UNIVERSITY OF MANITOBA

UNIVERSITY OF MANITOBA
PROCEDURES

Procedure:	**USE OF COMPUTER FACILITIES**
Parent Policy:	Use of Computer Facilities Policy
Effective Date:	January 25, 2005
Revised Date:	November 20, 2013
Review Date:	November 20, 2023
Approving Body:	President
Authority:	
Responsible Executive Officer:	Vice-President (Administration)
Delegate:	Chief Information Officer, Information Services Technology
Contact:	IT Security Coordinator, Information Services Technology
Application:	Board of Governors members, Senate members, Faculty/School Councils, Students, External Parties (Sponsored Users), and All Employee Groups

Part I
Reason for Procedure

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

Part II
Procedural Content

Authorized Use

2.1 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; and

(e) Outside professional activity in accordance with University Policy.

2.2 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.

Unauthorized Use

2.3 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.

Consequences of unauthorized use

2.4 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.

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

2.6 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.

2.7 Ignorance of the Use of Computer Facilities Policy and Procedure is not an excuse for non-compliance.

2.8 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.

Part III
Accountability

3.1 The Office of Legal Counsel is responsible for advising the Vice-President (Administration) that a formal review of this Procedure is required.

3.2 The Chief Information Officer is responsible for the implementation, administration and review of this Procedure.

3.3 Board of Governors members, Senate members, Faculty/School Councils, Students, External Parties (Sponsored Users), and all Employee Groups are responsible for complying with this Procedure.

Part IV
Review

4.1 Governing Document reviews shall be conducted every ten (10) years. The next scheduled review date for this Procedure is November 20, 2023.

4.2 In the interim, this Procedure may be revised or repealed if:

(a) the Vice-President (Administration) or Approving Body deems it necessary or desirable to do so;

(b) the Procedure is no longer legislatively or statutorily compliant;

(c) the Procedure is now in conflict with another Governing Document; and/or

(d) the Parent Policy is revised or repealed.

Part V
Effect on Previous Statements

5.1 This Procedure supersedes all of the following:

(a) Policy 238: Use of Computer Facilities;

(b) all previous Board of Governors/Senate Governing Documents on the subject matter contained herein; and

(c) all previous Administration Governing Documents on the subject matter contained herein.

Part VI
Cross References

6.1 This Procedure should be cross referenced to the following relevant Governing Documents, legislation and/or forms:

(a) Use of Computer Facilities Policy;

(b) Intellectual Property Policy;

(c) Access and Privacy Policy; and

(d) Access and Privacy Procedures.