Mobile Device Management Policy

1.0 Overview

University employees use smart phones and tablets (smart devices) as a means of sending and receiving university email, synchronizing calendars and contacts, transmitting text messages and connecting to the Internet. The purpose of this policy is to describe the conditions under which the university permits the use of smart devices for its employees, and how the university manages mobile technology to minimize risk, especially in the event of loss or theft.

2.0 Scope

This policy applies to WPI faculty, staff, contractors, vendors, and other personnel who are granted privileges to access WPI resources.

3.0 Smart Device Definition

For the purposes of this policy, a smart device is a small form factor, typically handheld device with at least one wireless network interface for network access for data communications. This interface can use Wi-Fi, cellular networking or other technologies that connect to the Internet or other data networks.

The device contains local non-removable data storage and an operating system (OS) specific for the hardware of device.

4.0 University Owned Mobile Devices

Certain university employees are required to use smart devices to facilitate university business. Supervisors must identify those employees who require a smart device as part of their job responsibilities. The Information Technology department directly works with these individuals to assist with the purchase of a mobile device and the appropriate data/voice plan.

Employees are allowed incidental personal use of university owned smart devices as long as no applicable state or federal laws, and no university polices, are being violated by such use. Employees are reminded that university owned smart devices, data stored on a device, and the data/voice plans and records are sole property of the university. When an employee leaves the university the mobile device is to be wiped of WPI information and at the discretion of the

employee's Department the device can be given to or purchased by the employee, or returned to the University for recycling or redeployment.

University-owned smart devices must have the manufacturer's installed operating system (OS) and vendor updates must be accepted and installed when required.

Configuration of Mobile Devices

IT will administer and configure all mobile devices that are purchased by the University. For Apple devices (iPhones, iPads), a supervision notification, directed by Apple, will appear on the main Settings page of these devices. This will state that the device is being managed by WPI, which includes configuration of wireless settings, improved setup assistance, and a remote wipe if there is a security breach. WPI will not use this administration tool to track employees; it is a standard vendor banner displayed on iOS devices and is for security management only.

5.0 Personally Owned Mobile Devices

The university recognizes and allows employees, although not required to use a smart device as a requirement of their position, to connect personally owned smart devices to the university's resources to access and synchronize email data, contacts, and calendar information. All usage use must comply with state and federal laws, as well as with the university's own policies governing appropriate use of technology.

Personally owned smart devices that use university resources must have the manufacturer's installed operating system (OS) and keep current as possible of vendor updates.

6.0 Smart Device Security (university and personally owned)

If an employee, either due to work-related requirements or through their own personal choice, elects to access university's sensitive resources, which includes email, Workday or Salesforce, via a smart device, they must accept the security policies defined by the university that may be downloaded, installed and/or configured on the device upon connecting to university resources. The smart device security policies are designed to accomplish the following primary objectives.

- Require a pin/password/passcode to unlock the device
- Remotely wipe the device in the event of 10 failed login attempts
- Remotely wipe the device in the event that the device is lost or stolen
- Limit the amount of email that can be stored on the device to 4 weeks

The OS must be the one designed and built for the specific hardware. The OS is not to be modified in any way that compromises the device's security. Jailbreaking, the act of altering a smart device's OS, is strictly prohibited when connecting to WPI's sensitive resources.

Report a Lost or Stolen Mobile Device

A lost or stolen mobile device containing university data, whether university or personally owned, must be reported to Information Security by contacting Infosec@wpi.edu or calling the IT Service Desk at x5888 as soon as possible (ASAP). The missing device will be remotely wiped of all data to protect the university and the user from data lost.

Exceptions

The mission of WPI's Information Technology division is to support the WPI community with its academic and research objectives. We understand that in pursuit of these research and academic endeavors, exceptions to this policy may be required. For any faculty, student, or staff that requires an exception, please contact WPI's Chief Information Security Officer.

7.0 WPI Contract Roles

CONTACT PERSON
Chief Information Security Officer
Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609
Phone: (508) 831-6868

8.0 Enforcement

Any person that violates any of the measures found in this policy will be subject to disciplinary action, which may include termination or dismissal from WPI, or other appropriate disciplinary action.

9.0 Approval and Revisions

Policy Category: Institutional Risk & Compliance

Policy Approved By: Approved by WPI's Information Security, Risk and Compliance Committee on 9/26/2018.

Policy Reviewed Annually By: Chief Information Security Officer

Related University Policies: None

Last Modified: 5/02/19