University of Wisconsin Milwaukee **INFORMATION SECURITY POLICY**

No: S-59
AUTHORITY: UWM Faculty Senate **DATE:** November 15, 2007

I. PURPOSE

A university is an inherently open and diverse culture that fosters scholarship and debate. It is the intent of this policy to ensure the confidentiality, integrity and availability of student, employee and institutional data in support of this culture and the University's mission of learning, research and service. This policy establishes the framework for administrative, technical and physical security safeguards for University information systems and processes that protect the institution and its community from damage to its reputation among its peers, legal sanctions and financial loss. This policy establishes the University's commitment to protecting the privacy of the records that have been entrusted to it.

II. STATEMENT OF POLICY

It is the policy of the University of Wisconsin – Milwaukee to ensure the appropriate levels of confidentiality, integrity and availability of information maintained, collected or produced by the University; to protect against any anticipated threats or hazards to such records; and to protect against unauthorized access to or use of such records or data that could result in harm or inconvenience to any individual.

It is also the University's policy that its employees act in good faith to protect the confidentiality, integrity and availability of University records[1].

This policy is accomplished by the provision of a framework of standards and practices to ensure the University's ongoing development and application of data protection efforts.

III. Procedures

A. Position Description Language

It is recommended that position descriptions affirm the employee's responsibilities with respect to confidential information. Departments should consider including language such as the following within each position description:

> "It is the responsibility of University employees to cooperate with appropriate University personnel in taking reasonable steps to secure access to and confidentiality of designated confidential records and information that they use or maintain in the course of their duties; prudently act to mitigate anticipated threats or hazards to the security or integrity of such records; and engage reasonable precautionary measures against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to the subject of the records."

B. Employee Confidentiality Notice

It is recommended that employees with access to confidential information or records be

provided with and requested to acknowledge receipt of a notice outlining campus Information Security Policies. The notice serves to outline what constitutes confidential information, describe the expectations and responsibilities relating to protecting confidential information and data, and provide an understanding of the consequences of not complying with the requirement.

C. Employee Training

It is recommended that new and existing employees receive training in the area of maintaining confidentiality of records and data, as such training relates to the employees' responsibilities. Upon appropriate consultation, deans and division heads may choose to require such training. Training resources are listed below in the Appendix.

D. Ongoing Risk Assessment and Development of Safeguards for IT Resources

Individual departments or units are responsible for comprehensively assessing and monitoring the risks to nonpublic or personal data or information associated with UWM information systems under their control or direction, including relating to: personal computers, network and server access and design, information processing, remote access, and the electronic storage, transmission and disposal of nonpublic information. Departments are encouraged to seek input from the Information Security Officer, the Information Systems Auditor, and other campus experts in assessing and monitoring such risks.

The CIO, Information Security Officer and Information Systems Auditor will, on a regular basis, develop campus-wide procedures and safeguards to help departments control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards.

E. Ongoing Risk Assessment and Development of Safeguards for Paper and Other Non-Electric Records

Individual departments or units also are responsible for assessing risks to paper and other non-electronic records and consulting with the Information Systems Auditor and other campus experts regarding recommended safeguards to manage identified risks.

F. Records Retention and Disposal

University records are not the personal property of the parties that create and maintain them, but are the property of the University and, ultimately, of the State of Wisconsin. University offices and departments thus do not have the legal authority to dispose of paper records, delete files, erase documents, or purge data elements from a records series without first ensuring that the records may be destroyed under existing records retention schedules for common records. Such policies and schedules are to be distributed annually by the Secretary of the University.

If records to be destroyed are not covered by existing records retention schedules, units and offices must secure the approval of the Public Records Board (PRB) by requesting a records retention and disposition authorization (RDA), to cover their materials. An RDA is a binding legal authority for records disposal. The records-scheduling process enables the PRB to ensure that records are preserved permanently, if they are of long-term historical value, or

are retained and disposed of in the proper manner at the correct time. The University Archives provides information and assistance in preparing records schedules to all departments and acts as a liaison between the campus and the PRB. All offices should submit proposed RDAs to University Archives for review and approval; the University Archives will then forward the records schedules to the PRB for final approval and notify offices of the status of their RDAs. For further information about records retention schedules, contact UWM's Archives Department.

In any event, University employees may not take university records home or off campus for long-term storage or destruction.

G. Disposal of Computers and Other Devices

Surplus computers and computer-related devices shall be collected and processed for disposal in a manner to ensure that the disposal is environmentally responsible and that any data is securely removed from electronic media. For more information on disposal of computers and computer-related devices, contact University Safety and Assurances.

H Unauthorized Disclosure of Personal Information of Individuals

Wisconsin law obligates UWM to take certain steps when it becomes aware that personal information maintained by UWM, including social security numbers, drivers license numbers, and financial account numbers, have been disclosed to someone unauthorized to access that information. UWM departments shall comply with the Protocol established by UWM and published by Information & Media Technologies and Internal Audit, to ensure compliance with the law. Notices of Protocol publications, locations and updates are to be distributed annually or within 30 days of modification.

IV. ADDITIONAL RESOURCES AND INFORMATION RELATING TO INFORMATION SECURITY

Additional resources and policies that are available and relate to information security at UWM are listed on the attached Appendix A. These resources are subject to change and will be updated annually by the Secretary of the University's Office.

V. SANCTIONS

Failure to comply with this policy may result in loss of access privileges, University disciplinary action, and/or criminal prosecution. The appropriate due process and policies will be followed depending upon whether faculty, academic staff, classified staff or students are alleged to be involved.

FOOTNOTE

1. Wisconsin law defines public records as documents or documentary materials, regardless of physical form, made or received by any state agency or its officers or employees in connection with the transaction of public business. See Wis. Stat. 16.61(2)(b). Public records do not include: (1) duplicate copies of materials, the original of which is also in the custody of UWM, and which are maintained for convenience or reference only; (2) notices or invitations received by UWM that were not solicited by UWM and are not related to any

official action taken, proposed, or considered by the agency; (3) drafts, notes, preliminary computations and like materials prepared for the originator's personal use or in the name of a person for whom the originator is working; and (4) routing slips and envelopes.

APPENDIX A:
ADDITIONAL POLICIES AND RESOURCES RELATING TO INFORMATION SECURITY

A. Confidentiality of Educational Records or the Family Educational Rights Privacy Act ("FERPA")

UWM provides a policy manual, online training, legal references, and other information regarding the protections afforded student educational records under FERPA on its FERPA website.
https://www4.uwm.edu/current_students/records_grades/ferpa.cfm

B. Privacy and Security of Patient Health Information or the Health Insurance Portability and Accountability Act ("HIPAA")

UWM provides policies and procedures, online training, legal references, and other information regarding the requirements for protection of patient health information under HIPAA on its HIPAA website.
http://www.hipaa.uwm.edu/

C. Protections for Financial Information or the Gramm-Leach-Bliley Act ("GLBA")

The following links provide additional information on the GLBA:

- Gramm-Leach-Bliley Statute

http://www.ftc.gov/privacy/glbact/glbsub1.htm

- Gramm-Leach-Bliley Privacy Regulations

http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html

- Gramm-Leach-Bliley Safeguarding Regulations

http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html

- Federal Trade Commission Fair Information Practice Principles

http://www.ftc.gov/reports/privacy3/fairinfo.htm

- Federal Trade Commission Guidance on Financial Privacy

http://www.ftc.gov/opa/2006/03/jointprprivacy.shtm

- Bureau of Consumer Protection Guidance on Privacy of Customer Financial Information

http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.shtm

D. Digital Millenium Copyright Act ("DMCA")

The following links provide additional information on the DMCA:

- DMCA Statute

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ304.105.pdf

- Copyright Office DMCA Summary

http://www.copyright.gov/legislation/dmca.pdf

- UWM DMCA Statement

https://www4.uwm.edu/uits/security/alerts/news_details.cfm?item_id=1562

E. USA Patriot Act

The following links provide information on the UWA Patriot Act:

- USA PATRIOT Act Statute

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

- Department of Justice USA PATRIOT Act Homepage

http://www.lifeandliberty.gov/

F. Recruitment Guidelines and Resources

The State of Wisconsin Office of State Employment Relations has developed a Recruitment Resource Guide for Classified Employees.
http://oser.state.wi.us/docview.asp?docid=1816

UWM has developed a Recruitment Guide for Faculty and Academic Staff**.**
http://www4.uwm.edu//Acad_Aff/facstaffprog/recruitmentguide.cfm

The Office of Legal Affairs publishes a guide to Legal Issues in the Recruitment Process.
http://www.uwm.edu/Dept/LEGAL/Pages/OLA_Publications/legal_issues.html

UWM is required by law to conduct criminal background checks for certain employees, including those with fiduciary responsibilities and employees/student interns in caregiver positions. Human Resources publishes a Criminal Background Check Policy.
http://www.uwm.edu/Dept/HR/refmaterial/criminalbackground/AppCrimBackgrndPolicy.doc

G. Employee Resources

UWM employee codes of conduct include:

- State of Wisconsin Employment Code of Ethics for Classified Employees

http://www.legis.state.wi.us/rsb/code/er-mrs/er-mrs024.pdf

- American Association of University Professors Statement of Professional Ethics (UWM Faculty Document 2229)

http://www.uwm.edu/Dept/SecU/facdocs/2229.pdf

- UW System Unclassified Code of Ethics (Wisconsin Administrative Code Chapter

UWS 8)
http://www.legis.state.wi.us/rsb/code/uws/uws008.pdf

Training on additional information security topics is periodically available through Professional Development Opportunities.
http://mydevelopment.uwm.edu/

H. Wisconsin Laws and Administrative Code Regulations relating to Confidentiality and Security

- Wisconsin Statutes Section 16.61, Disposition of Public Records
http://www.legis.state.wi.us/statutes/Stat0016.pdf

- Wisconsin Statutes Section 19.35 et seq, Wisconsin Public Records Law
http://www.legis.state.wi.us/statutes/Stat0019.pdf

- Wisconsin Statutes Chapter 36, University of Wisconsin System
http://www.legis.state.wi.us/statutes/Stat0036.pdf

- Wisconsin Statutes Section 943.70, Computer Crimes
http://www.legis.state.wi.us/statutes/Stat0943.pdf

- Wisconsin Administrative Code Chapter UWS 8, Unclassified Staff Code of Ethics
http://www.legis.state.wi.us/rsb/code/uws/uws008.pdf

- Wisconsin Administrative Code Chapter UWS 18, Conduct on University Lands
http://www.legis.state.wi.us/rsb/code/uws/uws018.pdf

- Wisconsin Administrative Code Chapter ADM 12, Electronic Records Management
http://www.legis.state.wi.us/rsb/code/adm/adm012.pdf

- Wisconsin Administrative Code Chapter ER-MRS 24, Classified Employee Code of Ethics
http://www.legis.state.wi.us/rsb/code/er-mrs/er-mrs024.pdf

I. UW System and UWM Policies Relating to Information Confidentiality and Security

- UW Board of Regents Policy 25-3, Use of Information Technology Resources
http://www.uwsa.edu/bor/policies/rpd/policies.pdf

- UW Board of Regents Policy 3-2, Public Records Management
http://www.uwsa.edu/bor/policies/rpd/policies.pdf

- UW System GAPP 10, Computer Software Ownership
http://www.uwsa.edu/fadmin/gapp/gapp10.htm

- UW System GAPP 11, Sharing Services and Products

http://www.uwsa.edu/fadmin/gapp/gapp11.htm

- UW System GAPP 20, Computing Acquisitions Responsibility and Authority

http://www.uwsa.edu/fadmin/gapp/gapp20.htm

- UW System GAPP 20A, Telecommunications Acquisitions Responsibility and Authority

http://www.uwsa.edu/fadmin/gapp/gapp20a.htm

- UW System GAPP 27, Copyrightable Instruction Materials

http://www.uwsa.edu/fadmin/gapp/gapp27.htm

- UW System FPP 48, Laboratory/Classroom Modernization and General Computer/Network Access

http://www.uwsa.edu/fadmin/fppp/fppp48.htm

J. Other UWM Departments, Webpages, and Resources

- UWM Security Homepage

http://www.security.uwm.edu/

- UWM Department of Human Resources

http://www.uwm.edu/Dept/HR/

- UWM Public Records Custodian

http://www.uwm.edu/Dept/Univ_Rel/records.htm

- UWM Records Management

http://www.uwm.edu/Libraries/arch/recordsmgt/index.htm

- UWM Emergency Preparedness

http://www.uwm.edu/Dept/EHSRM/EMERGENCY/

- UWM Information Security Awareness Committee

https://www4.uwm.edu/uits/security/training/index.cfm

- UWM Information Security Roles

https://www4.uwm.edu/uits/security/policies/information_security_roles.cfm