Personal 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 requirements for using personal devices to access, create, host, and transmit confidential and/or protected information.

Applicability
This policy is applicable to all WashU network segments, networks, and campus locations.

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
WashU is required to ensure confidentiality, availability, and integrity of the information created, hosted, and transmitted. Unsecured personal devices pose a security risk to WashU information and network. Prior to using a personal device for WashU activities, WashU community members need to be aware of the requirements and expectations.

Personal devices used for university activities will be subject to the WashU Computer Use Policy.

- WashU community members will adhere to the specific department or school procedures for personal devices. Limited support may be provided by the school or department’s IT group.
- Students working in staff or faculty positions will use WashU provided computers.
• Personal devices may be reviewed if the device is determined to be within the scope of potentially relevant information defined in the litigation notification.

WashU will not accept liability for personal devices. In addition, WashU will not reimburse device owners for any devices purchased for personal use.

The device owner is responsible for the following:
• the maintenance, backup, or loss of data on any personal devices
• reporting any device lost, stolen, and/or recovered
• ensuring all security requirements are installed and updated
• installing OpenDNS on faculty and staff devices
• contacting their school or department’s IT group to verify the following are installed and current prior to connecting to the WashU network
  o Anti-virus
  o Auto Updates turned on
  o Anti-spyware
  o Personal Firewall
• ensuring, if the device is connected to the WashU clinical network or will access protected information it will:
  o Conform to all policies and protections
  o Be up to date on all patches and antivirus definitions
  o Connect through a VPN instead of public WiFi

School of Medicine
To reduce the risk of WashU School of Medicine information being stored or accessed from devices that may not be able to secure the information as required by state, federal, and industry regulations WashU community members will connect to WashU network with personal devices that are encrypted and able to receive vendor updates and patches. Minimum requirements are provided for Windows and Mac devices. Other vendor devices are acceptable as long as they are able to meet these requirements.

WashU device owners will not store protected health information on personally owned devices. If there is a need to store protected health information on a personally owned device, it must be protected with encryption in accordance with the WashU Encryption Policy. Failure to comply with the Encryption Policy will result in sanctions in accordance with the WashU Policy on Sanctions for Non-Compliance with HIPAA Policies.

WashU reserves the right to update and require any additional controls for personal devices based upon the risk to the WashU network or environment.

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**
- Computer Use Policy
- Information Classification Policy

**Reference**
- Encryption – Windows and Mac
- Minimum Device Requirements – School of Medicine

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

**Title:** Personal Device Security Policy  
**Version Number:** 1.0  
**Reference Number:** SC-01.03  
**Creation Date:** February 14, 2019  
**Approved By:** Security and Privacy Governance Committee  
**Approval Date:** May 16, 2019  
**Status:** Final  
**Scheduled Review Date:** June 1, 2022  
**Revision Date:**  
**Revision Approval Date:**  
**Policy Owner:** Information Security Office