Best Practices in Information Security for Employees:

Standards for Protecting the Information in Your Care

East Carolina University

October 4, 2021

Contents

Introduction

The best practices in this manual are designed to help you—as an ECU employee—*fulfill your responsibilities for protecting the information in your care*. For the purposes of this guide, an "employee" is defined as:

> **Any 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.**

Please keep in mind that the practices in this guide provide general guidance to the University community and many not address all aspects of your job or working environment. So, you may need to take additional precautions to ensure the information in your care is safe and secure. For example, if the information you handle falls under a federal regulation (e.g., HIPAA or FERPA), you will be required to take additional precautions over and above those defined by ECU policies, standards and best practices.

The information in this guide is organized so that you can find the information you need easily and quickly. For each of the best practices you will find:

- *Best practice:* a brief statement on your responsibility for this practice
- *Your activities:* a list of actions for you to take that will help you adopt the best practice
- *Guidance:* additional background information on the best practice and its adoption
- *Relevant Standard:* a reference link to the underlying ECU Information Security Standard

For more information on your responsibilities for legal and regulatory compliance contact your supervisor or departmental compliance coordinator for assistance.

If you have general questions about information security requirements and practices, contact Pirate Techs at 252-328-9866 or 800-340-7081.

To learn more, review all of the underlying ECU Information Security Standards for Employees.

Applicability

All University employees and volunteers must adhere to the standards in this manual.

Baseline requirements

The standards in this manual represent a minimum, or *baseline,* set of requirements for information security. More stringent controls may be warranted, depending on the value and sensitivity of an information resource.

Alternative controls

In cases where a standard cannot be implemented due to technical limitations, operational disruptions, or excessive costs, alternative controls shall be implemented that provide a similar level of security or risk. The use of alternative controls shall be approved by the appropriate management authority to ensure that any changes in university risk are within acceptable tolerances.

Higher education environment

The standards in this manual are based on the *ISO 27002 Information Technology Security Techniques — Code of Practice for Information Security Controls*. These standards are designed for the University's operating environment and consider the unique aspects of our academic, research, service, administrative, legal, regulatory, and contractual activities and requirements.

Roles and responsibilities

These security manuals are organized according to the roles we serve at the University. While these roles are broadly defined, they are nonetheless helpful in defining our responsibilities for protecting the information resources in our care. These roles are defined as:

- *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 directors manage departmental operations and direct the use of departmental resources. 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.

Depending on your job duties or relationship with the University, you may serve multiple roles. For example, if you are a departmental manager, you would serve two roles: individual and management. Therefore, you would be responsible for adhering to the security standards associated with these two roles.

Depending on the type of information you handle, you may need to supplement this guidance with additional practices that are specific to your job role and responsibilities. For example, if you handle information that is protected by a federal regulation (e.g., student educational records or protected health information), you will be required to take additional precautions over and above those described in these best practices.

For more information on your responsibilities for legal and regulatory compliance, contact your supervisor. If you have general questions about information security requirements and practices, contact Pirate Techs at 252-328-9866 or 800-340-7081.

Definitions

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: desktop computers, laptops, tablets, smart phones, file servers, web servers, operating systems, networking devices, and software applications.

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.

University information: Information in any form (electronic, printed, spoken, etc.) that is collected, created, processed, stored, transmitted, or otherwise entrusted to the University in association with an authorized university activity.

Information Security Practices for All Employees

Employee Practice #1: Your responsibilities for information security

The Best Practice

Stay abreast of policies, standards, laws, and accepted practices that are relevant to what you do as an employee of the University and maintain the skills needed to carry out your information security responsibilities.

Your Activities

- Meet with your supervisor to review your responsibilities for information security and to identify the policies, standards, laws, and accepted practices that are relevant to your job duties.
- Complete required information security awareness training within 30 days of employment and refresher training at least once every two years.
- Consult with the relevant compliance offices as needed for guidance on specific compliance requirements.
- Work with your supervisor to assess your ability to fulfill your information security responsibilities, and to identify opportunities to develop and maintain the knowledge and skills you need to carry out those responsibilities.

Guidance

As an employee of East Carolina University, we're reminded that information security is everyone's business. The Information Security Regulation states that employees will take reasonable precautions to protect University Information from unauthorized and/or unlawful access, use, disclosure, destruction, and/or loss.

What you need to know about protecting University information depends on the nature of the information in your care. For example, if you handle personnel records for your staff, you should be aware of the most basic of security requirements and practices. This may include accessing the personnel records on the administrative computing system and not downloading them to your smartphone where they are vulnerable to loss or disclosure. However, if you manage a large database of highly sensitive healthcare records, you have a much higher duty of care and must adhere to a strict set of privacy, security, and regulatory practices.

Per ECU policy (Information Security Regulation) all ECU employees are required to complete information security awareness training within 30 days of employment and university designated refresher training at least once every two years. The official university designated training course is Employee Best Practices in Information Security Training which is available online in Cornerstone.

Your responsibilities for information security are conveyed through an assortment of official documents. These include your job description, employee performance plan, University policies, confidentiality statements, and software user agreements. External requirements, such as federal and state laws, often impose additional requirements that extend your responsibilities beyond those defined in official University documents.

If you are unsure of the security requirements that are relevant to what you do, contact your supervisor for assistance. You may also find that some of the information you handle is covered by a state or federal law and you may be directed to work with a compliance advisor in your area.

Besides the required information security awareness course for all employees, also offered at ECU are training opportunities related to several security-related specialized topics, including HIPAA privacy and security, GDPR, FERPA, and PCI compliance, and others. The ITCS Knowledge Base article Security Awareness Education at ECU on the university website summarizes security awareness training opportunities at ECU.

Your professional development is a shared responsibility between you and your supervisor. A key ingredient of this partnership is to maintain an ongoing dialogue with your supervisor about your professional development needs and potential learning resources.

Keep in mind that there are often many resource options for professional development. If you find that your first choice for a particular development resource is not practical for any reason, look around for alternatives. The options are plentiful, and you are likely to find other suitable learning resources.

Relevant Standards

- 1.1 Awareness and education

Employee Practice #2: Incident reporting

The Best Practice

Report security incidents and issues promptly through designated reporting channels.

Your Activities

- Promptly report security incidents and issues as you encounter them.

If you are unsure if a particular situation should be reported or to whom it should be reported, contact your supervisor for guidance. Besides reporting security concerns to your supervisor, university protocol is 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). 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.

Guidance

Do you know what to do if your ECU computer is stolen? What if you responded to a phishing email and fear your account is compromised? Do you or a coworker suspect that university data has fallen into the wrong hands? When you encounter a security concern or a security weakness, it is important that you report it through the appropriate channels and do so promptly. This allows the University to respond rapidly to contain the situation and the limit the impact to everyone involved.

The term, security concern, is any computer, network or university information-based activity which could result in misuse, damage, denial of service, compromise of integrity or loss of confidentiality of the ECU network, your computer (which is connected to the ECU network) and data (university information). Threats, misrepresentations of identity, or harassment of or by individuals using these resources can also result from a security concern. What is considered a reportable incident or issue depends upon the nature of the information you handle and the information systems you use. Security concerns you are required to report include, but are not limited to:

- Lost or stolen state/university computer or smart device
- Lost or stolen digital files containing sensitive information
- Unauthorized access to sensitive electronic information
- Unauthorized access to your computer
- Unauthorized access to a departmental information system or server
- Compromise of your ECU user account
- Disclosure of personally identifiable or sensitive information in response to a phishing scheme
- Compromise of your personally-owned computer or device containing any university data
- Unauthorized use of your user account
- Disclosure of sensitive data, email release or inadvertent posting of data on a websit
- Malware on your computer or university network
- Ransomware on your computer or university network

Relevant Standards

- 1.2 Reporting security weaknesses and events
- Report a Security Concern link

Employee Practice #3: Mobile computing security

The Best Practice

ECU is the legal owner of University Information. Before you access or store sensitive information on mobile laptops or devices, especially anything that might be used off-campus, you must:

- Obtain approval *prior to* storing sensitive information on your devices. As defined in the Mobile Computing Regulation, employees should access or store sensitive information only as authorized by the relevant data steward(s), compliance office(s), or University committee(s).
- Ensure all sensitive information stored on mobile devices is encrypted (Mobile Computing Regulation).
- As defined in the University Flexible Work Arrangement and Remote Work Regulation, sensitive information must not be processed or stored on a personally owned computer or device, but

instead must be processed on institutionally owned systems, stored in approved, secure remote storage, and accessed only by secure network access technologies (utilizing VPN or other multifactor authentication).
- Devices should be appropriately secure with such measures to include passphrase protection/PINs, up-to-date software and operating system security patches, anti-malware software, inactivity time-out, and physical device protection (Mobile Computing Regulation).
- Report the loss or theft of a mobile device to your supervisor, who shall ensure that ITCS and the relevant compliance office(s), data steward(s), university committee(s), and administrative head(s) are appropriately notified (Mobile Computing Regulation).

Your Activities

- Your use of mobile devices to conduct university business should be in accordance with university policies such as the Mobile Computing Regulation and University Flexible Work Arrangement and Remote Work Regulation.
- You are responsible for the protection of any sensitive information in your custody. Storage of sensitive information must be in accordance with approved storage and transmission mediums, and up-to-date guidance is available on the University Data Governance website, in the published document *Sensitive Data Storage and Transmission*: https://datagovernance.ecu.edu/sensitive-data-storage-and-transmission/

Guidance

Mobility versus security

Mobile devices take many forms and include such items as laptops, smartphones, tablets, removable hard drives, flash drives, and wearable computing devices. Because these devices are highly mobile by design, they are also highly susceptible to loss and theft. If you lose a mobile device that was used to store or access sensitive information, inform your supervisor immediately, and immediately notify Pirate Techs at 252-328-9866 or 800-340-7081.

As a general rule you do NOT store sensitive information on your mobile device or laptop. Storage of sensitive information must be in accordance with approved storage and transmission mediums, and up-to-date guidance is available on the University Data Governance website, in the published document *Sensitive Data Storage and Transmission*: https://datagovernance.ecu.edu/sensitive-data-storage-and-transmission/

Clear desk and screen policy. All employees should be mindful of best practice guidance as it pertains to adopting in your everyday habits a “clear desk and clear screen policy.” This means ensuring that sensitive information, both in digital and physical format, along with assets (e.g., laptops, smartphones, tablets etc.) are not left unprotected at personal and public workspaces when they are not in use, or when someone leaves his workstation, either for a short time or at the end of the day.

Home office. The home office has long been a popular choice for teleworkers, which only increased with the pandemic, but this presents special challenges in its own right. Family members and friends may be frequent visitors to the telework space and should be managed to prevent unauthorized access to university information. This may involve orienting your workstation so that others cannot view the information on the screen, locking the screen when not in use, and keeping the door closed when engaged in a conversation involving sensitive information.

Public areas. Likewise, when using a laptop, smartphone, or other device in a public or semi-public area (e.g., restaurant, airport, library, shared office cubicle area) be sure to prevent others from listening to sensitive conversations, viewing screen contents, or perusing email, voice mails, and stored data. Lock your screen when away from or not using your device.

Passwords and PINs
A security requirement is to set a passphrase or PIN directly on your mobile and telework devices. Beware of the auto login features of your mobile device. It is important that you do NOT configure your device in a way that allows anyone in possession of your device to have free and unimpeded access to your email account or other sensitive information. For example, if you leave your smart phone at a restaurant and another customer takes it home, they should not be able to access your email, work files, or any other university information system without entering a password or some other form of authentication.

Relevant Standards

- 1.3 Mobile and telework computing security

Employee Practice #4: Equipment and media disposal

The Best Practice

Remove all sensitive information from your computing equipment and media when selling, giving away or discarding them to prevent others from recovering the information.

Your Activities

- Assume that all data on a device includes sensitive information. It is unlikely that any device you handle contains only information that should be freely available to the public. Before selling, giving away or disposing of electronic equipment or media, contact Pirate Techs at 252-328-9866 or 800-340-7081 for current guidance on equipment and data sanitization.

Guidance

Assume that all data on a device includes sensitive information
When selling, giving away, or disposing of electronic equipment and media it is important that you remove all sensitive information so that it cannot be recovered by others. As a rule it is best to assume that if the device stores data, the data includes sensitive information. Thus, all of it should be removed. You don't have to look far to find news stories covering online purchases of used computers, copiers, and hard drives, which were later found to contain the personal information of others.

There's data on that?
Many of the electronic devices we use today are marketed as "smart" or "intelligent" and have the capability to store information internally. For example, you may be surprised to learn that our office printers and copiers may keep images of everything you printed or copied over the last few months. Think about that for a moment. Some of those printouts may include information you would rather keep private, such as SSNs, bank account numbers, employee performance reports, etc. Therefore, when

disposing or transferring electronic equipment to others, it is important to determine whether the equipment has the capability to store data. If so, be sure to have the data removed.

Removing all of the data
It is important to note that simple file deletions do not remove all data from storage media. Special forensic programs can be used to extract the data and rebuild some or most of the information on your devices. A common solution is to use a data wiping program to *sanitize* your devices before disposal. For other media, such as CD-ROMs and used hard drives with little commercial value, it may make sense to have them physically destroyed (e.g., crushed, shredded, or incinerated). For more information on the secure disposal of equipment and storage media, contact Pirate Techs at 252-328-9866 or 800-340-7081.

Relevant Standards

- 1.4 Equipment and media disposal

Employee Practice #5: Passphrases, passwords, and PINs

The Best Practice

Do not allow others to use or discover your passwords and be sure to use different passwords at work than you do for your personal accounts.

Your Activities

- Select *passphrases* that are easier to remember, and just as secure as, more complex passwords.
- Use different passphrases for your University user accounts than you do for your personal accounts.
- Hide your passwords so that no one else may see them, especially when logging in to a user account.
- Do not share your password with others, even as a favor to a friend.

Guidance

Passwords and passphrases
For now, passphrases/passwords are the most common form of authenticating our identity when accessing a University information resource. Passwords certainly have their problems. They can be difficult to remember. Avoid the urge to write them down on a piece of paper; it creates an additional problem by creating something else you must hide and secure. Fortunately, there are a few tricks that will help you select strong passwords that are easier to remember.

Consider using a different type of password, known as a *passphrase*. Passphrases are longer and more secure versions of passwords—that are *easier to remember*.

Password strength is based partly on how difficult it is for another person or software program to guess. The most difficult to guess passwords are those that use a variety of character types (e.g., upper case letters, lower case characters, numerals, and special characters) and are relatively long.

Password recommendations have historically focused on complexity and typically assume a password length of 6 to 10 characters. As you may imagine, as computing power has increased over time, our passwords have become easier to guess or crack with software. This is where the passphrase comes into play.

Passphrases are composed of a sequence of words and are often 12 to 15 characters or more in length. Passphrases derive their strength from their sheer length and a modicum of complexity, which will easily surpass the typical complex password. More importantly, passphrases are composed of meaningful words and are far easier for humans to remember. Chances are that you won't feel the need to write them down.

Separate your work and personal accounts and passwords
It's also good to keep your work and personal passwords separate. Do no use the same password for all. Doing so increases the likelihood that the password will be compromised. Then it's a short path for someone to gain access to your other accounts.

Relevant Standards

- 1.5 Passphrase selection and use

Reference – ECU Information Security Standards for Employees

1.1 Awareness and education

Purpose

To ensure that employees with access to university information resources maintain an awareness of applicable security requirements, understand their security responsibilities, and maintain the skills and knowledge necessary for fulfilling their responsibilities.

Standards

1.1.1 All employees (i.e., faculty, staff, student workers, vendors, contractors, and others conducting the business of the university) shall:

a) stay abreast of information security and privacy policies, standards, and practices that are relevant to their job roles and responsibilities

b) maintain a thorough understanding of their responsibilities for protecting the information resources in their care

c) maintain the knowledge and skills required to carry out their information security responsibilities

ISO 27002:2013 References

- 7.1.2 Terms and conditions of employment
- 7.2.2 Information security awareness, education, and training

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

1.3 Mobile and telework computing security

Purpose

To ensure that individuals using mobile or telework computing technologies protect university information resources from unauthorized access and use.

Standards

1.3.1 No sensitive information shall be stored on a mobile or telework computing device without prior authorization by the appropriate data steward or delegated management authority.

1.3.2 Mobile and telework computing devices that store sensitive information or provide access to sensitive information on other systems shall have adequate controls in place to protect against unauthorized access and use.

a) Access to sensitive information shall be password controlled in accordance with university passwords standards.

b) All sensitive information stored on a mobile or telework computing device shall be encrypted. When sensitive information is no longer needed for business purposes it shall be promptly removed from the mobile/telework computing device.

c) Sensitive information sent or received by a mobile or telework computing device shall be encrypted when transmitted over non-university networks.

d) Mobile and telework computing devices shall be properly maintained with regard to operating system, application, and security updates, and protected by anti-malware software and security software where applicable.

1.3.1 Mobile and telework computing devices that access or store sensitive information shall be physically protected from misuse, loss, and theft.

a) The use of a mobile or telework computing device in a public or semi-public area (e.g., restaurant or home office) shall be conducted in a manner that prevents unauthorized access to sensitive conversations, voice mails, screen content, remote applications, and stored data.

b) When a mobile or telework computing device containing sensitive information is lost or stolen, the event shall be promptly reported to the immediate supervisor of the person responsible for the device and to the ITCS Help Desk.

ISO 27002:2013 References

- 6.2.1 Mobile device policy
- 6.2.2 Teleworking

1.4 Equipment and media disposal

Purpose

To ensure that electronic equipment and removable media that is to be repurposed, transferred, discarded, or destroyed is done so in a manner that prevents the unauthorized disclosure of sensitive information.

Standards

1.4.1 All sensitive information on electronic equipment and removable media shall be permanently removed or destroyed prior to:

a) redeployment within the University
b) transfer of ownership to anyone external to the University
c) disposal by any means

1.4.2 Unless confirmed otherwise, it shall be assumed that any electronic equipment or removable media that is to be redeployed, transferred, or discarded contains sensitive information and shall be handled accordingly.

ISO 27002:2013 References

- 11.2.7 Secure disposal or re-use of equipment
- 8.3.1 Management of removable media

1.5 Passphrase selection and use

Purpose

To ensure that employees (faculty, staff, contractors, vendors, etc.) follow good practices for protecting their passphrases from disclosure and misuse.

Standards

1.5.1 Employees shall keep their passphrases confidential and not share them with coworkers or others.

1.5.2 Employees shall not use the same passphrases for work and personal user accounts.

ISO 27002:2013 References

- 9.3.1 Use of secret authentication information

Resources

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

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/
University Flexible Work Arrangement and Remote Work Regulation:
https://www.ecu.edu/prr/06/25/03