Statement of Policy

Washington University in St. Louis (WashU) is committed to conducting all university activities in compliance with all applicable laws, regulations and university policies. WashU has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objectives

This policy provides direction for appropriate use by students, faculty and staff of computer systems, network and data at Washington University in St. Louis (WashU). This applies to systems connected to WashU in any method and from any location.

This policy seeks to protect the integrity of the WashU information systems themselves: the computing or networking resources need to be accessible and secure for appropriate use consistent with the mission of WashU; the usurpation of these resources for personal gain, commercial gain or without authorization is unacceptable.
To manage systems and networks at WashU, comply with regulatory requirements and enforce the various Information Security Policies, WashU may log, review, retain, prohibit, or in any manner utilize any data or information stored or transmitted via WashU assets.

Relationship to WashU Policies

All WashU policies listed below apply to information technology as well as to other forms of communication and activity. In addition, these policies are fully recognized by the WashU Computer Use Policy. All users are responsible for being aware of and complying with regulations and Information Security Policies. Use of WashU systems or network that violates any of these policies will be investigated and sanctions may be applied, including termination.

Code of Conduct

Intellectual Property Policy

Freedom of expression / Freedom from Harassment

Social Media Policy

WashU students will reference the Student Technology Services Network Use Policy http://sts.wustl.edu/policies/network-use-policy/. When in a faculty or staff position, students are expected to adhere to department and / or school policies for network use.

Use of WashU Resources

WashU resources are shared resources available for students, faculty and staff to further educational, research, medical, service and university-related activities and missions. Staff, faculty and students should abide by federal, state, and city laws, regulations and university policy.

WashU does not monitor the content of web pages or other online communications and is not responsible for the views expressed by individual users.

The personal use of WashU systems and networks should be limited in nature, scope and appropriateness.

While the privileges and responsibilities vary between schools and departments, the use of university resources for personal commercial gain or for partisan political purposes (not including the expression of personal political views, debate and the like) is inappropriate and possibly illegal.

Individual university computer systems and departments have varying access requirements and resources. Departments or Schools may implement additional computer use guidelines as necessary. Copies of such additional computer user guidelines must be provided to Chief Information Security Officer.

Privacy

Although respect for privacy is fundamental to the University’s policies, understand that almost any information can in principle be read or copied; that some user information is maintained in system logs as part of computer system maintenance; that the University must reserve the right to examine computer files, and that, in rare circumstances, the University may be compelled by law or policy to examine even personal and confidential information stored, transmitted or accessed on University computing facilities.

Access to WashU Secure Systems

WashU provides access to internal and external system resources. Use of these resources may be governed by various state and/or federal regulatory requirements. All authorized users with access to protected information and systems are expected to be aware of and comply with the regulatory requirements that govern the use of the data as well as the resource. Guidance along with the specific regulatory requirements are provided at WashU through the University’s Area Specific Compliance Offices.
Students, faculty and staff should be aware of the University’s computer and data classification guidelines prior to utilizing external or personal computing resources through the WashU system. These guidelines are available on the CIO.wustl.edu and informationsecurity.wustl.edu websites.

Authentication

Students, faculty and staff are responsible for protecting their account credentials (user IDs and passwords). Users should not share credentials used for authentication and access to WashU systems and network verbally or in electronic or written communications. Unique credentials are required for all students, faculty and staff to access WashU systems and network. Inappropriate access of WashU resources may significantly impact education, research, and patient care and other University activities.

Personal devices

Devices purchased by a student, faculty or staff member used to access WashU data or network must conform to all WashU policies and device protections based upon data classification accessed, stored or transferred from the device. It is the responsibility of the device owner to secure the system or data. Faculty, staff and students may contact the department or school Help Desk to ensure their personal devices conform.

Misuse of resources

Students, faculty and staff are responsible for all activity involving their WashU accounts and are granted privileges and responsibilities with these accounts. These privileges are not to be used to violate any University policy, or city, state or federal laws or regulations. Access may be revoked in cases of misuse or threat to WashU systems and network.

Students, faculty and staff are not to use the WashU systems or network to cause harm or perform illegal activities including, but not limited to the following:

- Cause harm to individuals, University data, University network,
- Disable systems, programs or software
- E-mail Spam or harassment
- Modify or destroy data integrity
- Copyright infringement
- Malicious computer activity

Circumventing WashU policies to compromise the security of an account, system, devices, network or WashU partner will not be tolerated.

WashU Rights

Access

WashU, through the appropriate Systems Administrator or Management request, may deactivate a user’s privileges when deemed reasonably necessary to enhance or preserve the confidentiality, integrity or availability of the WashU systems or network.

Monitoring

WashU does not monitor student, faculty and staff system or network usage. Daily system processing and maintenance will log and backup the data. The individual right to privacy may, when personal files may need to be accessed for troubleshooting purposes or to investigate a reported incident, be overridden by authorized personnel to protect the integrity of the University's computer systems.

Security

WashU reserves the right to enforce security controls to preserve the confidentiality, integrity or availability of the WashU systems or network. These controls may affect the storage, transmission and access of confidential and protected information in accordance with WashU policies, regulations, state and federal laws or regulations.
WashU reserves the right to restrict access to internal or external resources based upon risk to the University systems or network.

Reporting

All WashU students, faculty and staff are responsible for reporting concerns or possible violations of this policy. Report concerns or possible violations to infosec@wustl.edu. Concerns or violations can also be reported anonymously on the University's hotline at (314) 362-4998.

Investigation

Violations of this policy may lead to an investigation involving but not limited to designated representatives for students, faculty or staff, Human Resources, General Counsel, Information Security, Internal Audit, the HIPAA Privacy Office , or other Area Specific Compliance Office.

Sanctions

Violations of this policy may lead to disciplinary action up to and including termination under either the Human Resources corrective action process or the HIPAA Sanction policy.

For questions about this policy, contact your school, department or unit system manager or e-mail Kevin Hardcastle (mailto:hardcastlek@wustl.edu), Chief Information Security Officer.

Title: Computer Use Policy
Version Number: 3.0
Creation Date: May 31, 1997
Applicability: WashU Faculty, Staff, Students and Guests
Reference Number:01.04
Status: Final
Revision Date: October 10, 2016
Policy Owner: Information Security Office