Mobile Device Security 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 methods of protection for all mobile computing and storage devices that contain or access protected or confidential information resources at WashU.

Applicability
This policy is applicable to all mobile devices used to create, store, transmit, and access WashU protected or confidential information.

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
With advances in computer technology, mobile computing, and storage devices have become useful tools to meet the needs of individuals and organizations. They are portable, easily lost, or stolen presenting a high risk for unauthorized access, disclosure of university information.

- The Information Security Office (ISO) will conduct periodic risk assessments to establish safeguards for secure use. It is responsible for assessing the use of mobile computing devices and the schools and departmental processes to ensure compliance with this policy.
• WashU community must give notification to their department or school if databases, email, or other repositories containing confidential or protected information will be downloaded to the mobile devices. In this way, the appropriate security controls can be applied to mitigate the additional risk associated with that information.

• Departments and schools will establish processes that allow them to keep track of mobile devices used to store confidential or protected information, any policies applied to them, and WashU community members who use them.

• Lost or stolen mobile computing devices must be reported to the Privacy Office or the ISO as soon as it is possible. This shall occur before the user of the device cancels the service with the provider.

• Security policies must be deployed to all mobile devices that will access or store protected information. Devices incapable of accepting these security policies must not access or store protected information. Mobile Device Guidelines will be used to establish these policies.

• The use of ePHI on mobile devices requires breach notification training and the understanding of their responsibilities to protect devices and promptly report any lost or stolen devices.

• Devices storing protected information will need to follow the Encryption Policy to protect information.

• Additional controls may be required for devices based upon the security risk assessment.

Policy Compliance
The ISO will measure the compliance to this policy through various methods, including but not limited to, reports, internal and 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
Encryption Policy

Reference
None

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

Title: Mobile Device Security Policy
Version Number: 3.0