ACCEPTABLE USE OF UNIVERSITY INFORMATION TECHNOLOGY RESOURCES

No: ____

Date: August 2, 2004
(Originally “Computer Use Policy and Guidelines” established in June 1995 and S-49.5 Software (Microcomputer) Use adopted in December 1997)

Authority: Regent Policy 97-2 (adopted 6/6/97)
UWM Administration

I. PURPOSE OF THE POLICY

UWM provides access to computers, databases, electronic mail, the Internet, software, and other information technology (IT) resources (University IT Resources) to its faculty, staff and students as well as community members in order to facilitate the pursuit of excellence in the University’s missions of scholarship, learning, teaching, research, and service. To preserve access to University IT Resources for the entire community, each resource user must know and comply with the institutional and external standards for acceptable use of these shared resources. The following policy is intended to foster ethical and amicable learning and working environments and to meet the requirements governing use of university resources.

II. GENERAL GUIDELINES AND SCOPE OF POLICY

University IT Resources are owned by UWM. Access to University IT Resources is a privilege conditionally granted to University IT users. This privilege includes the responsibility to use IT Resources for University-related academic, research, service, or employment activities and responsibilities. The University reserves the right to determine whether any particular use or level of use constitutes an inappropriate use.

This policy applies to all University IT Resources users. “User” is defined as any individual who uses, logs into, copies, attempts to use or log into, connects to, or attempts to connect to University IT Resources.

III. USER RESPONSIBILITIES
A. **Authorized Use**
UWM provides authorization for use of University IT Resources to each individual user for his or her own use. No person may use an authorization that belongs to another user. Users must protect the confidentiality of their personal identification codes and passwords and are expected to exercise reasonable care and common sense to insure that others cannot use their accounts or otherwise obtain access to their authorization for use of University IT Resources.

B. **Responsible Use of Resources**
All users are expected to avoid waste of limited resources. Such waste includes, but is not limited to, storage of disk files, careless execution of intensive programs, transfer of large amounts of data between computing systems during standard business hours (which degrades the performance of networks), the downloading of unlicensed programs or programs found on the Internet, and generation of excessive printer output or electronic mail.

C. **Incidental Personal Use**
Access to University IT Resources carries with it the responsibility for ensuring that the use of these resources is primarily for University purposes and University-related activities, and for maintaining the integrity and security of the University IT Resources. In the interest of making the use of University IT Resources a natural part of the day-to-day work of all members of the University community, incidental personal use is accepted. Nevertheless, one should use non-University sources of e-mail, internet access, and other information technology services for activities of an extensive or recurring nature that do not serve University purposes. For the security of the IT system, individuals having access to University IT Resources must take reasonable care to insure that unauthorized persons are not able to use their access to the system.

D. **Interference With University IT Resources**
Uses that interfere with the proper functioning of the University’s IT Resources are prohibited. Such inappropriate uses include, but are not limited to, inserting viruses into computer systems, sending e-mail spam or chain letters, destroying another user’s files, using software tools that attack University IT Resources, violating security standards, harassing other users (which includes exposing other users to materials that are perceived as offensive or excessive), misrepresenting yourself in any email message or posting, and breaking into, or attempting to obtain authorization to, University IT Resources for which a user does not have authorization.
E. **Malicious Activity**

Users may not alter or intentionally damage University’s IT Resources or interfere with another user’s authorized access to University IT Resources. Users may not unreasonably disrupt or impair University IT Resources in any manner.

F. **Commercial and Political Activities**

Users may not use University IT Resources to promote or solicit sales for any goods, services, unauthorized charities, or other contributions unless such use conforms to UWM rules and regulations governing the use of University resources or unless such a user is employing University IT Resources on behalf of a student organization recognized by the University. University employees may not use University IT Resources to solicit donations for a political campaign external to UWM. No one may use University IT Resources to promote or advance the interests of any for-profit non-University entity, group or organization for commercial purposes unless authorized by the Office of University Relations and Communications. See section III.H for cites to the laws, regulations and policies at issue in this section III.F.

G. **Software Use and Creation**

UWM prohibits the illegal duplication or unlicensed use of software on University IT Resources.

The University legally holds licenses for the use of software from many vendors and developers, but does not own the software or the related documentation. Unless specifically authorized by the vendor or developer, no one has the right to copy such software or its documentation, even if the use is for an educational purpose.

All users must use software only in accord with the applicable license agreement.

All users seeking to use personally owned software on university computers must maintain ownership documentation for that software at the site where the computer is normally located and to provide such documentation upon request. Personally owned software may be used on University computers only if its use does not interfere with any University IT Resources.

It is the policy of the UW System that, “…ownership of software created as a consequence of individual scholarship be vested with the creator. If the software is created under the sponsorship of a grant or contract, the ownership should be defined before the project is undertaken. If the software development is a joint effort (i.e., faculty and graduate students) the rights of ownership should be defined before the project begins. If the software is developed by an employee hired for that purpose, the software is owned by the University.”
H. **Laws and Policies**

Users may not use University IT Resources in a manner that violates federal or state laws or regulations or UW System or UWM policies including those listed in the Appendix.

IV. **ADMINISTRATIVE ACCESS AND MONITORING OF UNIVERSITY COMPUTERS**

The same principles of academic freedom and privacy (including the high level of confidentiality that researchers promise to their human subjects) that have long been applicable to written and spoken communications in the University community apply also to electronic information. UWM respects diversity of perspectives at this campus, and accordingly, does not condone either censorship or the unauthorized inspection of electronic files.

Users should also be aware that their uses of University IT Resources are not private. Although the University does not routinely monitor individual usage of its University IT Resources, the normal operation and maintenance of University IT Resources require the backup of data and communication records, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary to serve users and customary for any owner of IT-related resources.

Consistent with the constraints of confidentiality, the University may inspect files stored on any University IT Resources or monitor usage when there is cause to believe a user has violated the law or a UW System or UWM policy, or to defend a civil or criminal claim filed against the University. Monitoring related to such a violation must be authorized in advance by the Chief Information Officer (CIO) or by the CIO’s designee (www.oit.uwm.edu) in consultation with the Office of Legal Affairs. For faculty, notification to the University Committee is also expected. For Academic Staff, notification to the University Committee is also expected. Such monitoring will be conducted with notice to the user, unless, after consultation with the Office of Legal Affairs, it is determined that notice would seriously jeopardize substantial interests of the University or of third parties. In addition, if a supervisor deems it necessary to retrieve a non-networked file of assigned work from the computer of an employee who is unavailable for timely consultation, the supervisor should attempt to notify the CIO’s office or the Office of Legal Affairs, and the CIO’s office or the Office of Legal Affairs shall verify that such retrieval is essential and that the employee is indeed unavailable. For faculty, notification of the department executive committee (or designee) is expected. If the Office of Legal Affairs or the CIO’s office cannot be contacted in a timely manner, the supervisor, or the executive committee designee, may retrieve the work from the employee’s computer, but the supervisor may only retrieve the file in the presence of a witness so as to ensure that the supervisor’s actions do not extend beyond retrieval of a work file.
Users should be aware that their electronic records may be subject to the University’s obligation to respond to subpoenas or other court orders, reasonable discovery requests, internal audits, and requests for documents pursuant to the Wisconsin Public Records Law, §19.31 et al. Users should also be aware that, under state law, their stored files or usage of University IT Resources may be inspected in conjunction with a workplace misconduct investigation.

V. VIOLATION OF POLICY

A. Violations by Employees

Reports of violations of this policy by employees may be made to the CIO at (414) 229-1122 or to the employee’s supervisor. The person to whom the report is made should contact the Office of Legal Affairs at (414) 229-4278 or University Police at (414) 229-4627 if the report potentially involves illegal conduct.

The party to whom the violation was reported shall then notify the employee’s dean or director of the potential violation, and the dean or director shall work with the Provost’s Office, the CIO and the University Committee, the Academic Staff Committee or the Department of Human Resources, depending on the employee’s classification, in order to investigate the report and issue an appropriate sanction.

Discipline imposed for a violation of this policy shall be done only in conformance with other existing University rules and policies. In the event emergency circumstances require immediate disciplinary action, administration will consult with the applicable governance groups.

Faculty members may appeal disciplinary action brought under this policy to the University Committee for appropriate disposition or referral. Academic staff members may appeal any such disciplinary action to the Academic Staff Hearing and Appeals Committee. These committees then may make recommendations concerning the disciplinary action to the Chancellor. The decision of the Chancellor regarding disciplinary action related to this policy shall be final.

Classified staff members may appeal disciplinary action brought under this policy via the grievance process outlined in the collective bargaining agreement.

B. Violations by Students

Reports of violations of this policy by students may be made to the Office of Student Life at (414) 229-4632 or the CIO at (414) 229-1122. If the violation potentially involves illegal conduct, the Office of Student Life and/or the CIO should so notify the Office of Legal Affairs at (414) 229-4278 or University Police at (414) 229-4627.
The Office of Student Life and the CIO shall then work with the Provost’s Office to investigate the report and issue an appropriate sanction.

Students may appeal disciplinary action brought under this policy to the Chancellor. The decision of the Chancellor regarding disciplinary action related to this policy shall be final.

C. Sanctions

Depending on the nature and severity of the violation, users who violate this policy may lose the privilege to use University IT Resources, be subject to University discipline including termination, suspension or expulsion, and be subject to criminal prosecution.

VI. OTHER POLICIES

Individual units within the University may have supplemental written guidelines for use of University IT Resources that are under their control. Such guidelines must be consistent with this policy, but may provide additional detail, restrictions, and user guidelines. A copy of such guidelines must be filed with the Office of Information Technology and the CIO.
1. Section 17 U.S.C §101, et al., which is federal copyright law
(http://www4.law.cornell.edu/uscode/17/101.html)

2. Section 18 U.S.C. 1030, the federal law regarding fraud and related
activity in connection with computers
(http://www4.law.cornell.edu/uscode/18/1030.html)

3. Section 20 U.S.C. § 1232g, the Family Educational Rights and Privacy Act
(FERPA) (http://www4.law.cornell.edu/uscode/20/1232g.html)

4. Section 18 U.S.C. § 1462, the federal law concerning importation or
transportation of obscene matters
(http://www4.law.cornell.edu/uscode/18/1462.html)

5. Section 18 U.S.C. § 1465, the federal law regarding transportation of
obscene matters for sale or distribution
(http://www4.law.cornell.edu/uscode/18/1465.html)

6. Chapter 11, Wis. Stats., which restricts the use of state facilities for
political activities by state employees
(http://www.legis.state.wi.us/statutes/Stat0011.pdf)

7. Section 943.70, Wis. Stats., which defines and prohibits certain computer
crimes (http://www.legis.state.wi.us/statutes/Stat0943.pdf)

8. Section 948.12, Wis. Stats., which prohibits possession of child
pornography (http://www.legis.state.wi.us/statutes/Stat0948.pdf)

9. Chapter UWS 8, Wis. Admin. Code (for faculty and academic staff) and
Chapter ER-MRS 24, Wis. Admin. Code (for classified staff), which explain
ethical standards of conduct appropriate for use of one’s University
position and University resources
(http://www.legis.state.wi.us/rsb/code/uws/uws008.pdf and
http://www.legis.state.wi.us/rsb/code/er-mrs/er-mrs024.pdf)

10. Chapters UWS 14 and 17, Wis. Admin. Code, which establish standards
and disciplinary processes relating to academic and nonacademic
misconduct by students, including prohibitions on disruption of University
activities, damage to University facilities, harassment and similar matters
(http://www.legis.state.wi.us/rsb/code/uws/uws014.pdf and
http://www.legis.state.wi.us/rsb/code/uws/uws017.pdf)

11. Chapter UWS 18, Wis. Admin. Code, which governs conduct on University
lands (http://www.legis.state.wi.us/rsb/code/uws/uws018.pdf)
12. Chapter UWS 21, and UWM’s Use of Facilities Policy (Selected Academic and Administrative Policy S-23), which regulate use of University facilities (http://www.legis.state.wi.us/rsb/code/uws/uws021.pdf and http://www.uwm.edu/Dept/SecU/acad+admin_policies/S23.pdf)

13. UW System Regent Policy Document 97-2, “Policy on Use of University Information Technology Resources” (http://www.uwsa.edu/bor/rpd/bor_pols.pdf)


15. UWM Equal Employment Opportunity Policy (http://www.uwm.edu/Dept/OD_C/policies.html#eeop)

16. UWM Discriminatory Conduct Enforcement Procedures (http://www.uwm.edu/Dept/SecU/acad+admin_policies/S47.pdf)
