Best Practices in Information Security for Employees:

Standards for Protecting the Information in Your Care

East Carolina University
Information Security Office, ITCS

August 14, 2023

Information Security:
It's about more than technology.
It's about people.

Contents

Introduction

The standards presented in this manual arise out of three key guiding principles framed in ECU policy, in the Information Security Regulation. First, the standards recognize that university information is a strategic university asset upon which ECU depends to achieve its strategic objectives, carry out its mission, and fulfill commitments to stakeholders. Second, all employees are responsible for protecting the university information in their care. Third, information security is an essential business function of every department, a principle that highlights the importance of ensuring that university information and IT systems within every respective department are used appropriately and adequately protected. 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*. **This manual (Best Practices in Information Security for Employees: Standards for Protecting the Information in Your Care) is aligned with the security awareness training published in Cornerstone with a similar name** (Best Practices in Information Security for Employees: Protecting the Information in Your Care).

For the purposes of this manual, 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 may 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 Standards:* a reference link to the underlying ECU Information Security Standards.

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 IT Service Desk at 252-328-9866.

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 Security, Cybersecurity and Privacy Protection - Information Security Controls* (ISO/IEC, 2022). 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, whether they're assigned to ITCS or another department, and 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 the IT Service Desk at 252-328-9866 or 800-340-7081.

Definitions

Information security: Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to preserve the confidentiality, integrity, and availability of information resources and IT systems. The university's approach to managing and implementing information security emphasizes the three foundational elements of people, processes, and technologies.

Information system: A set of information resources, including applications, services or other information-handling components, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Sensitive information: Information regulated by law, protected by contractual terms, or framed in university data classification policy, thus requiring access controls appropriate to the sensitivity of the information to be protected. At ECU sensitive information is formally defined as Level 3 and Level 4 classifications in accordance with university data governance. Examples of sensitive information include personally identifiable information, social security numbers, student educational records, protected health information, confidential or restricted research data, credit card numbers, and critical IT infrastructure data.

University information: Information in any form (e.g., electronic, printed or spoken) that is collected, created, stored, distributed, or otherwise used by employees in the course and scope of their employment or volunteer responsibilities, for any university purpose. This can include education, research, creative activities, and service.

Information Security Best Practices for All Employees

Employee Practice #1: Stay up-to-date on your information security responsibilities

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 and document your responsibilities for protecting the information in your care. Work with your supervisor to ensure you have the skills and resources needed to carry out your information security responsibilities.
- Information security roles and responsibilities held by any individual who leaves or changes job roles should be identified and transferred to another individual, under the direction of the supervisor.
- Complete required information security awareness training within 30 days of employment and refresher training at least once every two years.
- If you handle information that is covered by a federal regulation, state law or contractual requirements, contact the relevant ECU compliance office for assistance, and be sure you're familiar with relevant guidance published on the University Data Governance website: https://datagovernance.ecu.edu/. If your employment involves handling data types such as FERPA, HIPPA, or payment card data (PCI), staying up-to-date on your information security responsibilities may include completing training specific to these topics and related security and privacy requirements.

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 basic security requirements and practices, which 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. If your responsibilities involve managing a large database of highly

sensitive healthcare records, you have an even 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 Best Practices in Information Security for Employees 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, PCI compliance, GLBA, 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. Information security roles and responsibilities held by any individual who leaves or changes job roles should be identified and transferred to another individual, under the direction of the supervisor.

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 Security awareness and education

Employee Practice #2: Report security concerns

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.

Timely, consistent and effective reporting of information security events is critical in order to prevent or minimize the effect of information security incidents. 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 IT Service Desk at 252-328-9866 or 800-340-7081. 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. Reporting requirements may vary depend on the type of data that you and your coworkers handle, and there may be unique reporting requirements for compliance areas including HIPAA and PCI.

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
- Evidence of tampering of computer, point-of-sale device, or network
- Malware on your computer or university network
- Ransomware on your computer or university network
- Disclosure of sensitive data, email release, or inadvertent posting of data on a website

Relevant Standards

- 1.2 Report Security Concerns

- Report a Security Concern link

Employee Practice #3: Practice safe mobile computing, use remote work safeguards, and follow clean desk policy.

The Best Practices

- ECU is the legal owner of University Information. 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.
- 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).
- As a general rule, all computers, including laptops and mobile devices, should be encrypted, and appropriately secured with measures to include password protection/PINs, up-to-date software and operating system security patches, anti-malware and endpoint security software, and inactivity time-out (Mobile Computing Regulation).
- Following clean desk policy is important for workplace security regardless of your work location.

Your Activities

- 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).
- 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/
- As a general rule all laptops and mobile devices should be encrypted as a safeguard.
- 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), and administrative head(s) are appropriately notified (Mobile Computing Regulation).
- Regardless of your work location, follow clean desk policy by locking up sensitive documents, locking your screen when leaving your computer, and securing mobile devices or removable media.

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 susceptible to loss and theft. If you lose a mobile device that was used to conduct

university business, inform your supervisor immediately, and immediately notify IT Service Desk 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/

Remote work safeguards and clean desk policy. All employees should be mindful of best practice guidance as it pertains to adopting in your everyday habits a "clean desk policy." This doesn't mean maintaining a tidy desk, rather a clean desk is secure, such that a passerby can't gain access to your computer, or unattended sensitive files or documents, whether they're electronic or paper. Wherever you do your work, that is your work space, this could be your on-campus office or cubicle, home office, even a coffee shop or airport. Clean desk policy means locking up sensitive documents, locking your screen when leaving your computer, and securing mobile devices or removable media. Following clean desk policy is important for workplace security regardless of your work location, because when it comes to protecting sensitive university information, there is no "I'll be right back."

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, keeping the door closed when engaged in a conversation involving sensitive information, and locking up information and securing the area when you finish working on official university business. Be sure you don't have personal or sensitive information visible when sharing your computer screen in a remote meeting.

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 or viewing sensitive information on your screen. Lock your screen when away from or not using your device or computer, and protect the equipment itself from theft by keeping it under your supervision.

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: Use strong passwords, don't share them, and never reuse the same password on multiple accounts.

The Best Practice

Use strong passwords that combine complexity and length, don't share them, and never reuse the same password on multiple accounts, being especially careful to always separate your work and personal accounts and passwords.

Your Activities

- ECU recommends the practice of using a complex passphrase that is at least 15 characters long.
- Keep passwords confidential and never share them with others, even as a favor to a coworker or friend.
- Never reuse the same password on multiple accounts, and keep work and personal accounts separate.
- Always enable MFA for any of your accounts if it's not already enabled by default.
- Consider adopting the use of a best-in-class passphrase manager service or KeePass Password Safe.

Guidance

Passwords and passphrases

Passphrases/passwords are the most common form of authenticating our identity when accessing IT resources, including at ECU. Keeping up with passwords may seem like a chore at times, they can be difficult to remember, but 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. There are several items of best practice guidance that can significantly strengthen your use of passwords and better protect your account credentials.

ECU recommends the practice of using a "passphrase" which is a handy way to create a strong password that can be easily remembered. Passphrases are based on meaningful words and are far easier for humans to remember. For example, something like "Today I ran on treadmill for 2 miles" is an easy to remember phrase and might become: TiranoTf2miles! (15 characters)

Password strength will determine how easy or difficult it will be for another person or software program to successfully guess it or crack it. The strongest passwords combine complexity and length. Complexity means using a combination of multiple character types, and ensuring your password is not easily guessable. Never use a word in the dictionary, or the name of a person, place, or thing (unless combined alongside multiple words in a passphrase). Password cracking studies have highlighted the importance of using long passwords, a strong password should be at least 15 characters long. Strong passwords are resistant to password spraying attacks and cannot be easily guessed. While we all may share the same sentiment with something like PurplePirates#1, although this is 15 characters it's easily guessable and would be a terrible password.

Separate your work and personal accounts and passwords

Never share your password with others, even as a favor to a coworker. Do not share your password with others – even your supervisor. You are not authorized to share your ECU accounts with anyone, even for

a few moments. If another employee is unable to use their own account, direct that person to the IT Help Desk for assistance.

Never reuse the same password on multiple accounts, doing so increases the likelihood of account compromise. If one account (such as a personal account) is compromised, it's a short path for a hacker to gain access to a university account such as your PirateID.

Enable Multi-factor authentication (MFA)
The use of MFA has been proven to significantly reduce the chance of account compromise. It's highly recommended that you enable MFA for any of your online accounts if it's not already enabled by default.

MFA (Multi-factor Authentication) is an enhanced security measure that requires both the user's passphrase along with a second method to verify identity. MFA has been described as requiring something that you know (passphrase) and something that you have (such as a phone) to verify identity. To manage two-step verification of user identify ECU has adopted Microsoft Azure technology which allows for several secondary methods of verification (text message, mobile authenticator app, and phone call). The university's SSO (single sign-on) system requires MFA when off-campus and when using the VPN.

Relevant Standards

- 1.4 Strong passphrase selection and use

Employee Practice #5: Learn to recognize and respond appropriately to various phishing attacks

The Best Practice

Because phishing attacks and similar social engineering tactics are a primary vector for malicious cyber activity that can impact the university, employees should recognize and respond appropriately to various phishing attacks.

Your Activities

- Be skeptical, and do not click links or attachments you're not sure are legitimate.
- Never reveal your passphrase to anyone.
- Report phish to phish@ecu.edu or submit a security concern to ITCS.
- Verify a sender. Call the business using a phone number from their website, or information from an official statement, bill, or credit card. DO NOT click the links in the email.
- Keep your anti-virus/malware software regularly updated.
- Update your computer and software. Install the latest patches and updates for your operating system and other software applications.

Guidance

As university employees it's important that we understand the connection between our own cyber behavior and the potential effects, positive and negative, on the university's information security. In your daily use of email, it's important to remain suspicious and be on your guard against potential social

engineering attacks that come your way through email messages. The vast majority of data breaches originate with a phishing attack. Don't take the bait! Interacting with the phishing messages can result in damage to your computer, theft of university information, identify theft, or network attack. Phishing attacks often play on your emotions or curiosity and are intended to trick you into reacting quickly and carelessly.

Types of phishing attacks

Phishing is one of the most common cyber security threats, and phishing emails in general try to look innocent and disguise themselves as legitimate messages. There are many types of phishing attacks, including common phishing, spearphising, clone phishing, whaling, vishing, and SMishing. Phish are baited with fraudulent content designed to make you a victim, and while they typically are delivered through email, phishing attacks can also some through text messages, phone calls, or printed mail.

- Common phishing: Common phishing typically doesn't target a single recipient but are sent in massive email blasts with the expectation that some percentage of recipients will take the bait.
- Spearphishing: Spearphishing targets a few specific recipients at a time. Whaling is a type of spearphishing targeted at a prominent individual, someone with influence or privileged, high-level access in an organization or company.
- Clone phishing is a sophisticated type of phishing that tries to duplicate the email signature, website, or brand of another trusted company or official. For example, it might provide a link to a storefront that's a counterfeit designed to mirror the real thing.
- SMishing and vishing are targeted against smartphone users, vishing comes through voice mails, with the attackers attempting to impersonate a company or organization in the attempt to steal private information or your credit card number. SMishing messages come through text massages, typically with a fraudulent link, prompting you to enter private information such as your account credentials, or download a malicious file.

Be careful of attachments

Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

Phishing Email – ITCS Knowledge Base article

ITCS has published a website article called Phishing Email that provides additional information on how to recognize and respond to phishing attacks, and how to report them.

InfoSec IQ training content

Published in Cornerstone are training segments on many pertinent security awareness topics including phishing, business email compromise, and malware.

Relevant Standards

- 1.5 Recognize phishing and other social engineering attacks

Employee Practice #6: Equipment and media disposal and information deletion

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 IT Service Desk 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 optical disks 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 IT Service Desk at 252-328-9866 or 800-340-7081.

Relevant Standards

- 1.6 Equipment and media disposal

Reference – ECU Information Security Standards for Employees

1.1 Security 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, through formal and informal training.

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 as relevant for their job function, and complete any required training.1.

1.1.2 Required security awareness training should include topics reflecting all essential information security best practices, including responsibilities for protecting sensitive information, the importance of reporting security concerns, practicing safe mobile computing, remote work safeguards, clean desk policy, password security policy, and recognizing and responding to various phishing attacks.

ISO 27002:2022 References

- 5.34 Privacy and protection of PII
- 6.3 Information security awareness, education and training
- 6.5 Responsibilities after termination or change of employment
- 6.6 Confidentiality or non-disclosure agreements
- 8.7 Protection against malware

1.2 Report security concerns

Purpose

To ensure that security concerns and events are reported in a timely and consistent way through appropriate channels in order to prevent or minimize the effect of information security incidents, and their 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.

1.2.2 Enhance user awareness and training by examining lessons learned from security incidents, and using such lessons to provide examples of what can happen, how to respond to such incidents, and how to avoid them in the future.

ISO 27002:2022 References

- 5.26 Response to information security incidents
- 5.27 Learning from information security incidents
- 6.8 Information security event reporting

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, regardless of their work location.

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) Employees should follow clean desk policy regardless of work location, locking their screen when leaving their computer, locking up or securing sensitive paper documents, and securing mobile devices or removable media.
c) 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 Service Desk.

ISO 27002:2022 References

- 6.7 Remote working
- 7.7 Clear desk and clear screen
- 7.9 Security of assets off-premises
- 7.10 Storage media
- 8.1 User endpoint devices
- 8.12 Data leakage prevention
- 8.24 Use of cryptography

1.4 Strong passphrase selection and use

Purpose

To ensure that employees (faculty, staff, contractors, vendors, etc.) follow best practices for selecting unique passwords that are kept confidential.

Standards

1.4.1 Employees shall keep their passphrases confidential and not share them with coworkers or others.
1.4.2 Employees shall not use the same passphrases for work and personal user accounts.
1.4.3 UNC System Standard 1400.3 requires multi-factor authentication (MFA) to protect sensitive information.
1.4.4 ECU Password Security Policy defines the university's requirements for strong passwords to safeguard against password spraying, password cracking, or other account compromise.

ISO 27002:2022 References

- 5.17 Authentication information
- 8.5 Secure authentication

1.5 Recognize phishing and other social engineering attacks

Purpose

Train employees to recognize phishing attacks and similar social engineering tactics as a primary vector for malicious cyber activity, and how to respond appropriately.

S*tandards*

1.5.1 Employees should understand the potential consequences (positive or negative) of their own behavior on the university's information security posture.

1.5.2 Employees should understand that phishing attacks and similar social engineering tactics are a primary vector for malicious cyber activity that can impact the university.

1.5.3 While phish, which can contain various malicious attachments, links, or deceitful content, are most often delivered through email, fraudulent messages can also come through text messages, phone calls, or printed mail. Employees should recognize various types of phishing attacks and how to respond appropriately.

ISO 27002:2022 References

- 6.3 Information security awareness, education and training
- 8.23 Web filtering
- 8.7 Protection against malware

CIS Controls References

- 14.1 Establish and maintain a security awareness program
- 14.3 Train workforce members to recognize social engineering attacks

1.6 Equipment and media disposal and information deletion

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

1.6.1 Storage media should be managed through their life cycle of acquisition, use, transportation, and disposal in accordance with the university's data classification and handling requirements.

1.6.1.1 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

1.6.2 Information stored in information systems, devices, or in any other storage media should be deleted when no longer needed or required, according to retention and disposition requirements.

1.6.3 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 27002:2022 References

- 7.7 Clear desk and clear screen
- 7.10 Storage media
- 7.14 Secure disposal or re-use of equipment
- 8.10 Information deletion

Resources

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

IT Security - Compliance (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
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