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

Applicability
This policy is applicable to all WashU accounts, 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
Controls to grant, modify, and review account access are necessary to ensure WashU protected and confidential information is secure. In addition to controls, 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.

- WUSTL Key is the preferred method of authentication to WashU systems and network.
- WashU community members are responsible for actions initiated from their accounts.
- Unique accounts and password are required to access WashU resources.
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.

- Access provided will be monitored by management, data owners, and/or system administrators to ensure separation of duties is maintained.
- Privileged accounts with access to protected and confidential systems and control code will be documented and reviewed.
- Role changes and inactivity will necessitate access levels to be modified as soon as possible. Access will be limited upon separation from the university.
  - The supervisor/manager is responsible for requesting removal of access to WashU information.
  - Any exception requests will need to be reviewed by the Information Security Office (ISO).

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 quarterly (at a minimum)
- Access to confidential and public information will be reviewed annually (at a minimum).

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: Managing Access Policy
Version Number: 3.0
Reference Number: AC-01.01
Creation Date: January 24, 2008
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