

# Mobile Computing Regulation

Updated: November 18, 2019

**POLICY:**

REG08.05.12

**TITLE:**

Mobile Computing Regulation

**CATEGORY:**

Information Technology

**SUB-CATEGORY:**

Security and Compliance

**AUTHORITY:**

Chancellor

**CONTACT:**

Chief Information Officer, ITCS (252) 328-9000

**RELATED POLICIES:**

[University Student and Employee Computer Use Policy](#)

[Academic Computer Use Policy](#)

[Data Governance Regulation - Interim](#)

[Software and Data Collection Services Acquisition Regulation - Interim](#)

[Information Security Regulation](#)

[Family Education Rights and Privacy Act \(FERPA or Buckley Amendment\)](#)

[Health Insurance Portability and Accountability Act \(HIPAA\) Privacy Policies](#)

[Health Insurance Portability and Accountability Act \(HIPAA\) Security Policies](#)

[Social Security Numbers \(SSN\) and Personal Identifying Information \(PII\) Regulation](#)

[Volunteer Regulation](#)

**ADDITIONAL REFERENCES:**

[ECU Information Security Best Practices and Standards](#)

[ECU Data Classification Standard](#)

[International Standards Organization \(ISO\) 27002 Code of Practice for Information Security Controls](#) (formally adopted by all University of North Carolina institutions)

[North Carolina Identity Theft Act](#)

[North Carolina Human Resources Act](#)

[Family Educational Rights & Privacy Act of 1974 \(FERPA\)](#)

[Health Insurance Portability and Accountability Act \(HIPAA\) Security Rule Summary](#)

[Health Insurance Portability and Accountability Act \(HIPAA\) Privacy Rule Summary](#)

[Health Information Technology for Economic and Clinical Health \(HITECH\) Act](#)

[Payment Card Industry Data Security Standards \(PCI-DSS\)](#)

[Gramm-Leach-Bliley Act \(GLBA\)](#)

[EU General Data Protection Regulation \(GDPR\)](#)

**HISTORY:**

New regulation approved by Chancellor's Executive Council on November 18, 2019.

**PREVIOUS VERSIONS:**

No previous versions available.

## 1. Purpose

1.1. This Regulation defines ECU Employee and volunteer responsibilities for the appropriate use, support, and oversight of University Information on Mobile Computing Devices and Removable Electronic Media.

## 2. Scope

2.1. This regulation applies to all persons and entities employed by or performing work on behalf of the University, including, but not limited to, staff, faculty, student workers, residents, contractors, and volunteers (the “Covered Persons”).

## 3. Definitions

3.1. IT Support Staff: An employee who provides technical or end-user support of a University-owned or managed IT system or service to other persons, regardless of their affiliation with the University. For the purpose of this policy, this pertains to University-owned Laptops and supported Mobile Computing Devices.

3.2. Administrative Head: An employee who manages departmental operations and directs the use of departmental resources. This role is typically associated with an administrative department director or a college dean, though this oversight responsibility extends to Vice-Chancellors and other leadership positions who may be charged with these duties.

3.3. Covered Device: Any Mobile Computing Device or Removable Electronic Media, regardless of whether it is owned by the University or is the personal property of a Covered Person.

3.4. Mobile Computing Device: A portable computing device that provides persistent data storage and runs software applications much like a typical computing device. Examples of Mobile Computing Devices include, but are not limited to: smartphones, tablets, laptops, and wearable computing devices.

3.5. Removable Electronic Media: A portable electronic storage device that provides persistent data storage but lacks processing capability for running software applications. Examples of Removable Electronic Media include USB flash drives, removable hard drives, and optical media such as CDs and DVDs.

3.6. University Information: Information in any form (e.g., electronic, printed or spoken) that is collected, created, stored, distributed or otherwise used by Covered Persons in the course and scope of their employment, or volunteer responsibilities, respectively, for any University purpose, including, but not limited to teaching, research, and service.

**3.7. Sensitive University Information:** A subset of University Information that is confidential pursuant to applicable regulation, law, contractual obligation or other legal requirement., such as FERPA, HIPAA, the North Carolina Identity Theft Protection Act, and the Payment Card Industry (PCI) Data Security Standard. Examples of Sensitive University Information include but are not limited to: Social Security Numbers (SSNs), credit card numbers, bank account numbers, Protected Health Information, educational records, personnel records, and research data, records, and information of a proprietary nature.

## 4. Policy Statements

4.1. It is the policy of East Carolina University that Covered Persons who access, use, transmit or store University Information on a Covered Device shall protect it from unauthorized and/or unlawful access, use, disclosure, and destruction.

4.2. University Rights: ECU is the legal owner of University Information. Covered Persons have no expectation of privacy regarding University Information created, used stored, or residing on Covered Devices.

4.3. Covered Device Access: Covered Persons shall make available University Information on Covered Devices to authorized University representatives as required for the University to conduct business and/or comply with applicable legal or policy requirements. This includes, but is not limited to, providing University Information on Covered Devices for the purpose of responding to litigation, public records requests, and audit requirements. Covered Persons shall provide appropriate assistance to authorized University officials (such as the Covered Person's supervisor or person in the Covered Person's supervisory hierarchy, University legal counsel, or internal or external auditors) to make available University Information on Covered Devices. Monitoring or otherwise accessing a Covered Device to enforce University policies requires specific approval of the Chancellor or the Chancellor's designee.

4.4. Covered Person Responsibilities: Covered Persons shall take reasonable precautions when using a Covered Device to protect University Information from unauthorized and/or unlawful access, use, disclosure, destruction, and/or loss. Covered Persons shall adhere to all applicable federal regulations, state laws, contractual

requirements, and University information security policies and standards.

4.4.1. Device use authorization: Covered Persons shall use Covered Devices to access or store Sensitive University Information only as authorized by the relevant data steward(s), compliance office(s) or University committee(s). Depending on the data involved (e.g., Protected Health Information, educational records, Social Security Numbers, and Banner IDs), the acceptable uses and documentation requirements are defined by the same respective authority(ies).

4.4.2. Device security: Covered Persons shall ensure all Sensitive University Information stored on Covered Devices is encrypted, and the Covered Devices are secured in accordance with University policies, the ECU Information Security Standards, and applicable regulations, laws and contractual requirements. Examples of additional security measures include, but are not limited to password protection, up-to-date software and operating system security patches, anti-malware software, inactivity time-out, and physical device protection.

4.4.3. Device replacement and disposal: Covered Persons shall ensure that all Sensitive University Information stored on Covered Devices is removed or rendered inaccessible before replacing, disposing or otherwise relinquishing possession of the devices to persons who are not authorized to access the information.

4.4.4. Loss or theft of a Covered Device: Covered Persons shall promptly report the loss or theft of a Covered Device containing Sensitive University Information to their supervisors, who shall ensure that ITCS and the relevant compliance office(s), data steward(s), University committee(s), and Administrative Head(s) are appropriately notified.

4.5. IT Support Staff Responsibilities: Designated IT Support Staff shall utilize approved technology resources to assist Covered Persons in meeting with their responsibilities for the appropriate use of University-owned Mobile Computing Devices.

4.5.1. Encryption of University-owned Laptops: IT Support Staff shall enable industry-standard encryption on all University-owned laptops, prior to being provided to Covered Persons for the first time, and following each time serviced thereafter.

4.5.2. Encryption of University-owned Mobile Computing Devices: IT Support Staff shall enable industry-standard encryption on all other supported University-owned Mobile Computing Devices, prior to being provided to Covered Persons for the first time, and following each time serviced thereafter.

4.5.3. Maintenance of University-owned Laptops: IT Support Staff shall deploy all software and operating system security patches and updates for all University-owned laptops following appropriate testing and approval.

4.5.4. Maintenance of University-owned Mobile Computing Devices: IT Support Staff shall deploy all software and operating system security patches and updates on all other supported University-owned Mobile Computing Devices following appropriate testing and approval.

4.5.5. Support of University-owned Laptops: IT Support Staff shall provide technical assistance for all Covered Persons for all University-owned laptops, as it pertains to the storage, access, and use of all University Information.

4.5.6. Support of University-owned Mobile Computing Devices: IT Support Staff shall provide technical assistance for all Covered Persons for all other supported University-owned Mobile Computing Devices, as it pertains to the storage, access, and use of all University Information.

4.6. Administrative Head Responsibilities: Administrative Heads shall ensure Covered Persons are aware of their responsibilities to take reasonable precautions when using a Covered Device to protect all University Information from unauthorized and/or unlawful access, use, disclosure, destruction, and/or loss, as well as to adhere to all applicable federal and state laws, contractual requirements, and University Information security policies and standards. In addition, Administrative Heads shall ensure that IT Support Staff are aware of their responsibility to assist Covered Persons in meeting with their responsibilities for the appropriate use of Covered Devices.

## 5. Guidance

5.1. Covered Persons shall refer to their respective ECU Best Practices in Information Security manual(s) and/or the relevant data steward(s),

compliance office(s), and University committee(s) for specific guidance on fulfilling the responsibilities outlined herein.

Covered Persons shall contact the Information Technology and Computing Services (ITCS) department for any assistance needed with University technologies to fulfill these requirements.

## 6. Violations

6.1. Violation of this Regulation may result in disciplinary action, up to and including dismissal from employment or volunteer position, being taken in accordance with applicable University policy.