

East Carolina University (ECU) Mobile Device Security Guidelines

Mobile devices are subject to increased risk of loss, breakage, theft and unauthorized use. The purpose of this document is to provide guidance for the appropriate use and security of mobile devices in order to protect the East Carolina University (ECU) network and/or information from unauthorized access or disclosure and minimize the threat of theft and loss.

Document Sections:

- [General Guidelines](#)
- [Recommendations](#)
- [Definitions](#)

General Guidelines for the Use of Mobile Devices

1. For all department portable devices, inventory the serial numbers, locations and employees to whom they are issued.
2. Desktop and laptop computers purchased using state funds (including grant monies) are required to be ordered through the [Combined Pricing Initiative \(CPI\)](#), the bulk IT purchasing program. Visit the website for computer models, specifications and pricing details.
3. If sensitive data must be stored on flash drives, purchase drives equipped with onboard hardware-based AES encryption. ITCS recommends [Ironkey](#) encrypted flash drives. Please note that the passwords used on these encrypted flash drives must adhere to the same strength requirements as an [ECU PirateID](#). These drives should also be included on the department's portable device inventory.
4. Personal mobile devices that access the ECU network must conform to best security practices such as [strong passwords](#), [updated antivirus](#) and [updated security patches](#), if applicable. If a mobile device cannot conform to the best practices outlined above, use best security practices available and avoid storing sensitive data on the device.
5. ECU-issued Windows devices receive automatic antivirus and operating system security patch updates when connected to the ECU network. Remember to regularly connect the device to the ECU network to receive these updates. All other devices require users to enable automatic updates for antivirus and security patches.
6. Always perform a virus scan on a flash drive when:
 - this is the drive's first use (brand new, out of the package)
 - the drive belongs to someone else (e.g., vendor, co-worker, student)
 - the drive is out of your span of control

Recommendations for the Secure Use of Mobile Devices

1. **Use of Personal Devices.** Never download ECU data to non-ECU portable devices. Store the data on an ECU administrative system, [ECU managed Server or Pirate Drive](#) and access the data via the secure [Virtual Private Network \(VPN\)](#).
2. **Appropriate Access and Use of Sensitive Information.** Sensitive information must not be stored on mobile devices without prior approval from your department Director or Chair. Additional reviews by ECU data owners are required for the following types of data: FERPA, HIPAA, credit card, Social Security Numbers (SSN) and certain personal identifiable information (PII). Contact the ITCS Help Desk @ 252-328-9866 to request an information security consult for these types of data.
3. **Use of Personal Identifiable Information (PHI).** Additional security controls and standards must be implemented if storing PHI. Please review the [HIPAA Workstation Security](#) and [HIPAA Portable Device Policies](#) prior to storing PHI and contact Information Security prior to storage.
4. **Physical Protection.** Mobile devices owned or issued by the university must not be left unattended and, when possible, must be physically locked away or secured. In addition, any portable media (for example, portable hard drives, CD or DVD disks) used to back up systems containing sensitive information must be encrypted and stored securely in locked drawers, cabinets or other secure enclosures at ECU.
5. **Lost or Stolen Devices.** Immediately contact your supervisor and the ECU Police (252.328.6787) to report a lost or stolen ECU mobile device. The university must report all stolen university-owned computers to the State Bureau of Investigation (SBI). Immediately notify the ITCS Help Desk at 252-328-9866 if there is any possibility the lost or stolen device contained sensitive data. Err on the side of caution, if unsure.
6. **Virus Protection.** Any mobile device capable of using antivirus software must have the software installed and configured to maintain updated virus signatures. Visit the [antivirus software entry](#) of the ITCS service catalog to learn more.
7. **Use of Encryption.** All laptops, tablet PCs, flash drives and other mobile devices that store sensitive data must consistently encrypt all files using the university's [standard encryption technology](#). Any device storing HIPAA, FERPA, PCI (credit card) and SSNs must be registered with Information Security prior to storage. If you have sensitive data stored on your desktop and/or departmental servers, contact the IT Help Desk (252.328.9866) to request an IT security consult to ensure this information is registered.
8. **Secure Connectivity.** Any sensitive information transmitted to or from the mobile device (e.g., wireless or the Internet) must be encrypted ([ECU encrypted wireless network](#) or [VPN over Internet](#)).
9. **Disabling Unused Services.** Wireless, infrared, Bluetooth or other connection features should be turned off when not in use.
10. **Password Storage.** Storing user IDs and passwords is prohibited on unencrypted mobile devices.
11. **Use in Public.** Reasonable care must be taken when using mobile computing facilities in public places, meeting rooms or other unprotected areas outside of ECU's premises to avoid the unauthorized access to or disclosure of the information stored on or accessed by the device.
12. **Traveling Abroad.** When traveling abroad with an ECU-owned mobile device, please contact [John Chinn](#), University Export Controls Administrator, at 252-328-9473 to discuss export control requirements prior to your travel.
13. **Report a Security Incident.** Immediately report to your supervisor any suspected misuse or data breach of a mobile device and the ITCS Help Desk at 252.328.9866.

14. **Termination of University Relationship.** All university-owned mobile devices must be returned to ECU prior to or immediately upon termination of the assigned user's relationship with the university. In addition, university-purchased software installed on personal mobile devices must be removed immediately by the user. All sensitive information must be removed from the device immediately prior to or upon termination of the assigned user's relationship with the University.
15. **Proper Disposal of the Device.** All ECU devices, including mobile devices and other electronic equipment used to store sensitive information must be sanitized prior to transfer to another user, disposal or repair. Contact the ITCS Help Desk at 252.328.9866. See the [Disk Sanitizing](#) Policy.

Definitions

- **FERPA.** The Federal Family Educational Rights and Privacy Act defines the requirements for the protection of the privacy of student records.
- **GBLA.** The Gramm-Leach-Bliley Act, a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.
- **HIPAA.** The Health Insurance Portability and Accountability Act defines the requirements for the protection of the patient privacy and the security of their protected health information (PHI).
- **Mobile Device.** Includes any device that is both portable and capable of collecting, storing, transmitting or processing electronic data or images. Examples include but are not limited to, laptops or tablets (e.g., iPads), personal digital assistants (PDAs) and "smart" phones such as Blackberries and iPhones. This definition also includes storage media, such as USB hard drives or USB flash drives, SD or Compact CDs, DVDs, Flash cards and any peripherals connected to a mobile device.
- **PCI.** The Payment Card Industry Data Security Standard is a set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.
- **Personal Mobile Device.** Includes any mobile device not owned or issued by ECU.
- **PHI.** Protected Health Information is any information about health status, provision of health care or payment for health care that can be linked to a specific individual.
- **PII.** Personally identifiable information*
- **Sensitive information.** Includes PII, PHI, student educational record information (FERPA) that is protected by law or regulation, financial data protected by law or regulation (PCI, GLBA), as well as other proprietary information that, if inappropriately disclosed, can cause harm to the university. Guidelines for identifying and protecting sensitive information at ECU are discussed in [Guidelines for Protecting Sensitive Data](#).

***PII Examples:**

- Social security or employer taxpayer identification numbers
- Driver's license, state identification card or passport numbers
- National identification numbers
- Checking account numbers
- Savings account numbers
- Credit card numbers
- Debit card numbers
- Passwords
- Fingerprints
- Digital Identity