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

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.

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 the 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.

Title: Litigation Hold Policy
Version Number: 2.0
Creation Date: September 26, 2007
Applicability: Protected, Confidential and Public
Reference Number: 01.02
Status: Final
Revision Date: April 6, 2016
Policy Owner: Information Security Office