Best Practices in Information Security for ECU Management:

Standards for Protecting the Information in Your Care

East Carolina University

October 4, 2021

Contents

Introduction 3
Definitions 4
Information Security Practices for Management 5
Management Practice #1: Employee awareness, acknowledgements, and responsibilities 5
Management Practice #2: Information system compliance 7
Management Practice #3: Physical security of employee work areas 9
Management Practice #4: Continuity of operations (COOP) planning 11
ECU Information Security Standards for Management 13
1.2 Reporting security weaknesses and events 13
2.1 Information security awareness and education 13
2.2 Acknowledgments of responsibility 14
2.3 Securing office and work areas 14
3.1 Business continuity management 14
3.2 Business continuity plan maintenance 15
4.1 Legal, regulatory, and contractual compliance 15
4.2 Policy and standards compliance 16
Resources 18

Introduction

This manual provides best practice guidance based on ECU's Information Security Standards. The guidance is to assist ECU Administrative heads and/or Supervisors, in fulfilling their charge for protecting the University Information and IT/Information Systems in the care of their departments and employees. For the purposes of this guide an "Administrative Head" is defined as:

> **the administrative director of a university department, such as an academic department chair, administrative department director or college dean. Administrative Heads direct departmental operations and the use of university resources within their departments.**

Best practices and standards

Each best practice provides practical guidance on implementing an ECU information security standard. Where the security standard establishes a requirement (e.g., business continuity plans must be tested), its associated best practice describes what you can do to meet the standard. For each of the best practices in this guide you will find:

- *Best practice statement:* a brief description of your responsibility for this practice
- *Your activities:* a list of actions to help you implement the best practice
- *Guidance:* additional background information on the best practice and its implementation
- *Relevant standard:* a reference link to the underlying ECU information security standard

Baseline requirements

The best practices and standards in this guide represent a minimum, or *baseline,* set of practices and requirements for managing information security in your department. More stringent controls may be warranted, depending on the nature of the information and information systems involved. For example, if your employees handle regulated information, such as that covered by HIPAA or FERPA, your employees will be required to take additional precautions beyond those defined by the best practices in this guide.

Alternative controls

In cases where a best practice or standard cannot be implemented (e.g., excessive costs, technical limitations or operational disruptions) alternative controls must be implemented that provide a similar level of security and risk. The use of alternative controls must be approved by the appropriate management authority to ensure that any changes in university risk fall within acceptable levels.

Higher education environment

The ECU information security best practices and standards in this guide are based on an international framework for information security management, the *ISO 27002 Information Technology Security Techniques – Code of Practice for Information Security Controls*. Although based on a framework intended for all sectors, the ECU best practices and standards are tailored to ECU's academic, research and administrative environments, providing better relevance and practicality for a higher education institution.

Roles and responsibilities

The ECU information security best practices and standards are divided into three separate guides, each designed for a specific role:

- *Employee:* A person employed by the University or who serves as a University volunteer. This includes anyone performing work on behalf of the University, such as staff and faculty members, student workers, contractors, and unpaid volunteers.
- *Management:* The administrative director of a University department, such as an academic department chair, administrative department director or college dean. Administrative Heads direct departmental operations and the use of university resources within the department. This manual also describes information security standards important for supervisors of employees.
- *IT Support:* 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 guidance on your responsibilities for regulatory compliance, contact the relevant ECU compliance office. If you have questions about the ECU best practices and standards in information security, contact the Information Security Office.

Definitions

University information: Information in any form (e.g., electronic, printed or spoken) that is collected, created, stored, distributed or otherwise used by the University for academic, research, administrative, healthcare or other authorized purposes.

Sensitive information: The UNC System 1400.3 Standard defines sensitive information as information regulated by law, protected by contractual terms, or defined in classification and other policies relevant to the constituent institution. At ECU, a standard for data classification has been approved based on four levels of data, entitled *ECU Classification Levels*. ECU is recognizing "sensitive information" as covered in the 1400.3 Standard to be equal to the ECU data classification levels of Level 3 and Level 4.

Level 3 - Confidential/Sensitive covers data such as research data, student data that is not designated as directory information, and other confidential data for which unauthorized disclosure could have a serious adverse impact on the university, individuals, or affiliates. Level 4 - Highly Restricted includes Social Security numbers, payment card numbers, medical records, restricted information protected by nondisclosure agreements, and restricted research data.

Information system: Any combination of hardware, software, data, and electronic communications that collectively serves a particular purpose. Information systems include, but are not limited to: laptops, tablets, smart phones, desktop computers, file servers, web servers, operating systems, networking devices, and software applications.

Information Security Practices for Management

Management Practice #1: Employee awareness, acknowledgements, and responsibilities

The Best Practice

Ensure your employees' information security responsibilities are clearly defined, conveyed, and fulfilled.

Your Activities

- Direct your managers to integrate relevant information security responsibilities into employee job descriptions, performance plans, business processes and routine communications.
- Ensure your employees formally acknowledge their responsibilities on a periodic basis.
- Charge your managers with ensuring your employees have the skills, resources and motivation necessary to fulfill their information security responsibilities.

Guidance

Information security is more about people than technology

Information security is far more about people than it is about technology. Any employee can circumvent our security technologies and place ECU and the people we serve at risk. Such actions can disrupt university operations; create compliance failures and financial penalties; and breach the privacy of our students, employees, and healthcare patients who entrusted us with their personal information.

Employee awareness and responsibilities

Most data breaches occur at the hands of well-meaning employees, who are simply trying to do their work. However, the resulting investigations almost always reveal that an employee failed to follow established policy and guidance. This is why is it important that you ensure *your employees are aware of and understand the importance of their information security responsibilities.*

You can strengthen employee awareness within your department by ensuring employee security responsibilities are suitably integrated into job descriptions, performance plans, business processes and routine communications about their work. This establishes clear and consistent expectations for how your employees must fulfill their responsibilities to protect the information and IT systems in the care of your department.

Reporting security concerns

You will recall that one of the information security best practices for all ECU employees is to report security concerns promptly through designated reporting channels. As emphasized in the required online course *Employee Best Practices in Information Security Training*, employees are advised to seek guidance from their supervisors concerning security concerns. Please be mindful that supervisors in your department should be prepared to provide good guidance to employees. Please ensure that security

concerns are reported to ITCS, this can be handled easily by contacting Pirate Techs at 252-328-9866 or 800-340-7081 (or through Pirate Techs Support Chat, or Submit a Ticket in TeamDynamix). Information security events should be assessed by ITCS to determine if they are to be classified as information security incidents and thus responded to in accordance with documented plans and procedures.

Periodic employee acknowledgements

Employee acknowledgements benefit both the employee and the University. A good acknowledgement statement not only provides a clear statement of responsibilities to the employee, it also documents the employee's receipt and understanding of this information for the University. In short, a signed acknowledgement statement allows our employees to *confirm* that they are aware of and understand their information security responsibilities.

Periodic employee acknowledgements provide greater assurance that your employees are up to date on the latest risks to ECU information, as well as any corresponding adjustments to their responsibilities. Fortunately, you can take advantage of existing acknowledgement processes that are administered centrally, such as those provided by ITCS when employees access various IT services. However*, your managers should also integrate employee-specific information security responsibilities into formal job descriptions and performance management plans, where they are reviewed and signed periodically by your employees.*

Employee skills, training resources, and motivation

The skills and resources needed by your employees depend on the nature of the information they handle and the associated compliance obligations of handling that information. For many employees the most basic information security guidance may be sufficient, such as that found in ECU policies, standards, employee awareness activities (e.g., ITCS newsletters, website articles, and email blasts), and the required online course *Employee Best Practices in Information Security Training*.

Information Security Best Practices for ECU Management **(online training)**. Some employees are most receptive to guidance when that information is delivered by those with direct authority over their work and priorities. To help supervisors with giving effective and accurate guidance to employees, an information security course designed for managers and supervisors is also offered. This course, *Information Security Best Practices for ECU Management*, is available online in Cornerstone, is designed to complement our general security awareness training, and is aligned with content in this document.

If your employees work with regulated information, such as patient treatment information or student educational records, your managers should ensure your employees participate in the appropriate compliance training. For guidance on employee awareness and training contact the appropriate compliance office or the Information Security Office.

In addition to ensuring your employees have the necessary skills and resources, your managers must ensure your employees have the motivation to fulfill their responsibilities. A common approach is to formally integrate information security responsibilities into job descriptions and performance

management plans. This ensures that your employees are aware that they are accountable for fulfilling their information security responsibilities, just as they are for any work responsibility.

Relevant ECU Information Security Standards

- 1.2 Reporting security weaknesses and events
- 2.1 Information security awareness and education
- 2.2 Acknowledgments of responsibility

Management Practice #2: Information system compliance

The Best Practice

Ensure the management and use of computers, information systems and IT services within your department comply with all relevant policies, standards, laws and contracts.

Your Activities

- Assign responsibility to a designated person(s) for documenting the policy, legal and contract requirements that are relevant to your departmental information systems and IT services.
- Direct your managers to ensure all information systems and IT services provided or administered by their respective areas adhere to the relevant compliance requirements.
- Oversee that servers managed by distributed IT staff within your department comply with the ECU Technical Vulnerability Management Plan.
- Ensure that software, cloud solutions, or data collection services managed by your department, that are associated with sensitive information, meet UNC System standards and ECU requirements to implement MFA to protect sensitive information.
- Ensure information and data security compliance for your department, and assign responsibility to a designated person(s) for periodically reviewing compliance, identifying areas of noncompliance, and documenting corrective actions.

Guidance

Begin with UNC System and ECU policies and standards

Administrative Heads are responsible for ensuring the security of all University information as it is collected, created, access, distributed or otherwise handled by their respective departments, as well as the security of IT systems and services provided or managed by their respective departments (ECU Information Security Regulation, para 5.2). ECU information security policies and standards are based on the same basic security practices as many regulations, laws, and industry standards. You will find that by complying with University policies and standards you will have a head start on complying with many of the external requirements that apply to your department's activities. Increasingly, there have also been important information technology and information security policies and standards approved by the UNC Board of Governors. ECU policies and standards help to ensure compliance with UNC System standards.

Multi-factor authentication to protect sensitive information. As a constituent institution of the UNC System, the statewide policies approved by the Board of Governors apply to ECU, which includes Policy 1400.3 on User Identity and Access Control. Pursuant to this policy, a 1400.3 system-wide standard became effective 7/15/2020, and requires that institutions implement MFA to protect sensitive information. Proposed software or technology systems being proposed for purchase, and undergoing assessment by ITCS, or being brought forward as requests before compliance committees or data stewards, must meet the university's MFA requirement to protect sensitive information. Normally, multi-factor authentication should be achieved through the university's SSO (integrated with Microsoft Azure AD).

Oversee to ensure that servers managed by your department meet IT requirements. As defined in the ECU Information Security Regulation (para 3.1), Administrative Heads manage departmental operations and direct the use of departmental resources (ECU Information Security Regulation, para 3.1). As noted earlier, the ECU Information Regulation (para 5.2) states that Administrative Heads are responsible for ensuring the security of all University information handled by their respective departments, as well as the security of IT systems managed by their respective departments. In your oversight of servers managed by your department, one important dimension of this is ensuring that departmental servers comply with the ECU Technical Vulnerability Management Plan. System Administrators must document departmental servers in an ITCS Server Assessment, and department servers must be onboarded into the ITCS approved vulnerability scanning program. ECU vulnerability management processesntify and evaluate the technical vulnerabilities of your information systems and remediate those vulnerabilities in a timely, effective, and systematic manner.

Ensure information and data compliance for your department

As defined in the *University Flexible Work Arrangement and Remote Work Regulation*, sensitive information, defined as level 3 and level 4 data classifications in accordance with University data governance, must not be processed or stored on a personally owned computer or device. When your employees work remotely off-campus, be mindful that sensitive information must be processed on institutionally owned systems, stored in approved storage, and accessed only by secure network access technologies (utilizing VPN or other multifactor authentication).

Administrative heads, as outlined in the *Mobile Computing Regulation*, are responsible for ensuring that their employees are aware of responsibilities to take reasonable precautions when using mobile devices and laptops to protect 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. Administrative heads must also ensure that IT Support Staff in their departments are aware of their responsibilities concerning mobile device support.

Assign responsibility for compliance management and reporting

It is important that you assign responsibility to a person or persons within your department for periodically assessing your compliance efforts, identifying compliance gaps, and developing remediation

plans. This will allow you to review your compliance levels on a moment's notice and be prepared to take advantage of opportunities for improvement as they arise.

Third-party (outsourced) IT services

If your department contracts for a third party IT service, your department must *manage* that service as it would an IT service provided by your employees. This means that you must ensure the third party service complies with all policies, standards and laws relevant to the handling of University information and management of IT services.

Please keep in mind that *your department must obtain formal approval before contracting with a third party IT service provider or placing any University information in the hands of a third party.* If you need more information, contact Pirate Techs at 252-328-9866 or 800-340-7081.

Relevant Standards

- 4.1 Legal, regulatory and contractual compliance
- 4.2 Policy and standards compliance
- 7.2 Procedures and responsibilities for authorized access to university information (please see *Best Practices in Information Security for IT Support Staff: Protecting the Information in Your Care*)
- 7.3 Information security monitoring and reporting

Management Practice #3: Physical security of employee work areas

The Best Practice

Ensure your managers take appropriate precautions to prevent unauthorized physical access to sensitive information in your employee work areas.

Your Activities

- Direct your managers to take reasonable precautions to prevent unauthorized physical access to sensitive information in all forms (electronic, printed, and spoken) wherever it may be handled, including home offices and remote work sites.
- Ensure your department manages third party access to restricted work areas in a manner that prevents unsupervised and unauthorized access to ECU information and information systems.

Guidance

Physical security is for all employee work areas, not just data centers

While the physical security of your employee work areas may be far less demanding than that of a secure data center, some basic precautions are appropriate nonetheless. For example, controlling the flow of office visitors will help your department limit unauthorized access to employee work areas where sensitive data may be handled. It is important that your department prevent visitors from easily viewing computer screens, browsing paper documents, or listening in on sensitive conversations.

Physical security in layers

You can reduce the likelihood that someone will gain physical access to your sensitive data by applying security in layers. For example, a visitor who passes by a reception desk undetected may be denied access to an unstaffed office area by a locked door.

Consider some of the following measures as part of a multilayer strategy for securing your work areas:

- Create a reception area or process to assist visitors and prevent them from gaining unimpeded access to nearby workstations and office areas.
- Position desks and computing workstations so that visitors find it difficult to view the contents of computer screens and printed documents.
- When staff members are out of the office, keep their office doors closed and locked.

Third party service personnel

There are times when third party service personnel (e.g., utility workers and contractors) must gain access to your restricted work areas. In these situations you must take precautions to prevent third party personnel from having unsupervised access to ECU information and information systems. One approach is to position a departmental employee at a nearby workspace to monitor the activities of third party personnel. It is helpful to the employee to know that such a precaution protects the third party as much as it does the University.

Protect your data backups

Lost and stolen data backups are a common source of data breaches. Not surprisingly, nearly all of our data backups contain sensitive information and must be physically protected from unauthorized access and theft. One option is to store your backup media (e.g., USB flash drives and removable hard drives) in locked cabinets or secure office areas that are inaccessible by unauthorized persons.

As an alternative to removable backup media, which are highly susceptible to theft and loss, consider backing up your data directly to an ECU departmental Piratedrive. The ECU Piratedrive system is located in a secure data center and is well protected from unauthorized access. For assistance with establishing a departmental Piratedrive contact Pirate Techs at 252-328-9866 or 800-340-7081.

Relevant Standards

- 2.3 Securing office and work areas

Management Practice #4: Continuity of operations (COOP) planning

The Best Practice

Maintain a Continuity of Operations (COOP) plan that ensures ECU mission essential functions and critical departmental functions will continue when disaster strikes, as well as ensure ECU information is protected during continuity and recovery activities.

Your Activities

- Designate a Continuity of Operations (COOP) Coordinator with responsibility for developing your departmental COOP plan.
- Charge your COOP Coordinator with maintaining your COOP plan through annual reviews, tests, and updates to ensure the plan remains viable and relevant to your business environment.
- Charge your COOP Coordinator with documenting the COOP plan reviews and tests, as well as ensuring your employees are properly trained to carry out their COOP responsibilities.

Guidance

Plan for disaster before disaster strikes

The worst time to plan for a disaster is when you are in the middle of one. Without a COOP plan you will discover that some of the resources upon which you depend—people, facilities and services—will not be available when you need them the most. To exacerbate the situation, you will also discover that the planning process itself burns up precious time—time that you need to keep your critical business functions up and running.

It is important that you formally designate a COOP Coordinator for your department with responsibility for developing and maintaining your COOP plan. Direct your Coordinator to work closely with the Office of Environmental Health & Safety (OEHS), who coordinates Continuity of Operations (COOP) planning for the University. Your COOP Coordinator should also review the OEHS COOP website and contact OEHS at 328-6166 or safety@ecu.edu for guidance.

Keep your plans current and relevant

Everything around us changes almost continuously. Thus, it is crucial that you keep your COOP plan updated to ensure it remains effective and relevant as things change around you. For example, if you plan to use a nearby computing lab as a temporary office, you may discover that the equipment does not support your recent software upgrade. It is far better to discover such changes in a test environment than during a real disaster. So, it is important that your department *reviews, tests and updates your COOP plan at least annually, and in response to significant changes in your business environment (e.g., new business processes and campus resource needs).*

Disaster recovery planning versus business continuity planning

Although disaster recovery and business continuity sound similar, they are quite different. Disaster recovery planning focuses on restoring services, such as technology and electrical services. Business continuity planning focuses on keeping your critical functions going *while* those services are being restored and may not be available to you.

Protect University information during business continuity and recovery activities

In the chaos that can follow a disaster it is easy to forget about mundane information security practices. However, doing so may place University information at high risk of loss and disclosure. Consequently, you should ensure that appropriate security measures are integrated into your departmental business continuity plan. For example, your COOP plan should consider how you will prevent unauthorized access to temporary office spaces and safely transport sensitive information from one location to another.

Relevant Standards

- 3.1 Business continuity management

ECU Information Security Standards for Management

1.2 Reporting security weaknesses and events

Purpose

To ensure that security weaknesses and events are quickly reported through appropriate channels to minimize the window of exposure and potential harm to the University and its stakeholders.

Standards

1.2.1 Employees shall promptly report potential security weaknesses and incidents through formal reporting channels in accordance with applicable incident reporting procedures.

ISO 27002:2013 References

- 16.1.2 Reporting information security events
- 16.1.3 Reporting information security weaknesses

2.1 Information security awareness and education

Purpose

To ensure that employees with access to university information resources are aware of and understand their responsibilities for protecting those resources.

Standards

2.1.1 All employees with access to university information resources shall be:

a) informed of their information security responsibilities as appropriate to their job duties and responsibilities
b) trained in information security practices that are relevant to their information security responsibilities
c) periodically reminded of information security policy, statutory, and regulatory requirements that are relevant to their job duties and responsibilities

ISO 27002:2013 References

- 6.1.1 Information security roles and responsibilities
- 7.1.2 Terms and conditions of employment
- 7.2.1 Management responsibilities
- 7.2.2 Information security awareness, education, and training

2.2 Acknowledgments of responsibility

Purpose

To ensure that employee responsibilities for information security are clearly defined, conveyed and acknowledged.

Standards

2.2.1 The information security responsibilities of all employees with access to university information resources shall be formally documented as appropriate to their roles and responsibilities with the university.

2.2.2 Employees shall formally acknowledge their information security responsibilities. The acknowledgements shall be:

a) obtained prior to gaining access to university information resources or as soon afterward as is practical

b) renewed on a periodic basis

c) documented for reporting and assurance purposes

ISO 27002:2013 References

- 6.1.1 Information security roles and responsibilities
- 7.1.2 Terms and conditions of employment
- 8.2.1 Management responsibilities

2.3 Securing office and work areas

Purpose

To ensure that office and work areas where sensitive information is handled are appropriately secured to prevent unauthorized information access.

Standards

2.3.1 Physical security controls shall be used in employee work areas to prevent unauthorized physical access to sensitive information.

ISO 27002:2013 References

- 11.1.3 Securing offices, rooms, and facilities

3.1 Business continuity management

Purpose

To ensure that essential university functions and critical departmental functions continue when a disaster or other disruptive event occurs.

Standards

3.1.1 All ECU mission essential functions and critical departmental functions shall be covered by business continuity plans to ensure such functions will continue in the event of a disaster, service outage, human error or other disruptive event.

3.1.2 Business continuity and disaster recovery plans shall address all relevant information security requirements to ensure the protection of information resources during business continuity and disaster recovery activities.

ISO 27002:2013 References

- 17.1.1 Planning information security continuity
- 17.1.2 Implementing information security continuity

3.2 Business continuity plan maintenance

Purpose

To ensure that business continuity and recovery plans remain effective and relevant as changes in the business or threat environments occur.

Standards

3.2.1 Business continuity plans and disaster recovery plans shall be reviewed annually and whenever there is a significant change in the business environment. The reviews and their results shall be documented.

3.2.2 Business continuity plans and disaster recovery plans shall be tested annually and whenever there is a significant change in the business environment. The tests and their results shall be documented.

ISO 27002:2013 References

- 17.1.3 Verify, review, and evaluate information security continuity

4.1 Legal, regulatory, and contractual compliance

Purpose

To ensure the selection, design, operation, and management of university information systems comply with all applicable legal, regulatory and contractual requirements.

Standards

4.1.1 All information stored or processed by an information system shall be protected from loss, destruction or misuse in accordance with applicable legal, regulatory, and contractual requirements.

4.1.2 All legal, regulatory and contractual requirements applicable to an information system shall be documented and made available to the appropriate management authority.

ISO 27002:2013 References

- 18.1.1 Identification of applicable legislation and contractual requirements
- 18.1.3 Protection of records
- 18.1.4 Privacy and protection of personally identifiable information

4.2 Policy and standards compliance

Purpose

To ensure that university processes and activities are carried out in compliance with university information security policies and standards.

Standards

4.2.1 Information systems shall be regularly assessed for compliance with university information security standards and requirements.

4.2.2 All operational processes involving the use of sensitive information shall be regularly reviewed for compliance with university information security policies, standards, and guidance.

4.2.3 Areas of noncompliance shall be evaluated to identify the causes of noncompliance and document corrective actions.

ISO 27002:2013 References

- 18.2.2 Compliance with security policies and standards
- 18.2.3 Technical compliance review

7.3 Information security monitoring and reporting

Purpose

To ensure security weaknesses and concerns are quickly discovered, reported, and remediated to minimize the window of exposure and potential material or reputational harm to the university.

Standards

7.3.1 Procedures shall be developed and widely communicated for the reporting of security concerns and suspected weaknesses of critical or sensitive university information systems. Mechanisms shall be put in place to monitor and learn from identified security incidents (16.1.1, 16.1.2, 16.1.3, 16.1.6).

7.3.2 Technical vulnerabilities of critical or sensitive university information systems shall be identified, evaluated, and remediated in a timely manner and based on risk to the university (12.6.1).

7.3.3 Application of security patches or updates for critical or sensitive university information systems shall followed established change management procedures. This includes testing changes in non-production environments, where practical. Where testing is impractical, backups of critical or sensitive data or information shall be performed prior to application of security patches or updates (12.1.2, 12.6.1).

7.3.4 Where security patches or updates for critical or sensitive university information systems are not available or cannot be applied, alternative measures shall be taken to manage risk(s) and a risk acceptance shall be documented, reviewed, and accepted by the appropriate division Vice Chancellor or designee as described in the *Software and Data Collection Services Acquisition Regulation* (12.6.1).

ISO 27002:2013 References

- 12.1.2 Change management
- 12.6.1 Management of technical vulnerabilities
- 16.1.1 Responsibilities
- 16.1.2 Reporting information security events
- 16.1.3 Reporting information security weaknesses
- 16.1.6 Learning from information security incidents

Resources

The following online resources provide additional information on the secure handling of information and information systems.

Data Governance Regulation: https://www.ecu.edu/prr/01/15/06
Governance, Compliance & Security (ITCS Service Catalog):
https://ecu.teamdynamix.com/TDClient/1409/Portal/Requests/ServiceCatalog?CategoryID=3660
Information Security Best Practices Manuals:
https://ecu.teamdynamix.com/TDClient/1409/Portal/KB/ArticleDet?ID=67419
Information Security Regulation: https://www.ecu.edu/prr/08/05/08
Information Technology & Computing Services (ITCS): www.ecu.edu/itcs
Mobile Computing Regulation: https://www.ecu.edu/prr/08/05/12
Report a Security Concern:
https://ecu.teamdynamix.com/TDClient/1409/Portal/KB/ArticleDet?ID=67469
Security Awareness Education at ECU:
https://ecu.teamdynamix.com/TDClient/1409/Portal/KB/ArticleDet?ID=67574
Sensitive Data Storage and Transmission: https://datagovernance.ecu.edu/sensitive-data-storage-and-transmission/
Software and Data Collection Services Acquisition Regulation: https://www.ecu.edu/prr/08/05/11
University Flexible Work Arrangement and Remote Work Regulation:
https://www.ecu.edu/prr/06/25/03
UNC System Policy 1400.1 Information Technology Governance:
https://www.northcarolina.edu/apps/policy/doc.php?type=pdf&id=96
UNC System Policy 1400.2 Information Security:
https://www.northcarolina.edu/apps/policy/doc.php?type=pdf&id=112
UNC System Policy 1400.3 User Identify and Access Control:
https://www.northcarolina.edu/apps/policy/doc.php?type=pdf&id=115