Washington University in St. Louis

Office of Information Security
University Information Security Policies

Access to Faculty or Staff Email, Files or Systems Policy

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
The policy and associated guidance provide a well-defined and organized approach for access to faculty or staff electronic information or systems at WashU.

Applicability
This policy is applicable to all accounts, electronic messaging, and systems connected to all WashU network segments.

Audience
The audience for this policy is all WashU faculty, staff, and IT users with elevated permissions.

WashU students will need to be aware of this policy. This also applies for all other agents of the university with access to WashU information and network for contracted services. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as “WashU community”.

Roles & Responsibilities

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

WashU does not monitor individuals’ 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 and former WashU faculty or staff email accounts requires approval from Human Resources Employee Relations.

Requests will be processed through the university ticket system. Upon approval, access will be provided to the manager, supervisor, or designee only for a period of 30 days for WashU department or school purposes. Extensions will require approval from the Office of Information Security (OIS).

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 and former WashU faculty or staff files or systems requires approval from Human Resources Employee Relations.

Requests will be processed through the university ticket system. Upon approval, access will be provided to the manager, supervisor, or designee only for a period of 30 days for WashU department or school purposes. Extensions will require approval from the OIS.

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 Human Resources Employee Relations. If approved, Human Resources Employee Relations. will contact the IT Department to request the logs for the specified time period.

Faculty or Staff Access Log Requests
Requests from faculty or staff for logs related to email, internet, or account access require approval from Human Resources Employee Relations.

Access requests from Federal, State, or Local Agencies
Requests will be coordinated with the Office of General Counsel and/or Human Resources and will follow the Information Security Incident Management Process.

Policy Compliance
The OIS will measure the compliance to this policy through various methods, including, but not limited to - reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the OIS in advance. Non-compliance will be addressed with management, Area Specific Compliance Office, Human Resources, or the Office of Student Conduct.

Related Policies
Computer Use Policy

Reference
Incident Management Process

Policy Review
This policy will be reviewed at a minimum every three years.

Title: Access to Faculty or Staff Email, Files or Systems Policy
Version Number: 2.0
Reference Number: AC-01.03
Creation Date: February 7, 2017
Approved By: Security and Privacy Governance Committee
Approval Date: June 15, 2018
Status: Final
Scheduled Review Date: March 1, 2022
Revision Date: September 8, 2023
Revision Approval Date: September 22, 2023
Policy Owner: Office of Information Security