Policy on Acceptable Use of Information Technology Resources
University of Minnesota Auxiliary Services
September 1, 2015

This policy summarizes guidelines and restrictions in accordance with the University’s Acceptable Use of Information Technology Resources policy. Print and read the policy and retain it for your files. The policy can be viewed online at: policy.umn.edu/it/itresources

The University of Minnesota is the owner of the department’s technology resources and assets. Computers, networks and electronic information systems are essential resources for accomplishing University work. The University grants members of the University community shared access to these resources in support of accomplishing the University's mission. These resources are a valuable community asset to be used and managed responsibly to ensure their integrity, security, and availability for appropriate educational and business activities. All authorized users of these resources are required to use them in an effective, efficient, appropriate, and responsible manner.

Definition of Technology Resources
Technology resources include, but are not limited to, facilities, technologies and information resources used for University information processing, transfer, storage, and communications. Included in this definition are desktop computers, laptops, tablets, software and systems, computer labs, classroom technologies, computing and electronic communications devices and services, such as modems, e-mail, networks, telephones (including cellular), voice mail, fax transmissions, video multimedia, and instructional materials.

Definition of Acceptable Use
This term consists of these related concepts:
- Information/data and systems may only be used by authorized individuals to accomplish tasks related to their jobs. Use of the information and systems for personal gain, personal business, or to commit fraud is prohibited.
- Information not classified as Public must be protected, and must not be disclosed without authorization. Unauthorized access, manipulation, disclosure or secondary release of such information constitutes a security breach, and may be ground for disciplinary action up to and including termination of employment.

Securing and Using Technology Resources
Users are required to follow these security and use requirements in their daily interaction with technology resources:
- User will not download, install, connect, modify, attempt to repair, move or change hardware and software settings or configurations unless directed to do so by their manager/director in consultation with IT staff.
- User will not download software to a departmental computer without approval from departmental IT Staff. This includes, but is not limited to, screensavers, games, freeware/shareware, courseware, utilities, and demonstration software. Unauthorized software will be removed if it is discovered during routine maintenance of the system or if reported by the supervisor.
- Use of web browsers and email may not be used for more than minimal personal use. The University accepts no responsibility or liability for any personal communications as private and does not examine or disclose the contents except for system maintenance, security purposes, or
when there is reason to believe that an individual is violating the law, University wide policies, or department policies.

Mail that is scanned and found containing a possible virus may be blocked from your mail box. Unauthorized removal or circumvention of virus scanning software may result in disciplinary action.

Screen savers with passwords should be used on equipment running software applications that have confidential information such as payroll information, student financial information, billing information, etc. Laptops and other devices carried outside of the offices must be password protected and if appropriate, encrypted. Do not carry confidential or protected data on flash drives.

Never share your password with others. If you must, change it as soon as possible. You may be required to change it on a regular basis.

All essential data files must be backed up on a regular basis. Your supervisor will provide you with the appropriate network drive and data directory locations for backing up your data. IT staff can create departmental data directories and grant users the appropriate access rights for backup locations on the server. Files saved to the server are automatically backed up.

University technology resources will not be used for any unauthorized or illegal purposes such as, but not limited to, pornography, gambling, private business practices, selling personal property, distributing inappropriate materials (non-University business related information), plagiarism, theft, copyright infringement, and/or harassment.

User will report any incidents which may have compromised technology resource security including, but not limited to, lost equipment, lost data, viruses, and compromised passwords.

Supplements to this policy may be provided by each department.

Depending on the nature and severity of the offense, policy violations will result in loss of access privileges, disciplinary action, criminal prosecution, and/or termination of employment.

Please read the statement below and sign and date the form. Forward the completed form to your supervisor or manager.

I have read the University of Minnesota Auxiliary Services policy and have a clear understanding of the policy guidelines.

____________________________________________  _____________________________
Employee Name – Printed                      Department

____________________________________________
Employee Signature

____________________________________________
Date