Administrative Policy Acceptable Use of Information Technology Resources

+Table of Contents

Questions?

Please use the contact section below.

Policy Statement

Computers and other Information Technology (IT) Resources (as defined below) are essential in accomplishing the University's mission. IT Resources need to be used and managed responsibly to ensure the integrity, confidentiality, and availability of those resources for the University's education, research, outreach, and administrative objectives. University community members are granted access to these resources in support of accomplishing the University's mission.

All users of University IT Resources, whether or not they are affiliated with the University, are responsible for their appropriate use. By making use of these resources, users of IT Resources agree to comply with Board of Regents policies; University administrative policies; federal, state, or local laws; and contractual obligations.

University IT Resources are provided for individuals who are enrolled, employed, or formally affiliated with the University of Minnesota. Units that grant guests access to IT Resources must make their persons aware of their acceptable use responsibilities. The University accepts no responsibility or liability for any unauthorized or personal use of its IT Resources by users.

Acceptable Use Responsibilities

Acceptable use includes respecting the rights of others, avoiding actions that jeopardize the integrity, confidentiality, or availability of IT Resources, and complying with all relevant legal or contractual requirements.

Acceptable use includes but is not limited to the following list. Users of University of Minnesota IT Resources must agree to and accept the following:

A. Comply with Applicable Laws, Regulations, and Policies

- Comply with all state, federal, and local laws, regulations, and University policies.
- Comply with all legal, licensing, and intellectual property rights, terms of service, and contractual obligations related to the IT Resources used.
- Users must understand that any records and communications they create related to University business, electronic or otherwise and regardless of whether a personally owned device or resource is used, may be subject to disclosure under the Minnesota Government Data Practices Act. If further advice is needed, consult the the Data Access and Privacy Office under the Office of the General Counsel.
- Comply with the University's records retention schedule as defined, see Appendix: *Records Retention Schedule*.

B. Appropriate Use of IT Resources

- Only use IT Resources you are authorized to use, and only in the manner and to the extent authorized. An ability to access a resource does not imply authorization to use that resource.
- Comply with all measures of security controls on all IT Resources used for University business whether University or personally owned.
- Do not share authentication credentials with other individuals, including family members, and protect authentication credentials from unauthorized use.
- Do not circumvent or attempt to circumvent security controls.
- Do not interfere with the integrity, confidentiality, and availability of IT Resources.
- Do not scan University IT Resources without authorization.
- Do not use IT Resources to harass, intimidate, or engage in inappropriate behavior.
- Do not knowingly download or install software or applications onto University IT Resources that do not follow relevant University policies, do not meet University security requirements and standards, disrupt service, or that do not have a reasonable business or academic use. See Administrative Policy: *Entering into Contracts*.
- Do not engage in widespread dissemination of unsolicited or unauthorized electronic communications.
- Do not engage in excessive use of IT Resources, including network capacity, personal use that could disrupt or delay University service, or that results in any measurable cost to the University.
- Do not resell or grant access to University IT Resources without authorization.
- Do not use IT Resources for personal commercial gain, campaigning for political candidates, or ballot initiatives that would otherwise be inconsistent in accordance with the University's tax exempt status. See Administrative Policy: *Public Service: Campaigning for or Holding Public Office*.

C. Respect the Privacy and Rights of Others

- Users must not violate the privacy and rights of others. Technical ability to access others' information or Resources does not, by itself, imply authorization to do so.

D. Safeguard University IT Resources

- All users of IT Resources are required to use security controls provided by the University, including user specific controls as defined in Administrative Policy: *Information Security*.
    - Failure on the part of the user to employ in good faith the available security controls and to secure their personal information appropriately means that the University may not reimburse the loss of misdirected salary, expense reimbursements, financial aid or any other assets.

Privacy and Security Controls

The University takes reasonable steps to protect its IT Resources; however, use of IT Resources does not guarantee absolute security and privacy. Users should be aware that any use of University IT Resources may be monitored, logged, and reviewed by University approved personnel or discovered via legal proceedings.

When the University becomes aware of violations, either through routine system administration activities or from a complaint, it is the University's responsibility to investigate; take action to protect its resources and provide information relevant to an investigation as necessary.

IT Resources are not examined or disclosed except:

- as required for routine system maintenance;
- as part of maintaining the security of University IT Resources;
- where there exists reason to believe a law or University policy is being violated; or
- as permitted by relevant policy or law.

Enforcement

Individuals who use IT Resources in a way that violates a University policy, law, regulation, or contractual agreement, or violates an individual's rights, may be subject to limitation or termination of user privileges and appropriate disciplinary action, legal action, or both. Alleged violations will be referred to the appropriate University office or law enforcement agency.

The University may temporarily or permanently restrict access to IT Resources if it appears necessary to protect the integrity, security, or continued operation of these Resources or to protect itself from liability.

Individuals or units should report non-compliance with this policy to University Information Security (security@umn.edu). To report anonymously, use the *University UReport confidential reporting system*. See Administrative Procedure: *Report Information Security Incidents*.

Units within the University may define additional conditions of use for IT Resources or facilities under their control. Such additional conditions must be consistent with or at least as restrictive as any governing Board of Regents or Administrative policy, and may contain additional details or guidelines.

Reason for Policy

The purpose of this policy is to outline the acceptable use of information technology resources at the University of Minnesota in order to:

- Comply with legal, regulatory, and contractual requirements.

- Protect the University against damaging legal consequences.
- Safeguard University Resources and the University Community.

Procedures

- *Report Information Security Incidents*

Forms/Instructions

There are no forms associated with this policy.

Appendices

- *Examples of Reportable Acceptable Use Violations*
- *Public Records: Guidelines for Electronic Communications*
- *Use of Personal IT Resources for University Business*
- *Use of Personal Mobile Devices for University Health Care Components*

Frequently Asked Questions

1. **Where to report alleged copyright infringement occurring in the umn.edu domain in accordance with the *Digital Millennium Copyright Act (DMCA) (pdf)*?**

   Send notifications to the University's designated agent in the Office of Information Technology – University Information Security.

Contacts

Subject	Contact	Phone	Email
Primary Contact(s)	**Brian Dahlin**	**612-625-1505**	**bdahlin@umn.edu**
Information Security	University Information Security	612-625-1505	security@umn.edu
Legal Advice	Office of the General Counsel	612-624-4100	ogcweb@umn.edu

Responsible Individuals

Responsible Officer

- Vice President and Chief Information Officer, Office of Information Technology

Policy Owner

- Chief Information Security Officer, Office of Information Technology

Primary Contact

- Brian Dahlin
  Chief Information Security Officer, Office of Information Technology

Definitions

Authentication Credentials

Any factor, data, or device that is used in the process of verifying identity.

Data Custodian

The University designated individual responsible for serving as a steward of University data in a particular area (e.g., principal investigator (PI)).

Data Owner

The individual with primary authority and accountability for specified information (e.g., a specific business function) or type of data (e.g., research). Where there is a designated University compliance officer, the compliance officer is generally the data owner.

Excessive use

Use that is disproportionate to that of other users, is unrelated to academic or employment-related needs, or that interferes with other authorized uses.

Harassment

Use of University information technology resources in ways that have the purpose or effect of adversely affecting the safety, security, or privacy of others. This form of harassment may include but is not limited to: 1) computer or other electronic communications that are repeated, unwelcome, and likely to humiliate, threaten or intimidate, 2) electronic monitoring of the whereabouts of others, and 3) unauthorized accessing of others' personal online accounts and information. See the University Policy Library for policies that cover other types of harassment (e.g. Administrative Policy: *Sexual Harassment, Sexual Assault, Stalking and Relationship Violence*).

Information Technology Resources (IT Resources)

Facilities, technologies, and information resources used for information retrieval, processing, transfer, storage, and communications in support of University research, education, outreach, and administrative needs. This definition is not all inclusive but rather reflects examples of equipment, data, content, tools, supplies, and services. This also includes services that are University owned, leased, operated or provided by the University or otherwise connected to University resources, such as cloud and Software-as-a-Service (SaaS) or Infrastructure-as-a-service (IaaS), or any other connected/hosted service.

Included in this definition are computers, mobile devices, computing and electronic communications devices and services, authentication credentials, e-mail, networks, telephones (including cellular), voice mail, fax transmissions, video, multimedia, licensed information resources, computer labs, classroom technologies, and research

and instructional materials.

Personal IT Resources

Personally owned IT Resources that are not purchased using any University funding.

Personal Information

Information that relates to and/or identifies the community member as an individual, such as bank account numbers and social security numbers.

Security Controls

Processes, software, configurations, or hardware used by system and network administrators to ensure the integrity, confidentiality, and availability of information technology resources and data.

Controls are any administrative, management, technical, or legal method that is used to prevent, detect or correct risks. Controls are also known as safeguards or countermeasures. Controls include practices, policies, procedures, programs, techniques, technologies, guidelines, and organizational structures.

Unit

Any organizational entity within the University. Includes, but is not limited to colleges, departments, centers, institutes, offices and programs.

University Community Member

A University community member is a student, faculty, or staff member, University guest, alumni, volunteer, contractor, or employee of an affiliated entity.

User

All users of University IT Resources, whether or not they are affiliated with the University, who are permitted to make use of University information technology resources, including students, staff, faculty, alumni, guests, sponsored affiliates, and other individuals who have an association with the University.

Responsibilities

User

- Review, understand, and comply with policies, laws and contractual obligations related to access, acceptable use, and security of IT Resources.
- Consult with University Information Security on acceptable use issues not specifically addressed in this policy.
- Protect personal information and personal assets used to access personal information or University data.
- Follow the user specific security controls in Administrative Policy: *Information Security* on personal assets, including but not limited to encryption, patching, virus protection, and two-factor authentication.
- Report possible violations of this policy to University Information Security (security@umn.edu). To report anonymously, use the *University UReport confidential reporting system*.

Campus, College, and Department Administrators

- Work with University Information Security to investigate alleged violations of this policy.
- Report possible violations of this policy to University Information Security (security@umn.edu).

Data Custodian, Data Owner, Technical Staff

- Protect the privacy of users, unless designated as University-approved personnel to monitor, examine or disclose this information.
- Respond to questions from users related to appropriate use of IT Resources.
- Work with University Information Security to investigate alleged violations of this policy.
- Report possible violations of this policy to University Information Security (security@umn.edu).

University Chief Information Officer

- Designate individuals who have the responsibility and authority for IT resources.
- Designate individuals who have the responsibility and authority for establishing policies for access to and acceptable use of IT resources.
- Designate individuals who have the responsibility and authority for monitoring and managing system resource usage.
- Designate individuals who have the responsibility and authority for investigating alleged violations of this policy.

University Chief Information Security Officer

- Delegate authority and responsibility for investigating violations of this policy.
- Designate individuals who have the responsibility and authority to refer violations to appropriate University offices or law enforcement agencies for resolution or disciplinary action.
- Designate individuals who have the responsibility and authority to employ security controls and ensure that appropriate and timely action is taken on acceptable use violations.

Office of Information Technology (OIT) – University Information Security

- Investigate possible violations of this policy.
- Refer alleged violations to appropriate University offices and law enforcement agencies for resolution or disciplinary action.
- Ensure that appropriate and timely action is taken on alleged violations.

- Coordinate with Internet Service Providers and law enforcement agencies on violations of this policy.

University Police Department

- Respond to alleged violations of criminal law.
- Coordinate all activities between the University and outside law enforcement agencies.

General Counsel

- Provide legal advice to University staff to ensure compliance with state and federal law including the classification of University data.
- Identify groups to include as University community members.

Related Information

Related Board of Regents Policies

- *Academic Freedom and Responsibility*
- *Code of Conduct*
- *Employee Group Definitions*
- *Student Conduct Code*

Related Administrative Policies

- *Copyright Ownership*
- *Data Security Breach*
- *Entering into Contracts*
- *Information Security*
- *Managing University Records Retention*
- *Sexual Harassment, Sexual Assault, Stalking and Relationship Violence*

Related Laws, Regulations, and Contracts

- Digital Millennium Copyright Act (DMCA) (PDF)
- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- *Minnesota Government Data Practices Act*
- *Payment Card Industry Data Security Standard (PCI DSS)*
- *Gramm–Leach–Bliley Act (GLBA)*
- Computer Fraud and Abuse Act, 1986
- Electronic Communications Privacy Act

Related Appendix

- *Examples of Public, Private and Confidential Information*
- *E-mail and Protected Health Information*

Other

- *Mass Email Requirements and Guidelines*
- *Practice Safe Computing* - General Information on Available Security Controls
- *Recognize and Report Information Security Incidents*
- *Filming and Photography on Campus*

History

Amended:

October 2024 - Comprehensive Review Revisions:

1. Policy: Clarified and modified policy statement section; further defined Acceptable Use responsibilities; new definitions for authentication credentials, excessive use, security controls replaces security measures.

2. Clarified definition of Information Technology Resources (IT Resources).
3. Updated Appendices.
4. Removed Appendix: E-mail and Protected Health Information from the AUP Policy. This appendix is owned by the governing Protected Health Information Policy and linked under the Related Appendix section of this policy.
5. Renamed Use of Personally Owned Mobile Devices for University Business Appendix to Use of Personal IT Assets for University Business

Amended:

October 2019 - Comprehensive Review.

1. Clarified and modified policy statement section
2. Updated the appendices
3. Updated and added definitions/responsibilities to align with definitions/responsibilities in other Information Security policies
4. Moved the Notifications for Copyright Infringement procedure to FAQ
5. Updated Related Information to remove a since retired policy and add a link to recognize and report information security incidents
6. Added an associated procedure *Report Information Security Incidents*. The review of the procedure is part of the comp review for *Data Security Breach*.

- Update the definitions to align with the definitions in the other information security policies
- Update the responsibilities to add Data Custodians and Data Owners
- Update the Related Information section to remove the Internal Access to and Sharing University Information policy that was retired June 2019 and add a link to Recognize and Report Information Security Incidents

Amended:

January 2019 - Establishing that reimbursements of salary, expenses, financial aid, and any other forms of reimbursement will not be provided if the original disbursement is stolen due to the individual not enabling available security controls that would have prevented the theft.

Amended:

August 2015 - Comprehensive review. Minor Revision. Update policy statement to include relevant policy content from other sections of the policy or appendix; update contacts, appendices, definitions, responsibilities, and related information section; remove administrative procedure on Reporting Violations of Acceptable Use of Information Technology Resources, remove administrative procedure on Taking Disciplinary Action, remove appendix University Network Operational Continuity, remove appendix Using Information Technology.

Amended:

August 2010 - The following appendices have been superceded by Administrative Policy: *Securing Private Data, Computers and Other Electronic Devices*:

- Anti-Virus Standard

- Critical Server Identification Guideline
- Information Technology Support Guidelines
- Information Technology Support Staffing Standard
- Mac OS X Basic Desktop Security Guidelines
- Password Standard
- Physical Security for Critical Servers Guideline
- Secure Data Deletion Standard
- Securing Microsoft Domain Controller Standard
- Securing Private Data Standard
- Security Patch Application Standard
- Server Security Guidelines
- University Network Management Guidelines
- Windows 2000/XP Basic Desktop Security Guidelines
- Windows Vista Basic Desktop Security Guidelines

The following appendix was superceded by Administrative Policy: *Wireless Network Infrastructure*:

- Wireless Access Point Technical Standards

Amended:

September 2007 - Added Windows Vista Basic Desktop Security Guidelines to Related Information and Appendices.

Amended:

July 2007 - Added Physical Security of Servers guideline to Related Information and Appendices.

Amended:

May 2007 - Updated Duluth Contacts.

Amended:

November 2006 - Added Password Standard to related information and appendices.

Amended:

October 2006 - Added Mac OS X Basic Desktop Security Guidelines to Related Information and to Appendices (Appendix P).

Amended:

May 2006 - Added this sentence to policy statement: "Units, campuses that grant guest access to University information technology resources must make their guests aware of User Rights and Responsibilities."

Amended:

April 2005 - Revised definitions and responsibilities section and procedure 2.8.1.1. Added Appendix N: Examples of Reportable Security Incidents and Appendix O: Critical Server Identification Guideline. These changes made to address issues related to HIPPA.

Amended:

July 2004 - Appendix E: OIT Securing Network Infrastructure Guideline was changed to a standard, and content was significantly revised. Title is now: University Network Standards for Network Security & Operational Continuity. Appendix G: Protecting Private Data Guidelines upgraded to Standards. Added Appendix L and M: Information Technology Support Staffing Standard, and Information Technology Support Guidelines.

Amended:

April 2004 - Title for appendix A is now: Using Information Technology Resources Standards to more accurately reflect that it is required. Appendix A was listed as a "guideline" before formal definitions of guidelines and standards were established.

Amended:

January 2004 - Critical Security Updates and Patches Guideline is now a Standard. Added OIT Server Installation Security Guidelines and OIT Windows 2000/XP Desktop Installation Guidelines to Related Information and Appendices.

Amended:

August 2003 - Added Procedure 2.8.1.3 - Notifications for Copyright Infringement.

Amended:

March 2003 - Added Critical Security Updates & Patches Guideline and Secure Data Deletion Standard to Related Information and Appendices. Amended: October 2002 - Updated contacts section and Reporting Violations procedure with correct email address and phone number for abuse complaints.

Amended:

September 2002 - Added links to Securing Network Infrastructure Guideline, Securing Microsoft Domain Controller Guideline and Protecting Private Data Guideline to Related Information and Appendices.

Amended:

May 2002 - Added links to OIT Anti-Virus Standards and OIT Wireless Access Point Technical Standards to Related Information and to Appendices.

Amended:

September 2001 - Added link to University Network Management Guidelines in Related information.

Amended:

July 2000 - Updated Appendix A and Related Information sections.

Amended:

April 1999 - Updated and reordered Contacts section, and Procedure 2.8.1.1, Reporting Violations.

Amended:

August 1998 - Revised Policy Statement, Responsibilities, Definitions and Appendix A: Guidelines for Using Information Technology Resources. Updated and reorganized related information section. Intent of the revision is to more clearly address issues related to commercial use, spamming, University ownership of data, and University liability for personal or unauthorized use. Title changed from Acceptable Use of Computers, Networking, and Information Technology to Acceptable Use of Information Technology Resources. Responsible Officer changed from Executive Vice President and Provost to Chief Information Officer.

Amended:

December 1997 - Responsible Officer changed from Senior Vice President of Academic Affairs to Executive Vice President and Provost.

Effective:

December 1996