Litigation Hold 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 approach to notify, identify, collect, and retain electronic information relevant to requests from the Office of the Executive Vice Chancellor and General Counsel (OGC) for preservation or collection of electronic information.

Applicability
This policy is applicable to all WashU information, infrastructure, systems, and network segments.

Audience
The audience for this policy is all WashU faculty, staff and students. It 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
OGC will notify WashU employees of a request to retain electronic information for a pending legal action. This notification will identify the relevant individuals and the nature and scope of information sought. The CIO, Department IT Director and Chief Information Security Officer (CISO) will be copied to assist in the process.

Pursuant to the instructions in the litigation hold notification from OGC, WashU Department or School staff designated to assist the Information Security Office (ISO) and OGC will identify information that falls within the scope of potentially relevant information defined in the notification (e.g., for wrongful termination claims, potentially relevant information may include
records of performance appraisal, documentation of reason for termination and e-mails that discuss the process within the time period specified).

- Policies and procedures concerning e-mail retention, mailbox size limits, workstation redeployment procedures and backup and recovery retention will also be provided to the designated staff by the ISO.
- IT staff will preserve a copy of the email stored on the server and a copy of any local e-mail files (e.g., PST and mobile devices such as laptops, thumb drives, and PDAs).
- The information provided to the ISO by the IT Staff will need to be stored in a manner to allow for subsequent review. All media collected will need to be securely stored with logged access controls.

The information will be retained until OGC approves the release of the information. Tapes or files that contain information collected will not be recycled or deleted until OGC approves deletion. Reminders may be sent annually to determine the status of the collected information.

**Policy Compliance**
The ISO 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 ISO in advance. Non-compliance will be addressed with management, Area Specific Compliance Office, Human Resources or the Office of Student Conduct.

**Related Policies**
None

**Reference**
None

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

**Title:** Litigation Hold Policy  
**Version Number:** 2.0  
**Reference Number:** PL-01.06  
**Creation Date:** September 26, 2007  
**Approved By:** Security and Privacy Governance Committee  
**Approval Date:** April 6, 2016  
**Status:** Final  
**Scheduled Review Date:** March 1, 2022  
**Revision Date:** February 26, 2019  
**Revision Approval Date:** March 15, 2019  
**Policy Owner:** Information Security Office