Computer Use Policy and Procedures
Taken directly from University of Manitoba Governing Documents

Policy Use of Computer Facilities

Effective Date: January 25 , 2005
Review Date: January 25 , 2015
Approving Body: Board of Governors
Authority:
Implementation: President delegated to the Vice-President (Administration)
Contact: Vice-President (Administration) or Executive Director, Information Services Technology (IST)
Applies to: See List Below

This policy applies to:

(a) Board of Governors members
(b) Senate members
(c) Faculty/School Coucils
(d) Students
(e) External Parties Sponsored users
(f) All Employee groups

1.0 Reason for Policy

1.1 Access to University networks and computing facilities is necessary for academic staff, support staff and students to do their work and accordingly this policy is necessary to ensure the integrity and availability of these resources.

1.2 This policy defines responsibilities and obligations for all users of all computer systems and networks owned and operated by the University of Manitoba.

2.0 Policy Statement

The use of University computer systems and networks imposes certain responsibilities and obligations on users of the facilities. Such use is granted by the University of Manitoba subject to compliance with University policies and procedures as well as with local, provincial and federal laws.

2.1 **Responsibilities**

2.1.1 Information Services and Technology (IST) Responsibilities:

To provide assurance of consistent equitable service, IST is responsible for:

(a) The safety, integrity and security of University owned and operated systems and networks;

(b) Coordinating the investigation of alleged unauthorized use of University computer systems and network under the authority of the Vice President (Administration);

(c) Providing current security information and anti-

virus updates to the University community and where possible installing these updates on machines connected to the campus network automatically via the network; and

(d) Periodically informing and reminding the University community of current procedures to be followed to ensure the integrity of University computing and networking facilities.

2.1.2 Users Responsibilities

To provide equitable access and employment of University owned and operated systems and networks, users have a responsibility to:

(a) Use resources only for authorized purposes as defined by the University;

(b) Protect their userid (is the access word assigned to each user of the University systems by IST) password and system from unauthorized use. Users are responsible for all activities on their userid that originate from their system with their knowledge.

(c) Access only information that is their own, that is publicly available or to which they have been explicitly granted access by the owner of the information;

(d) Comply with local, provincial and federal laws;

(e) Comply with system security mechanisms;

(f) Use only legally licensed versions of copyrighted software or copies of documents and media in compliance with terms and conditions of any vendor licensing agreement, copyright or sale terms and conditions;

(g) Comply with all University policies regarding intellectual property;

(h) Ensure that systems under their control have current security updates and anti-virus software installed regardless of ownership of the equipment;

(i) Engage in ethical workplace behaviors reflecting:

(i) academic honesty;

(ii) acceptable language of discourse;

(iii) restraint in the consumption of shared resources by refraining from monopolizing systems and/or overloading networks with excessive data or activity, degrading services, or wasting any other related resource;

(iv) respect for intellectual property and ownership of data; and

(v) respect for individual rights to privacy and freedom from harassment in such forms as intimidating, disrespectful or obscene messages,

jokes or images.

3.0 Accountability

3.1 University Secretary for initiating a formal review of this Policy and Secondary Documents.

3.2 Responsibility for investigating alleged unauthorized use of University computer systems and network lies with IST under the authority of the Vice President (Administration).

4.0 Secondary Documents

4.1 The Vice-President (Administration), in consultation with the President, may approve Procedures which are secondary to and comply with this Policy.

5.0 Review

5.1 Formal Policy reviews will be conducted every ten (10) years. The next scheduled review date for this Policy is January 25, 2015.

5.2 In the interim, this Policy may be revised or rescinded if:

(a) the Approving Body deems necessary; or

(b) the relevant Bylaw, Regulations or Policy is revised or rescinded.

5.3 If this Policy is revised or rescinded, all Secondary Documents will be reviewed as soon as reasonably possible in order to ensure that they:

(a) comply with the revised Policy; or

(b) are in turn rescinded.

6.0 Effect on Previous Statements

6.1 This Policy supersedes the following:

(a) all previous Board/Senate Policies, Procedures, and resolutions on the subject matter herein;

(b) all previous Administration Policies, Procedures, and directives on the subject matter contained herein; and

(c) Policy 238: Use of Computer Facilities.

Procedure: Use of Computer Facilities

Effective Date: January 25, 2005
Review Date: January 25, 2015
Approving Body: President
Authority: Policy: Use of Computer Facilities
Implementation: Vice-President (Adminstration)
Contact: Executive Director of Information Services Technology (IST)
Applies to: Students, External Parties [Sponsored Users], and Employees [All Employee Groups]

1.0 Reason for Procedures

To enforce policies defining responsibilities of users and appropriate use of all computer systems and networks owned and operated by the University of Manitoba.

2.0 Procedures

2.1 **Authorized use**

2.1.1 Authorized use includes University purposes associated with:

(a) Teaching and learning support

(b) University approved research including graduate theses

(c) Community services in furtherance of or related to the above

(d) Administration of the University

(e) Outside professional activity in accordance with University policy

2.1.2 Users may use their computers and network accounts for non-University matters except where such use would be prohibited by this or other University policy or where such use unreasonably interferes with academic uses, job performance, or system performance/operations.

2.2 **Unauthorized use**

2.2.1 Unauthorized use of University owned computer systems and networks includes:

(a) Use of or access to another person's system, userid, password, files, email or other data without that person's permission unless authorized by the Vice-President (Administration);

(b) Attempting to circumvent security facilities on any system or network or failing to keep security on University owned equipment current;

(c) Engaging in any activity that might be purposefully harmful to systems or to any data stored thereon;

(d) Placing any destructive or nuisance programs such as viruses or worms into a system or network;

(e) Sending fraudulent, harassing, threatening or obscene messages;

(f) Transmitting commercial advertisements, solicitations or promotions for any other commercial purpose not authorized by the University administration;

(g) Intentionally accessing or collecting pornography or other material inappropriate to a public workplace except when such collection is necessary for a research project approved by the University Ethics Committee;

(h) Sending unauthorized bulk email (spam);

(i) Using the system to excess in non-University related activities;

(j) Using the systems or networks for personal financial gain, excluding outside professional activity as defined above;

(k) Unauthorized use of the "University" name; and

(l) Engaging in any other activity that does not comply with the above policy.

2.3 **Consequence of unauthorized use**

2.3.1 Persons found to have used University owned and operated computer systems and networks for unauthorized purposes are subject to University discipline up to and including dismissal/expulsion and/or any other action in accordance with applicable University governing documents and collective agreements.

2.3.2 In cases of financial loss to the University, restitution may be sought.

2.3.3 IST may disconnect any machine connected to a University operated network, including faculty owned computing and networking equipment which does not have current security facilities installed and which could jeopardize the integrity and operation of the University network.

2.3.4 Ignorance of the Policy: Use of Computer Facilities or these Procedures is not an excuse for non-compliance.

2.3.5 To ensure consistency of application, investigation

of unauthorized use is the sole responsibility of IST to coordinate under the authority of the Vice President (Administration). When unauthorized use is suspected, you should contact either:

(a) Computer Security Coordinator, IST;

(b) abuse@umanitoba.ca; and

(c) Security Services, Director.

3.0 Accountability

3.1 The University Secretary is responsible for notifying the contact person for this Procedure when a formal review is required.

3.2 The Executive Director of Information Services and Technology is responsible for the communication, administration and interpretation of this procedure.

4.0 Review

4.1 Formal Procedure reviews will be conducted every ten (10) years. The next scheduled review date for these Procedures is January 25, 2015.

4.2 In the interim, this/these Procedure(s) may be revised or rescinded if:

(a) the Approving Body deems necessary; or

(b) the relevant Bylaw, Regulation(s) or Policy is revised or rescinded.

5.0 Effect on Previous Statements

5.1 These Procedures supersede the following:

(a) all previous Board/Senate Procedures, and resolutions on the subject matter contained herein;

(b) all previous Administration Procedures, and resolutions on the subject matter contained herein; and

(c) Policy 238: Use of Computer Facilities.