COLLEGE POLICY: 467

INFORMATION TECHNOLOGY MOBILE DEVICE MANAGEMENT

PURPOSE

UA Cossatot implements necessary controls, technologies, and devices to secure information systems and critical data. Mobile devices are an inevitable part of our daily lives, and they are used to conveniently perform business-related activities and provide access to data. However, mobile devices have fewer security controls to keep systems and data secure. This policy was developed to define the best practices and principles to secure individual devices, university systems, and data.

SCOPE

This policy applies to all mobile devices—university-owned or personal—accessing UA Cossatot systems and data to conduct college business by college employees.

Sensitive Data: Sensitive data is a blanket term used to designate classes of data with a high level of security that the college is legally or contractually required to protect. Sensitive data refers to any element of data that is uniquely or in aggregate protected by federal regulations (ex: HIPAA, FERPA), categorized as PII or PHI, or any other data that has been identified as business-critical or business-sensitive data, such as financial records or intellectual property of UA Cossatot.

Mobile Devices: Mobile devices are smartphone or tablet type devices that typically run Apple IOS or Android operating systems. These often very portable devices include some form of internet connectivity (Wi-Fi and/or Cellular) and are used to perform various functions such as reading and responding to emails, providing access to various enterprise applications, and interacting with various documents.

POLICY

This policy is intended to ensure all employees follow safe computing practices when using mobile devices. Users are encouraged to apply these best practices to all mobile devices, including those that are not used for accessing campus data, to minimize risks and data loss associated with lost or stolen devices. UA Cossatot understands and respects that the use of personal devices to access campus data is a personal choice that happens to provide significant benefit to the campus and the community served. UA Cossatot does, however, have an obligation to this same user community that access to campus data and resources is done in a safe and secure manner. Employees choosing to opt-out of this set of identified best practices or employees that have devices that cannot comply with the best practices identified below must not access campus data from their mobile devices.

To ensure compliance with UA System policies, UA Cossatot policies, laws, and regulations, employees using mobile or personal devices to perform college business, functions, and tasks or accessing and processing college data, IT must implement application protection policies with the following security best practices and device settings to protect the security of the mobile devices and campus data:

1. Sensitive or business-critical data must not be stored on the mobile device.
2. College data on the mobile phone will be encrypted.
3. All applications must be installed from official application repositories. (e.g. Google Play or Apple App Store)
4. Auto-updates must be enabled for the mobile devices operating system and all applications running on the device.
5. Device screen must be locked with a passcode, fingerprint, face recognition, or similar method.
6. Device auto-lock must be enabled.
7. If the device supports "Remote Wipe" this functionality must be enabled to permit the end-user to erase a lost or stolen device.
8. The device operating system must not be altered or modified. (e.g. "rooted" or "jailbroken").

Additionally, some mobile devices provide additional security features that may be beneficial to end-users, such as "Find My Device (Phone)." UA Cossatot encourages end-users to weigh the benefits of enabling such capabilities (such as recovering a lost device). UA Cossatot can in no way use these additional features for administrative oversight on personally owned devices.

Users uncertain whether their devices comply with these requirements or those that have further questions are encouraged to contact the IT department for additional help.

PRIVACY OF PERSONAL DATA

The application protection policies are designed to protect college data and information from loss or disclosure. These policies in no way allow administrative access to personal data, files, photos, messages, address book, etc. stored on personal devices.

ENFORCEMENT AND SANCTIONS

Any user attempting to circumvent the best practices and device settings mandated in this policy may face revocation of access, suspension of accounts, or other disciplinary action.

Policy History:
March 7, 2022

PROCEDURE: NONE