8.8.1 Introduction

8.8.1.1 Application

A. This policy governs use of computing resources including computers and related equipment, as well as local area networks and connections to larger networks such as, but not limited to, the Internet.

B. It applies to all computing and networking resources connected to Concordia's facilities, including those owned by Concordia and those owned by individuals who have been authorized to install personal computing resources at Concordia.

C. It applies to all users of Concordia's computing resources including students, faculty, staff, alumni, and guests of the institution.

8.8.1.2 User Rights

A. Concordia honors and respects the privacy and academic freedom of its members, and strives to permit maximum freedom of use consistent with this policy.

B. Access to the information technology facilities owned and operated by Concordia, as well as personally owned resources which have been approved to be installed at Concordia, imposes certain responsibilities and obligations and is granted subject to Concordia's policy and the applicable provincial and federal laws.

C. Approval to install personally-owned resources shall be given by the administrative head of a particular organizational unit in consultation with Information Technology Services.

D. Use of Concordia's information technology facilities implies that the user has agreed to comply with and be subject to this policy.

8.8.2 Departmental Computing Facilities

Upon authorization of the President's Cabinet, a department may operate a computing facility outside of the auspices of the Information Technology Services Department.

Under such circumstances, the responsibilities delegated to Information Technology Services under this policy shall be the responsibility of the department, with the following exceptions:

1) All routable IP addresses must be obtained from Information Technology Services.
2) Any extension of the campus network infrastructure outside of individual offices, classrooms, or labs must be approved by Information Technology Services.
3) No wireless Access Point will be installed on campus without authorization from the Information Technology Services Department.
4) Information Technology Services will retain authority to audit as defined in 8.8.8.1.5 below.
5) Any publicly available network services must be approved by Information Technology Services.

8.8.3 **Appropriate Use**

8.8.3.1 Purpose of Use

Computing resources are to be used

1) for the institution's programs of instruction, research, communications, and the official work of the offices, departments, and recognized organizations of Concordia and its corporately approved external affiliations;
2) to fulfill the usage privileges identified in the contractual obligations of Concordia to its employees.

8.8.3.2 User Responsibility

Users are responsible for ensuring that computing resources are used in an effective, ethical, and legal manner. Users have a responsibility not to abuse the network and resources, and to respect the privacy rights of others.

8.8.3.3 Appropriate Use Guidelines

1) Computing resources are provided for everyone's use. Any activity that adversely affects the overall availability of resources is considered an abuse of these resources.
2) Any activity that knowingly compromises the security of the network or the security of other computers on the Internet is prohibited.

8.8.4 **Privacy**

A. In general, information stored on institutional computers is considered confidential, whether protected or not, unless the owner communicates that such information is available to other individuals or groups.

B. Information Technology Services may observe traffic in the normal course of their responsibilities for the administration and protection of computing and networking systems. The contents of all traffic observed will be held in strict confidence by Information Technology Services except when it becomes necessary to investigate breaches of security or policy. Any information that becomes known in these processes will be shared only on a need-to-know basis within the confines of the investigation.

C. Concordia reserves the right to copy, remove, inspect, or otherwise alter data files, system resources, or user files in the regular conduct of its duty to maintain computing facilities. However, in all cases, all individual privileges and rights to privacy will be preserved to the greatest extent possible.

D. If a user encounters or observes a potential breach or discontinuity in system or network security, the user must report the problem to the Information Technology Services Department.

8.8.5 E-mail – Security and Monitoring

A. Users should never consider electronic communications either private or secure unless appropriate encryption measures are taken.

B. Messages sent to nonexistent or incorrect user names may not be returned directly to the user but are delivered to a person designated as the Postmaster for either the remote or local site.

C. Users should not engage in an unsolicited mass distribution of any commercial e-mail.

D. The transmission or link to any communication where the meaning of the message, or its transmission or distribution would violate any applicable law or regulations, including those which deal with obscene or harassing material, is prohibited.

8.8.6 Security of Data

8.8.6.1 Concordia Commitment

Concordia attempts, to the best of its ability, to maintain a secure and constantly available system. Scheduled down-times are announced, but there will always be the chance of unforeseen system failures.

8.8.6.2 User Responsibility

1) An Information Technology Services user account is for use only by the person to whom it is assigned. A user having any computer account is responsible for the use made of that account.
2) The ultimate responsibility for the security and confidentiality of programs, data, and other information rests with the users. Therefore, users must understand and use the security features of their computing environment.
3) Each user is expected to make correct and sufficient use of the security and confidentiality tools provided for each computer system.
4) Each user is expected to maintain security and confidentiality in appropriate ways such as:
   - Keeping passwords and other types of authorization secure.
   - Selecting a strong password (i.e. alpha-numeric with upper and lower case characters) and changing it frequently.
   - Understanding the level of protection each computer system automatically applies to data files and supplementing it, if necessary, for sensitive information.
   - Being aware of computer viruses and other destructive computer programs, and taking steps to avoid being a victim or carrier.
   - Ensuring that important data is backed up.

8.8.7 **Liability – Concordia Responsibility**

Network performance, connectivity, and data retention is not guaranteed. Concordia will use reasonable efforts to ensure that those portions of the service over which the institution has direct control are functioning properly. Concordia is not responsible for any loss a user suffers, or any party claiming through or under a user, arising out of the use of network services or inability to use the services, or loss of information.

8.8.8 **Software**

8.8.8.1 Licensing

1) The Information Technology Services Department maintains software licenses for software that is provided on institution-owned computing resources. Additions, removal, or transfer of such software without authorization is prohibited.
2) Intentional ownership or possession of illegal or damaging software constitutes violation of this policy.

3) A user must not attempt to decrypt or translate encrypted material, or obtain system privileges to which they are not entitled.
4) Users are responsible for ensuring that they are in compliance with license agreements before downloading or distributing software or other copyrighted materials.
5) Information Technology Services has the authority to conduct an inventory of all software residing on any computing equipment covered by this policy.
6) User-installed software must have a valid license. The license must be retained by the user and available for audit purposes.

8.8.8.2 Support

The Information Technology Services Department only supports software purchased by the institution under the advisement of Information Technology Services.

8.8.8.3 User Responsibility

A user who installs software is responsible for ensuring that the provisions of the licensing agreement were abided to. Although subject to audit of the license by Information Technology Services, the ultimate responsibility will reside with the user.

8.8.9 **Off-campus Use**

8.8.9.1 Approval Process

Under certain circumstances, a member of Concordia may be provided Concordia-owned computing equipment for Concordia-related work at the individual's residence (At-Home Computer). Under these circumstances, the following guidelines shall apply:

1) The request for an At-Home Computer shall be made in writing to the Academic Dean, Vice-President, or President as appropriate.
2) Upon approval, Information Technology Services shall be notified.
3) Information Technology Services shall record any Concordia-owned licenses on the equipment and retain the information for future use. A copy shall be provided to the user.
4) Information Technology Services shall remove any confidential or non-required data or software from the equipment.

8.8.9.2 User Responsibility

1) The user shall ensure that any Concordia data on the equipment is maintained in a secure manner.
2) The user is responsible to ensure that the integrity of any Concordia-licensed software is maintained.
3) All other user responsibilities as defined in this policy shall apply.

8.8.10 **Sale or Disposal of Computing Equipment**

Any computer owned by Concordia and subject to disposal or sale must be processed by Information Technology Services, which, in turn, will remove all Concordia-licensed software and any Concordia data from the equipment.

8.8.11 **Access and Authorization of Use**

8.8.11.1 Access and Authorization

1) Computing access is automatically issued to new students in university-level programs upon enrollment.
2) Staff members can obtain access to Information Technology Services by contacting the Information Technology Services Department.

8.8.11.2 Extent of Services

Information Technology Services user accounts provide:

1) Electronic mail facilities.
2) Personal disk space on Information Technology Services file servers.
3) Logon access to general-purpose logon computers.
4) Access to the Internet.
5) Support for personal and departmental web pages.

8.8.11.3 Termination

1) When an individual ceases to be a member of the Concordia community, the individual's computer accounts may be deleted without notice. Prior to account deletion, files owned by the university will be transferred to active accounts. It is the

responsibility of individual owners of files to request any other legitimate transfer of files.

2) Employees retiring from Concordia may register to use computer and network accounts subject to any copyright or licensing requirements. At the discretion of faculties and departments, retired employees may also be registered for access to computing facilities. In all cases, the retired employee must abide by the policies and procedures adopted by Concordia.

8.8.11.4 Wireless Access

No wireless access point will be installed on campus without authorization from the Information Technology Services Department.

8.8.12 **Investigation of Abuses of Computing Privileges**

A. System administrators of the Information Technology Services Department have the responsibility to take remedial action in the case of suspected abuse of computing privileges. Information Technology Services reserves the right to suspend or modify user computer access privileges, examine files, passwords, accounting information, printouts, and any other material that may aid in an investigation of suspected abuse.

B. Concordia reserves the right to withhold access to the computer facilities provided to individuals if there are reasonable grounds to suspect that their continued access to the facilities would pose a threat to the operation of the facilities or the good name of Concordia, or if the use is expected to violate the principles of appropriate use.

C. Whenever reasonably possible, user cooperation and agreement will be sought in advance.

8.8.13 **Disciplinary Measures**

Inappropriate conduct and violations of this policy are subject to discipline, which may include revoking of account, disciplinary action as described within each relevant Handbook, and/or legal action.