POLICY 1.20 – Computing Resources Security

Policy Category: General
Effective Date: April 28, 2005
Revised: (NEW)

PURPOSE

1.00 The University of Western Ontario Systems Computing Resources Security Policy has been created to foster an environment that will protect The University of Western Ontario and its students, staff and faculty from information security threats that could compromise the privacy, productivity, reputation, or intellectual property rights.

2.00 The rights of academic freedom and freedom of expression apply to the use of University computing resources. So, too, however, do the responsibilities and limitations associated with those rights. The use of University computing resources, like the use of any other University-provided resource and like any other University-related activity, are subject to the normal requirements of legal and ethical behavior within the University community. Thus, legitimate use of a computer, computer system, or network does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

SCOPE

3.00 The policy applies to all information systems owned by and/or operated by the University, or that are operated by agents of the University. This policy applies to all users of the University computing resources, whether affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations including all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers and other members of the University community, including those who are affiliated with third parties, who access University computer networks both wired and wireless. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific units of the University or to uses within specific units. Consult the operators or managers of the specific computer, computer system, or network in which you are interested or the management of the Unit for further information.

ACCESS TO COMPUTING RESOURCES

4.00 All individuals must only use those computing resources and data that they are authorized to use and use them only in the manner and to the extent authorized. The ability to access computing resources and data does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the University.
5.00 All individuals must comply with all Canadian, Ontario, and other applicable law; all generally applicable University rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include the laws relating to libel, privacy, copyright, trademark, obscenity, and child pornography; the University’s Code of Student Conduct; the University’s Non Discrimination/Harassment Policy; and all applicable software licenses. Users who engage in electronic communications with persons in other jurisdictions or on other systems or networks should 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. Users are responsible for ascertaining, understanding and complying with laws, rules, policies and contracts applicable to their particular uses. For software licenses held by the University, ITS will provide information and clarification around issues of compliance. For all software the user has installed on a computer, the user is personally responsible for ensuring compliance.

6.00 All individuals must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Again, ability to access other persons’ accounts does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

7.00 The finite capacity of computing resources requires that all individuals limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. The University may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

8.00 Personal use of University computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other University responsibilities, and is otherwise in compliance with this policy and other University policies. Further limits may be imposed upon personal use in accordance with normal departmental procedures.

9.00 The campus data network is a shared facility with decentralized decision making. Within multi-user computing systems and communications networks, actions by one user can compromise security of other users. Members of the University are granted decision-making freedom for equipment connected to the network. This freedom is balanced by a responsibility to avoid placing others and the institution at undue risk. Information System Security Standards declared by Information Technology Services may set more stringent requirements for segments of the network involved in access to specific information systems.

INFORMATION SYSTEM SECURITY STANDARDS

10.00 In order to construct security policies that will neither be overlooked, nor ignored, it is necessary to make certain the security policy reflects realistic administrative and academic goals. Degrees of protection must be balanced against cost, convenience, risk probability, and consequences of failure.

11.00 Information Technology Services (ITS) shall declare economically efficient standards for information system security controls, which will provide effective risk mitigation, ensuring that all operations are consistent with the intent of the Code of Behavior for Use of Computing Resources and Corporate Data on information systems throughout the University. Standards shall be based on current assessments of threats in the operating environment, and shall include applicability statements. In most circumstances these policies will be developed in consultation with the University community particularly system administrators of data and computing resources.
RESPONSIBILITIES

12.00 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.

12.01 Information Technology Services (ITS)
Information Technology Services 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 the Information Technology Services department. Accordingly, the Information Technology Services Network Security Office 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.

12.02 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 information systems 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 the Network Security Office 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.

12.03 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 some of whom may be at different organizational levels. 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;
- Endeavour to employ ITS recommended practices and guidelines where appropriate and practical;
- 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 Network Security Office.

The 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.

12.04 Others

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 the Network Security Office. 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.

CAMPUS SECURITY

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

SECURITY AND PRIVACY

14.00 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.

15.00 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 subject 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.

16.00 Users should also 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 rendition of service. The University may also specifically monitor the activity and
accounts of individual users of University computing resources, including individual login
sessions and communications, including email, without notice, under any one or more of the
following circumstances:

(a) the user has voluntarily made them accessible to the public, as by posting to
news groups or the web;
(b) it reasonably appears necessary to do so to protect the integrity, security, or
functionality of university or other computing resources or to protect the
university from liability;
(c) there is reasonable cause to believe that the user has violated, or is violating,
this policy;
(d) an account appears to be engaged in unusual or unusually excessive
activity, as indicated by the monitoring of general activity and usage patterns
(e) it is otherwise required or permitted by law or University Policy.

17.00 The University, in its discretion, may disclose the results of any such general or individual
monitoring, including the contents and records of individual communications, to appropriate
University personnel or law enforcement agencies and may use those results in appropriate
University disciplinary proceedings.

ENFORCEMENT

18.00 Violation of this policy or associated guidelines, standards or procedures established by The
University may result in the temporary or permanent loss of access privileges. Violations of
other policies, laws or terms of employment which may occur through the use of University
computing resources are subject to all sanctions applicable under such policies, laws or
terms of employment.

REVIEW AND UPDATE PROCESS

19.00 The Director of Information Technology Services shall, in consultation with the Network
Security Office, Internal Audit, and the Senate Subcommittee on Information Technology,
review this Information Systems Security Policy no less frequently than every three years.

20.00 The Network Security Office 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 for approval.

21.00 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.

QUESTIONS

22.00 Questions relating to this policy may be directed to the Network Security Office, Information
Technology Services.