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 and organized approach to facilitate access being granted, managed and reviewed based on the roles of each computer user while remaining compliant with regulatory mandates.

Policy

Controls to grant, modify and review account access are necessary to ensure WashU protected and confidential information is secure. WashU departments and schools will develop and maintain processes to ensure access to protected and confidential information is assigned and managed based on the role of each workforce member.

- Unique accounts and password are required for each workforce member to access WashU resources.
- Workforce members are responsible for actions initiated from their accounts.
- Minimum necessary access to system data will be granted to perform necessary university functions. An approval process will be in place for access to protected information to comply with regulatory requirements.
- Role changes and inactivity necessitate access levels to be modified.
- The supervisor/manager is responsible for requesting removal of access to WashU information.

Emergency Access

Emergency situations may require modifications to access levels to facilitate caregiver access to systems housing protected information to provide patient treatment. This is approved when the denial of this access could inhibit or negatively affect patient care.

- Please refer to the specific school or department’s Disaster Recovery plan for more information.
- Protected information repositories that do not affect patient care are not subject to the foregoing emergency access requirement.
- When the emergency situation has subsided, the account access will be returned to the prior settings.

Review of Access

Supervisors are responsible to review the access levels of subordinates to confirm the required access is setup.
- Access to protected information will be reviewed at a minimum on a quarterly basis.
- Access to confidential and public information will be reviewed at minimum on an annual basis.

Title: Managing Access Policy
Version Number: 2.0
Creation Date: January 24, 2008
Applicability: Public, Confidential and Protected
Reference Number: 02.04
Status: Final
Revision Date: April 6, 2016
Policy Owner: Information Security Office