UNIVERSITY OF MANITOBA

UNIVERSITY OF MANITOBA
POLICY

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

Part I
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.

Part II
Policy Content

Policy Statement

2.1 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.

Responsibilities

2.2 **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.

2.3 **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.

Part III
Accountability

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

3.2 The Chief Information Officer, Information Services Technology (IST) is responsible for the implementation, administration and review of this Policy.

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

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

Part IV
Authority to Approve Procedures

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

Part V
Review

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

5.2 In the interim, this Policy may be revised or repealed if:

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

(b) the Policy is no longer legislatively or statutorily compliant; and/or

(c) the Policy is now in conflict with another Governing Document.

5.3 If this Policy is revised or repealed, 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 repealed.

Part VI
Effect on Previous Statements

6.1 This Policy 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 VII
Cross References

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

(a) Use of Computer Facilities Procedure;

(b) Intellectual Property Policy;

(c) Access and Privacy Policy; and

(d) Access and Privacy Procedure.