FITCHBURG STATE UNIVERSITY

Personal Device Policy

Version 1.1	**Last Updated:** 5/9/2024
Security Level: Public	**Issued:** 10/14/2022

Purpose

Fitchburg State University grants its employees the privilege of using personal tablets, laptops, and smartphones for work. Fitchburg State University reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below. This policy is intended to protect the security and integrity of Fitchburg State University's data and technology infrastructure.

Scope

The scope of this policy applies to all members of the Fitchburg State University community and any affiliates or devices connecting to Fitchburg State University's network.

Policy

Personal device acceptable use is defined as:

- Business use activities that directly or indirectly support the business of Fitchburg State University
- Devices may not be used on the Fitchburg State network at any time to store or transmit illicit materials, harass others, or otherwise perform actions contrary to the Acceptable Use Policy or other university policies.
- Employees may use their mobile devices to access company-owned resources such as email, calendars, contacts, documents, etc.

Devices and support:

- Smartphones, including iPhone and Android phones, are allowed and must have storage encryption turned on.
- Tablets, including iPad and Android, are allowed and must have encryption turned on.
- Connectivity and personal device issues are supported by the Technology Help Desk as best they can.
- Devices may need to be presented to the Technology Department for proper provisioning, review, and configuration of standard apps before they can access the network.

Security

- To prevent unauthorized access, devices must be configured according to Fitchburg State's policies and password-protected to access the company network.
- Data stored must be encrypted on all devices to University encryption standards.
- Employees may be prevented from downloading, installing, and using any app that is not allowed per licensing on the company's list of approved apps.
- The employee's device may be remotely disconnected and/or data wiped if
    - the device is lost,
    - the employee terminates his/her employment,
    - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must repair or wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The university reserves the right to disconnect devices, disable services or delete data without notification or user approval.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the university's acceptable use guidelines.
- The employee is personally liable for all costs associated with his or her personal device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of university and personal data due to an operating system crash, errors, bugs, viruses, malware, remote wipe command, and/or other software or hardware failures, or programming errors that may render the device unusable.

Roles

Staff: Understand and adhere to this policy.

Management: Determine who can bring personal devices to work. Periodically review access lists and notify IT when this list requires adjustment. Report suspected violations of this policy to the Information Security Program Manager.

Technology System Administrators: Execute procedures defined for assigning and removing access, and device configuration. Ensure that access is authorized and assigned duties require access capabilities. Ensure that the Technology infrastructure is protected against unauthorized access. Report suspected violations of this policy to the Information Security Manager.

Chief Information Security Officer: Oversee the policy's Compliance, review it periodically, and update it as needed.

References

CISv8 1.1 Establish and Maintain a detailed Enterprise Asset Inventory
CISv8 1.2 Address Unauthorized Assets

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including loss of access rights and/or termination of employment under adherence to their respective collective bargaining agreement. Students found to have violated this policy may have their access removed and may have additional actions taken as directed by the Student Code of Conduct.

Revision History

Date of Change	Revision	Responsible	Summary of Change
10/14/2022	1	Steve Swartz, CIO Sherry Horeanopoulos, CISO	Creation of Policy, Start of Revision Tracking, Formatting of Document
5/9/2024	1.1	Eric Boughton, CISO	Formatting