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.

Objective

This policy identifies a well-defined and organized approach for access to faculty or staff electronic information or systems at WashU.

Policy

This policy applies to access requests from management for active or former faculty or staff computing resources in accordance to the privacy expectations outlined in the WashU Computer Use Policy. This will include students while in a staff or faculty role.

“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.”

In addition, this policy outlines the actions IT staff must adhere to prior to granting access to any individual’s electronic activity.

If a legal or regulatory incident is suspected for an active or former member of WashU faculty or staff, management will contact the Office of General Counsel and / or Human Resources for guidance prior to requesting access to the current or former faculty or staff member’s email, files or system.

Access to Email Accounts

Management access to a faculty or staff member’s Email account should only be requested for continuation of university, school or department needs (e.g. ongoing projects, contacts, schedules, recruitment, contracts, grants, research) or in the course of an internal investigation.

- Access to active WashU faculty or staff Email accounts requires approval from a Human Resources Consultant.
- Access to former WashU faculty or staff Email accounts requires approval from the manager or supervisor.

Requests will be processed through the University ticket system. Upon approval, access will be provided to the manager or supervisor, or person they have designated only for a period of 30
days for WashU department or school purposes. Extensions will require approval from the Information Security Office.

**Access to Electronic Files or Systems**

Management access to a faculty or staff member’s files or systems used to access, store or transmit WashU information should only be requested for continuation of university, school or department needs (e.g. ongoing projects, contacts, schedules, recruitment, contracts, grants, research) or in the course of an internal investigation.

- Access to active WashU faculty or staff files or systems requires approval from a Human Resources Consultant.
- Access to former WashU faculty or staff files or systems requires approval from the manager or supervisor.

Requests will be processed through the University ticket system. Upon approval, access will be provided to the manager or supervisor, or person they have designated only for a period of 30 days for WashU department or school purposes. Extensions will require approval from the Information Security Office.

Access to any information will always be by administrators nominated by the Executive Director of End User Services or the area specific IT Director.

**Access to Internet Access Logs / Browser History**

Management access to active or former WashU faculty or staff Internet access logs requires approval from a Human Resources Consultant. If approved, the Human Resources Consultant will contact the IT Department to request the logs for the specified time period.

**Title:** Access to Faculty or Staff Email, Files or Systems  
**Version Number:** 1.0  
**Creation Date:** 02/07/2017  
**Approval Date:** 06/15/2018  
**Applicability:** Protected, Confidential and Public  
**Reference Number:** 02.09  
**Status:** Final  
**Policy Owner:** Information Security Office