PROCEDURE FOR POLICY 1.13 – Computing, Technology & Information Resources

Procedures Relating to Security and Privacy of Computing, Information and Technology Resources

1. The university employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that the university does not guarantee such security. Users should always engage in "safe computing" practices such as establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

2. The university shall disclose any breach of the security of an information system, following discovery or notification of the breach in the security of the system, to any individual whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the information system.

3. Users should be aware that their uses of university computing resources are not completely private. While the university does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service.

4. For software licenses held by the university, ITS will provide information and clarification around issues of compliance. For all end user or departmentally deployed software, the end user or department is responsible for ensuring compliance.

5. Any computer or network security incident that potentially involves criminal activity shall be reported to Campus Community Police.

6. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

RESPONSIBILITIES

7. Everyone who connects a computer to university computing resources has the potential to affect the security of those resources. Everyone must therefore share the responsibility for security. Every employee, contractor, or other worker must understand the university's policies and procedures about Information Security, and must perform his or her work according to such policies and procedures. Any person, group, or custodian accessing university information must recognize the responsibility to preserve the security and confidentiality of this information. Such information shall be used only for conducting university business or as appropriately authorized. Security controls may not be bypassed.

Specific responsibilities are as follows:

7.01 **Information Technology Services (ITS)**

ITS shall be responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information systems' security standards, guidelines, and procedures. While responsibility for information systems security on a day-to-day basis is every employee's duty, specific guidance, direction, and authority for information systems security is centralized for all of the university in ITS. Accordingly, ITS will advise on policy and practices, perform information systems risk assessments, prepare information systems security action plans, evaluate information security products, and perform other activities necessary to assure a secure information systems environment.

7.02 **Unit Heads**

Unit Heads, including Directors, are responsible for ensuring that security policy is implemented within the unit. These duties may be delegated; however, it is the responsibility of the head to:

- Ensure that unit employees understand security policies, procedures, and responsibilities;
- Provide and maintain safeguards for computing resources within his/her authority, consistent with policies and standards as defined by ITS;
- Approve appropriate data access, allowing staff to complete business-related assignments;
- Review, evaluate, and respond to all security violations, and take appropriate action which includes reporting incidents to ITS where circumstances require;
- Communicate to appropriate campus and university departments when employee departures, arrivals, and changes affect computer access;
- 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/unit;
- Provide ITS with the names, e-mail addresses and telephone numbers for at least two different contacts: a primary technical contact (usually a System Administrator); and a supervisor contact.

7.03 **System Administrators**

"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 others the responsibility may be shared by several individuals. If an administrator is not designated, the owner of a computer must assume the responsibilities of a System Administrator, or ensure, in collaboration with ITS and the Unit Head, that a System Administrator is designated.

System Administrators will:

- Endeavour to protect the communication networks and computer systems for which they are responsible consistent with policies and standards as defined by ITS;
- Ensure that systems they administer are operated in accordance with all applicable Information Security Standards and Policies;
- Co-operate with ITS in addressing security problems identified by network monitoring;
- Address security vulnerabilities identified by ITS scans deemed to be a significant risk to others;
- Report significant computer security compromises to ITS.

Unit-level responsibility for security of computing and communication systems rests with the System Administrators who manage those systems, or those who assume the responsibilities of a System

Administrator. ITS will help systems administrators carry out these responsibilities to the extent possible with available resources.

7.04 **Other Technical Administrators**

Others with access to computing resources which involve maintaining electronic administrative systems, applications, or data are responsible for implementing and maintaining a level of security consistent with that defined by ITS. Whenever information is maintained only on a personal computer, the user of that computer is necessarily also responsible for that information. The ultimate responsibility for this system lies with the Unit Head.

7.05 **Individual Users**

Individual users of computing resources must:

(a) Be familiar with, understand, and comply with relevant laws, policies, and procedures governing their use of the university's computing resources;
(b) When engaging in electronic communications with persons in other jurisdictions or on other systems or networks, be aware that they may also be subject to the laws of those other jurisdictions and the rules and policies of those other systems and networks;
(c) When accessing systems, electronic records, or information, ascertain what authorizations are necessary and obtain them before proceeding;
(d) Place appropriate limits on their personal use of resources, in accordance with university policy and any departmental procedures
(e) Avoid taking any action which will compromise the security of other users or place the university or the system at undue risk

REVIEWS AND UPDATES

8. The Executive Director of Information Technology Services shall, in consultation with ITS, Internal Audit, and the Senate Subcommittee on Information Technology (SUIT), review this Information Systems Security Policy no less frequently than every three years.

9. ITS shall review Information Systems Security Standards annually to ensure they result in effective and efficient protection against current risks. Revisions shall be submitted to the Senate Subcommittee on Information Technology (SUIT) for approval.

10. A contingent review shall be conducted if a significant loss occurs due to a risk that has not been adequately addressed in either Policy or Standards.

Procedures Related to Wireless Networking

1. These procedures are intended to increase the reliability and security of the wireless network access at the university and apply to all wireless networks and users of wireless networks at the university that connect to or affect the Western campus backbone network. Wireless networks are considered an augmentation of the university wired network which the university owns and manages through Information Technology Services (ITS).

RESPONSIBILITIES

2. ITS is responsible for the management of Western's wireless radio spectrum on campus. This includes responsibility for:

    - managing wireless networking services on campus.
    - management of wireless spectrum usage at Western. ITS may restrict use of any devices that can cause interference in the unlicensed radio spectrum used for wireless networking at Western.
    - scanning for rogue access points and blocking access to the Western backbone network to those that are detected.
    - maintaining a secure network and deploying appropriate security procedures.

3. Other departments may deploy wireless network access points or other wireless service on campus in coordination with ITS.

4. Private wireless access points in residences or offices are required to comply with the Western standards.

5. Encryption of wireless communications is required for all staff and faculty at the university and is highly recommended for students.

6. Any issues arising from research involving wireless networking will be resolved in co-operation with ITS, the researcher in question and/or the Vice-President (Research).

Required Security

7. Wireless network implementation at the university must be done in accordance with a security plan which must address the following issues:

    (a) Restricting network access so only authorized users can connect.

    (b) Preventing unauthorized users from viewing confidential data appearing on the wireless infrastructure, particularly passwords.

8. To the extent possible**,** all wireless users must use auto-update antivirus software and ensure that their machines are fully patched.

Procedures Related to University E-Mail

1. The university e-mail system is a vital part of the university's information technology services infrastructure. It is a service provided to support necessary communication in conducting and administering the business of the university, including teaching, research and scholarly activities. These procedures are intended to define the acceptable use of electronic mail (hereinafter “e-mail”) as a method of communication at Western, to outline responsibilities involving e-mail, and to provide guidelines for effective practices and processes to all faculty, staff, students, alumni, retirees, visiting faculty, and any others who have access to a university-assigned e-mail account. Such accounts may be centrally-assigned or assigned by a faculty or administrative unit.

2. Faculties or administrative units that establish their own e-mail accounts for the use of faculty, staff or students, shall work with Information Technology Services (hereinafter “ITS”) to ensure that mail directed to a user’s centrally administered e-mail account is properly managed.

RESPONSIBILITIES

Users

3. Since university email addresses are the property of the university and the e-mail bears identification marks of the university, users are expected to ensure that all communication is carried on in a professional, respectful, and courteous manner. Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the university unless appropriately authorized to do so.

4. In addition to complying with local legislation, and university policies and procedures, users who engage in communications with persons in other jurisdictions should be aware that they may also be subject to the laws of those other jurisdictions.

5. It is the account holder’s responsibility to retain any e-mail message or attachment that is required for ongoing purposes and to dispose of any e-mail message that is no longer required. Users should refer to the *Freedom of Information and Protection of Privacy Act* or the university’s Freedom of Information and Privacy Office for information regarding e-mail and access to information issues.

6. The unauthorized use of invalid or forged “From” addresses in an attempt to misrepresent the identity of the sender is prohibited.

7. Inappropriate or offensive e-mail, or e-mail that is fraudulent, harassing or obscene, must not be sent or forwarded, except as requested in making a complaint of inappropriate or offensive e-mail.

8. If a user receives harassing or threatening e-mail, he or she should refer to Policy 1.35, Non-Discrimination/Harassment

9. Users should be aware that the confidentiality of e-mail may be compromised by the applicability of law or policy, by unintended redistribution, or because of the inadequacy of current technologies to protect against unauthorized access. Users should exercise extreme caution in using e-mail to communicate confidential or sensitive matters.

10. Operators of e-mail services have no control over the security of e-mail that has been downloaded to a user's computer. E-mail users should employ whatever protections (e.g., passwords) that are available to them as a deterrent to potential intruders and the misuse of e-mail.

11. E-mail account holders may use their e-mail account for incidental personal purposes provided that such use does not: (1) directly or indirectly interfere with the operation of computing facilities or e-mail services, (2) burden the university with noticeable incremental cost, (3) interfere with the e-mail account holder's employment or other obligation to the university, or (4) contravene this or any other university policy or procedure. E-mail records arising from such personal use may be subject to access as described in the Access and Privacy section of these procedures.

Service Providers & ITS

12. Those responsible for maintaining university email servers are responsible for ensuring that institutional standards for security, user authentication and access control are appropriately applied. However, the security and confidentiality of e-mail cannot be guaranteed.

13. Searchable electronic address directories—some public, some private—may be maintained and populated from the e-mail addresses provided by the university. The contents of such e-mail address directories are institutional data. Faculty, staff, and students may, in special circumstances, request not to be included in public directories.

14. The university reserves the right to reject any e-mail that could compromise the university network and any systems connected to it. ITS will maintain reasonable processes to deal with e-mail containing viruses, to reject e-mail from known SPAM sites, and to scan incoming e-mail for SPAM, but the university cannot guarantee the success of such processes, and the user must accept the risk inherent in the use of the technology.

15. E-mail is backed up for purposes of disaster recovery only and not for recovery of specific items of deleted e-mail or other requests. There is no central back-up for archival purposes. Individual users are responsible for backing up any e-mail they require for ongoing purposes. The university is not responsible or liable for the content created, sent, forwarded, contained or stored in an e-mail account.

16. The university reserves the right to access e-mail records, in accordance with Procedures for Computing, Technology and Information Resources.

Procedures relating to Data Classification Standards

17. All users are responsible for classifying the data that they are using in their environment in accordance with the data classification definitions established by Information Technology Services which can be referenced here.

18. All users are subsequently responsible for protecting any University data that they require in the performance of their duties in accordance with the confidentiality of that data classification and standards of care as established by Information Technology Services which can be referenced here.