The University of Michigan-Flint
Access and Compliance
Proper Use of University Information Systems

Proper Use Policy

It is the policy of the University of Michigan-Flint to attempt to provide appropriate access to local, national, and international sources of information.
It is the policy of the university that information resources will be used by members of its community with respect for privacy and the public trust.
In accordance with the policies below, the university works to ensure that intellectual property and university records are protected from unauthorized use or distribution.

Authorized Use

As conditions of use for Information Technology Services (ITS) facilities and communication systems accessed through their use, all users agree to respect (1) the privacy of university records, (2) the legal protection provided by copyright and license agreements for programs and data, (3) the intended use for which access to the resources was granted, and (4) the integrity of the computing systems.

Appropriate Use

All users of computing resources should be mindful of the impact of their participation on the campus community, and should engage in only authorized use and should abide by standards of good citizenship in general.

Responsible Use

Users of ITS resources are expected to use those resources in a responsible and efficient manner. Users are expected to refrain from engaging in illegal, unauthorized, inappropriate, for-profit, or deliberately wasteful practices as outlined in the Standard Practice Guide.

Access and Compliance

The University of Michigan-Flint provides many information technology resources for its community. Whenever you use these resources, you implicitly agree to abide by the highest standards of responsibility to the faculty, staff, students and external users who share this environment. Users are required to comply with all state and federal laws and university policies and guidelines concerning appropriate use of information technology. Non-compliance is considered a serious breach of community standards and may result in disciplinary or legal action.

State and Federal Laws

Users of UM computing resources are subject to a number of state and federal laws.

- Family Educational Rights and Privacy Act (FERPA) http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- The State of Michigan Freedom of Information Act (FOIA) http://legislature.mi.gov/doc.aspx?mcl-Act-442-of-1976
- Federal Freedom of Information Act (FOIA) and the Federal Privacy Act of 1974 http://www2.ed.gov/policy/gen/leg/foia/foiatoc.html
- Electronic Protected Health Information (ePHI) is regulated by the Health Insurance Portability and Accountability Act (HIPAA) http://www.hhs.gov/ocr/privacy/
- Gramm-Leach-Bliley Act (GLBA) Student Loan Information http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act
- Payment Card Industry (PCI) Data Security Standards https://www.pcisecuritystandards.org/security_standards/index.php
- Social Security Number Privacy Act http://legislature.mi.gov/doc.aspx?mcl-Act-454-of-2004
- Michigan Identity Theft Protection Act, MCL 445.63 http://legislature.mi.gov/doc.aspx?mcl-445-63

University Policies and Guidelines

Users of UM computing resources are subject to a number of policies and guidelines.

Proper Use, Privacy and Security

These policies deal with protecting the rights of the community in regard to access to the information resource infrastructure, sharing of information, and security of intellectual products.

- Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan (SPG 601.07) http://spg.umich.edu/pdf/601.07.pdf
- Policy and Guidelines Regarding Electronic Access to Potentially Offensive Material (SPG 601.16) http://spg.umich.edu/pdf/601.16.pdf
- Information Security Policy (SPG 601.27) http://spg.umich.edu/pdf/601.27.pdf
- Information Security Incident Reporting Policy (SPG 601.25) http://spg.umich.edu/pdf/601.25.pdf

To report any suspected violation of information technology for UM-Flint faculty, staff, and students, please submit information via our online form at http://www.umflint.edu/its/forms/useradvocate.page

- Social Security Number Privacy Policy (SPG 601.14) http://spg.umich.edu/pdf/601.14.pdf
- Identity Misrepresentation (SPG 601.19) http://spg.umich.edu/pdf/601.19.pdf
- Privacy and the Need to Monitor and Access Records (SPG 601.11) http://spg.umich.edu/pdf/601.11.pdf
- Identification Photos; Identification and Access Control Cards (SPG 601.13) http://spg.umich.edu/policy/601.13
- Acquisition, Use and Disposition of Property (Exclusive of Real Property) (SPG 520.1) http://spg.umich.edu/pdf/520.01.pdf
- For more information consult UM-Flint FERPA privacy guidelines at http://www.umflint.edu/registrar/privacy.htm

Data Management

These policies deal with management and protection of the University of Michigan's institutional data resources.

- Institutional Data Resource Management Policy (SPG 601.12) http://spg.umich.edu/pdf/601.12.pdf
- Responsibility for Maintaining Information Technology Backup and Recovery Procedures (SPG 601.07-1) http://spg.umich.edu/pdf/601.07-1.pdf

This Standard sets expectations for compliance with respect to sensitive regulated data that fall under federal or state laws or regulations:

- Sensitive Regulated Data: Permitted and Restricted Uses http://cio.umich.edu/policy/sensitive-regulated-data.php

This Guideline sets expectations for fiduciary and stewardship responsibilities in the management of U-M information resources:

- University of Michigan Statement on Stewardship http://www.hr.umich.edu/stewardship.html

Digital Copyright

These university policies deal with use and distribution of copyrighted software programs.

- Ownership and Use of Computer Software (SPG 601.03) http://spg.umich.edu/pdf/601.03.pdf
- Management of Copyrighted Software (SPG 601.03-1) http://spg.umich.edu/pdf/601.03-1.pdf

This Digital Copyright Compliance site, http://safecomputing.umich.edu/copyright/ deals with the University of Michigan's compliance with the digital copyright protection provisions of the **Digital Millennium Copyright Act** (http://copyright.gov/legislation/dmca.pdf) and the **Higher Education Opportunity Act**(http://www2.ed.gov/policy/highered/leg/hea08/).
To report a suspected copyright violation, please consult information from the UM-Ann Arbor Information Technology (IT) User Advocate site located at http://www.umich.edu/~itua/copyright/index.html.

To learn more about using peer-to-peer file sharing safely and appropriately, visit the Be Aware You're Uploading (BAYU) website at http://www.umflint.edu/bayu/ and consult UM-Flint's ITS Helpdesk webpage http://www.umflint.edu/helpdesk/perm/students/safe-computing-copyright-issues-and-legal-downloading-2/

Additional Information

See Information Security Laws and Regulations Related to Handling Sensitive Data guide online at http://www.safecomputing.umich.edu/compliance/complianceTable.php for specific definitions and real-life examples of the regulated and sensitive data types included in the U-M standard.

The University of Michigan online Standard Practice Guide http://spg.umich.edu/.

For a complete list of all University of Michigan-Flint ITS resource policies
http://www.umflint.edu/its/policies

The University of Michigan-Flint Information Systems
Access and Compliance Statement

PURPOSE: By signing this form you certify that you have read the Access and Compliance document and that you agree to abide by the state and federal laws and university policies that apply to the proper use of data.

RESPONSIBILITY: The granting of access carries with it an implicit bond of trust that:

- You are responsible for all actions within your account. All actions can be traced back to you like a fingerprint.
- You will not allow anyone else to use your UM-Flint computer account to access or obtain access to sensitive data not within the scope of one's university responsibilities.
- You will refrain from engaging in illegal, unauthorized, inappropriate, for-profit, or deliberately wasteful practices as outlined in the Standard Practice Guide.
- You will be a responsible user of data, whether it is data relating to your own unit or another unit.
- Data that you obtain from these data sets will be stored under secure conditions.
- You will make every reasonable effort to maintain privacy of the data.
- You will make every reasonable effort to interpret the data accurately and in a professional manner.
- Prior to sharing data with others, electronically or otherwise, ensure that the recipient is authorized to access the data and understands their responsibilities as a user.
- You will sign off or lock the systems when not using them.
- You will keep passwords to yourself.
- You will store/secure/encrypt confidential and sensitive information, reports, etc. in an appropriate manner when not using them.
- You will dispose of confidential reports in an appropriate manner when done with them.
- If you suspect that your computer/cell phone/flash drive, etc... containing Personal Private Data has been compromised or has been lost/stolen you will report it to DPS at 810-762-3335 and ITS at 810-762-3123 immediately.

VIOLATIONS: Misuse of the data in or from these data sets will subject you to disciplinary action as described in Standard Practice Guide section 201.12 (Discipline-Performance and Conduct Standards) and as deemed appropriate by executive authority.

CERTIFICATION: I have read the document entitled, *Access and Compliance; Proper use of University Information Systems*, which can be found online at http://www.umflint.edu/its/documentation/Access_Comp.pdf and I understand my obligations as a responsible user of the data to which I have been granted access.

Name:_____ Uniqname: _____

Signature:_____ Date: _____

Title:_____ Department:_____