be contacted.
- e) If an organization or person external to the University is involved as a potential victim, then that organization or person should be advised as soon as possible.

#### **8.1.3 Reporting a Security Breach**

The person authorized by the CIO, Information Technology, to carry out the technical investigation of a security breach must submit a report to the Head of element outlining the following details (where possible):

- a. General nature of the security breach
- b. General classification of people involved in the security breach, (such as student, privileged staff member)
- c. Computer systems involved in the security breach
- d. Details of the security breach
- e. Impact of the security breach
- f. Unrealized, potential consequences of the security breach
- g. Possible courses of action to prevent a repetition of the security breach
- h. Side effects, if any, of those courses of action.

#### **8.1.4 Unauthorized Access Attempts**

This includes anything from harmless exploration to hacking in order to gain access to information. Unauthorized access also includes gaining access to computer systems for future use (e.g. extortion).

All unauthorized access attempts must be noted and logged. The Audit Trail/System Access Log must be reviewed regularly, exception reports generated and inspected by the System Administrator and appropriate action taken. A copy of the report of unauthorized access attempts must be produced and kept for future reference.

#### **8.1.5 Enforcement**

The University considers any breach of security to be a serious offence and reserves the right to copy and examine files or information resident on or transmitted via the University's information technology resources. Students deemed to be in breach of security are subject to disciplinary action. Faculty and staff deemed to be in breach of security is subject to disciplinary action available under legal provisions. Offenders may also be prosecuted under State, Federal and International laws.

Information Technology may temporarily remove material from websites, or close any account that is endangering the running of the system or that is being reviewed for inappropriate or illegal use.

## **9. AWARENESS & COMMUNICATION**

It is essential that all aspects of information security, including confidentiality, privacy and procedures relating to system access, should be incorporated into formal student, faculty and staff induction procedures and conveyed to existing university community on a regular basis.

Each employee, on commencement of employment, should be made aware that they must not divulge any information that they may have access to in the normal course of their employment. Staff must also be made aware that they should not seek access to data that is not required as part of their normal duties. Students must be made aware that they should not attempt unauthorized access to grades, course material and other information intended to be private and confidential.

System Administrators should be properly trained in all aspects of system security prior to supporting these systems.

### **9.1 DISASTER RECOVERY**

#### **9.1.1 Data Backup**

Production servers and computers offering network share resources are backed up regularly to provide protection against hardware failures and other disasters. Backups are also rotated off-site regularly.

#### **9.1.2 Individual Data Backup**

Individual computers are not backed up by Information Technology. Furthermore, backups for shared departmental servers may not be frequent enough to satisfy all users' requirements. It is strongly recommended that users make individual backups of critical data.

#### **9.1.3 Contingency Planning**

Contingency plans specify procedures designed to:

- i) Identify and respond to disasters
- ii) Protect personnel, systems, and data
- iii) Provide critical services with all or portions of the computing facility unavailable to recover full service capability

A contingency plan based on risk analysis shall be added to this policy document when available. This plan is being developed as a CSU System-wide effort.

## **9.2 SECURITY AWARENESS & TRAINING**

Regular meetings at various management and user levels are held at which current and pending security issues such as internal security bulletins, recently discovered exploits and measures, CERT incident reports are discussed and reviewed, and new potential risks are identified and planned for.

Users are required to follow security publications and to make use of all security resources (such as mailing list subscriptions and notification services) in order to keep abreast of pertinent security issues in their areas of expertise. Information Technology will host valuable information on Information and System security on its website. The website is updated frequently.

## **10. POLICY MANAGEMENT & REVISION**

Formulation and maintenance of the security policy is the responsibility of the CIO and the Information Security Officer, Information Technology.

This policy will be evaluated as appropriate by the CIO and senior management in consultation with Information Technology, and be revised if necessary.