Best Practices in Information Security for

IT Support Staff

Protecting the Information in Your Care

East Carolina University

September 14, 2015

Contents

Introduction

The best practices in this guide are designed to help you—as an IT support staff member—*fulfill your responsibilities for protecting the information and IT Systems in your care.* For the purposes of this guide, "IT support staff member" is defined as:

an employee who provides technical or user support of a university owned or managed IT System or service to other persons, regardless of their affiliation with the university.

Please keep in mind that the best 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 and IT Systems under your control are 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 the IT Help Desk at 252.328.9866.

To review all of the underlying ECU Information Security Standards, please click the link below.

ECU Information Security Standards Manual

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*. 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.
- *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 the IT Help Desk at 252-328-9866.

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: Any information for which disclosure may adversely affect individual privacy, public safety, or University operations and obligations. Examples of sensitive information include: student educational records, protected health information, data network diagrams, account passwords, and documents containing the locations of hazardous materials.

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 IT Support Staff

IT Services Practice #1: System acquisition, development and maintenance

The Best Practice

Integrate all relevant information security requirements into the business requirements for new and upgraded information systems and confirm the requirements are met *prior to placing them into production*.

Your Activities

- Confirm that the business requirements of new and upgraded information systems include all relevant security requirements before system selection, design or acquisition.
- Notify the information system owner or project manager of any security requirements that are absent in the business requirements.
- Confirm through testing or other means that the security requirements have been met prior to placing the new or upgraded information system into production.

Guidance

Information security is a business requirement

All University business (including academic and research functions) require that University Information and IT systems are secure and available when needed. To ensure our information resources are adequately protected, information security must be an integral component of the business requirements for any new or upgraded IT system.

When security is addressed *after* an IT system has been purchased or developed, scarce University resources are wasted and the University is faced with unnecessary risks to its information and IT systems. More specifically, we often find that:

1) additional, unplanned product and service purchases are required, resulting in unnecessary cost
2) manual workaround processes are often required, stealing time away from university personnel on a daily basis until the IT system can be replaced
3) many security weaknesses cannot be resolved, creating unnecessary risks to the University for the life of the IT system
4) some of the new IT system's features cannot be used for security reasons, preventing users from realizing the intended business benefits

Administrative efficiencies – a lost opportunity

A common reason for investing in a new IT system is to gain administrative efficiencies. However, when security requirements are absent from the business requirements, it is common to find that the gains in

efficiency are quickly lost when the new system is implemented. Additional staff time is diverted to manual processes and can quickly eclipse that saved by the purchase of the system. In addition, some of the administrative efficiencies are not realized, because one or more product features cannot be used for security reasons.

Technology and staffing requirements

All technology and support staffing needs must be addressed in the planning stages of a new or upgraded IT system. This will ensure the IT system provides the expected functionality and reliability. Examples of such needs include the funding of external service agreements, allocation of support staff, acquisition of infrastructure hardware or software and training of end users.

System testing and assessment

Before placing a new or upgraded information system into production, take whatever actions are necessary to confirm the security requirements are met, such as conducting system configuration reviews and vulnerability scans. Report the results to the information system owner or project manager as appropriate.

When security requirements can't be met

If you find that a new or upgraded system cannot meet security requirements, *you are required to take alternative precautions to reduce the risks to acceptable levels*. For example, if a new IT system is unable to enforce University password requirements at user login, you should establish a departmental password procedure, train your staff on the procedure, and regularly remind your staff of their obligations under the procedure.

Relevant ECU Information Security Standards

ECU Information Security Standard 5.1

IT Services Practice #2: Application data security

The Best Practice

When developing a software application, integrate data integrity controls into the application and data handling processes to ensure your application data is correct and appropriate.

Your Activities

- Include automated checks in the application to ensure data is validated on input for correctness and appropriateness.
- Confirm through automated or manual processes that processed data is correct and appropriate prior to distribution and reporting.
- Establish and follow a routine process for resolving data errors.

Guidance

Garbage in, garbage out

It is important that you incorporate data validation tests into your application testing procedures. This will provide you with assurances that your applications will detect and resolve common data problems. For example, if the incoming data is expected to be a numeric quantity that must fall within a particular value range, your application can be designed to automatically reject invalid entries.

Your applications may also be vulnerable to attack if the nature or size of the incoming data is not verified to be appropriate. For example, a buffer overflow attack can disrupt and take control of an application by forcing more data into an input field than is expected, overwriting a portion of the application program with malicious code. This type of attack is often used to gain access to account passwords and other privileged information. Fortunately, buffer overflow attacks are becoming less of an issue as newer application development environments provide memory management features that automatically prevent such attacks.

In addition, you should ensure that your information systems validate data at its output points as well. This is often accomplished with a combination of automated data checks and manual reviews by system owners and functional users.

Client-server architecture data security

If you are working within a client-server architecture, you can also utilize *dual data validation* to further ensure the data values processed by your applications are accurate and appropriate. Dual data validation is a common security practice, where the data values are confirmed to be of the correct type and within expected parameters (e.g., proper string length or numeric range) on both the client and server sides of the application architecture. The client side validation allows users to quickly identify and correct data issues at the entry point. And the server side validation adds a second level of security by confirming that the data values are correct and accurate before processing or storing for future use.

Protecting data in transit

Data in transit between applications and especially across public networks is susceptible to capture and tampering. Where appropriate, protect the data in transit with an established security protocol, such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL).

Relevant Standards

ECU Information and Security Standard 5.2

IT Services Practice #3: Sensitive Test Data

The Best Practice

Obtain approval before using sensitive data for testing, secure the data during testing, and remove the data promptly after testing.

Your Activities

- Obtain approval for the use of sensitive test data prior to testing.
- Identify any sensitive data elements in the proposed test data and remove all sensitive data elements that are not essential to the testing process.
- Ensure that adequate controls are in place to protect all remaining sensitive data.
- Avoid using live production data for testing to protect against modifying live data in use.
- Remove sensitive test data promptly when no longer needed for testing purposes.

Guidance

Testing environment security

If you must use sensitive information for your testing, be sure to strengthen the security controls in your test environment to an appropriate level and restrict access to those persons with a clear business need. A far better alternative is to modify the test data so it no longer contains sensitive information.

Live production data

There is a crucial difference between *live* production data and a *copy* of production data in the testing environment. Live production data is that which is currently in use for University operations and, if altered or erased, directly impacts those operations. Whereas a copy of production data, if altered, does not directly impact University operations–unless that data is subsequently moved into production use. Therefore, as a rule you should not use live production data for testing. You may consider using a copy of production data once you've taken all the proper precautions (e.g., approval, security and prompt removal).

Old test data

It is far better to remove test data after testing and recreate it when needed, than to keep copies of old data that are subsequently forgotten and misplaced. Old test data has a knack for showing up on repurposed servers many months or even years after the testing was completed. This is an all too common source of data breaches in the news. So, do not keep test data indefinitely unless you are tracking the data and are confident you can keep it secure.

Relevant Standards

ECU Information Security Standard 5.3

IT Services Practice #4: Application Source Code

The Best Practice

Restrict access to your application source code and development resources to prevent unauthorized code changes.

Your Activities

- Limit access to program source code and development resources to only those persons with a clear business need for access, such as application developers and managers.
- Develop written procedures for authorizing and implementing changes to program source code, libraries and related items.

Guidance

Source code, a blueprint

Application source code is one of the most critical University information assets; it is essentially a blueprint of our application software. Unauthorized changes to source code—unintended or otherwise—can cause application malfunctions that result in the loss of an IT service, an interruption of University operations and a corruption of University data. Limit access to program source code and ensure your development team follows written procedures for implementing changes, including the migration from development/test environments into production.

Source code management

You should actively manage the development and security of your application source code so that you have reasonable confidence that the resulting applications function as expected. Toward this end you should limit access to your code to only those persons who are formally authorized. This will require a combination of user access management and secure storage technologies (such as encrypted drive partitions and data backups).

In addition, you should follow a version control methodology to coordinate and track changes to your source code. This is especially useful when working in a distributed, collaborative environment where multiple developers may be working on the same application concurrently. Version control will allow you to track code changes and attribute them to specific persons, coordinate the "check out" of code to prevent unintended code loss, restore code to previous and more stable versions, and store your code in a secure repository.

Relevant Standards

ECU Information Security Standard 5.4

IT Services Practice #5: Outsourced software development

The Best Practice

Supervise outsourced development work to ensure it meets application development standards, functional requirements and contractual obligations.

Your Activities

- Before development work begins, formally define and document intellectual property rights, source code ownership, licensing agreements, and rights to audit.
- Test the work at key development stages to identify and resolve work quality and security issues.
- Confirm that the development work meets University and contractual requirements before signing off on the completion of work.

Guidance

Contracted work is your responsibility

It is important to closely monitor and supervise the outsourced development process to guard against unmet functional requirements, missed project deadlines, and security vulnerabilities in the finished product. Supervise your outsourced software developer to ensure that:

- legal issues, such as intellectual property rights, source code ownership, licensing agreements and rights to audit are agreed to in writing prior to the start of work
- the software is tested for security vulnerabilities prior to being put into production
- the resulting work meets University and contract requirements

Inspect the outsourced work during critical junctures in the development process to ensure it is proceeding as expected. This will enable you to identify and resolve issues early and avoid missed deadlines and cost overruns from last minute contract changes. Managing the work throughout the development process will help you avoid situations where you may feel pressured to accept lower quality work due to an impending deadline or a potential cost overrun.

Relevant Standards

ECU Information Security Standard 5.5

IT Services Practice #6: Change management

The Best Practice

Use a formal change management process to guide and control changes to your information systems.

Your Activities

- Use existing campus resources for change management such as change management committees, system testing procedures and templates for change requests and approvals.
- Wherever practical, test changes to assess their impact to the target system, other information systems and business functions.

Guidance

Preventing unanticipated problems

Consider a formal change management process for major system changes that can have a substantial impact to your information system or University business. A formal process should include:

- written description of the requested changes and their potential impacts
- testing of the requested changes
- implementation plans for the requested changes
- reviews of and authorizations for the requested changes

However, a formal process can require considerable effort on the part of you and your staff and may not be suitable for managing all information system changes. Consider a simplified change management process for changes with limited impact. A simplified process provides you with the basic benefits of change management, yet requires a smaller investment of your time and energy. The objective is to routinely analyze, test and plan the changes to your information systems in order to prevent unanticipated problems for your information systems and University business.

System testing can be difficult, but worth it

It may be tempting to forgo the testing of a proposed change, because of the sheer effort to do so. Regardless, testing is far superior to a theoretical analysis of what may or may not occur when a change is introduced to a system. You will find that system testing often uncovers unexpected problems, giving you the opportunity to address the issues before your users are impacted.

When documenting your change tests and their results, be sure to describe the limitations of the testing environment. This information will prove useful when planning similar tests in the future.

Relevant Standards

ECU Information Security Standard 5.6

IT Services Practice #7: Separation of production and test environments

The Best Practice

Where feasible, maintain separate development, test and production environments to prevent unauthorized changes to your production systems and data.

Your Activities

- Review your system development and testing needs and create separate development, test and production environments where feasible.
- Where feasible, establish unique user accounts and passwords for each of the development, test and production environments.

- Where it is not feasible to maintain separate environments, implement alternative controls to reduce the likelihood of unauthorized changes to your production systems and data.
- Work with your staff and fellow team members to segregate development, test and production support duties so that unauthorized production system changes are unlikely.

Guidance

Segregation of duties

Segregation of duties involves separating the duties of your team so that no one person can access or modify an information system or data without authorization or detection. As you may suspect, limited staffing is a common obstacle. You may find that your team has too few people to completely segregate the development, test, and production duties. For those that cannot be segregated, your team should implement other controls that will detect unauthorized activities or events. If you cannot prevent an event, make every effort to detect it so you can act on it.

To err is human . . . and expected

Simple human error can inflict as much damage as a malicious attack. At some point we have all lost track of which information system we're using and tried to make a changes to the wrong system. Imagine the harm that could come about when a developer momentarily loses track of the system in use and mistakenly makes changes to a production system. Regardless of the intent, the harm is done. A common solution is to limit or prevent development staff from gaining access to production systems. This may involve tasking a team member with moving software into production on behalf of a developer.

When segregating environments consider the following controls:

- Segregate support duties between production and non-production environments.
- Establish and follow formal processes for transferring software from development to production environments.
- Deploy development and production software on separate information systems, processors, domains or directories.
- Display system banners or other information that identifies the development, test or production environment in which the user is currently operating.

Change management in software development

Where practical, the person developing code changes should be different from the person who places those changes into production. Consider using software *deploys*, which are collections of code files that can be deployed together as a set to the test and production environments. Be sure to acquire approval of the changes prior to placing the software deploy into production.

Relevant Standards

ECU Information Security Standard 5.7

IT Services Practice #8: Software and operating system maintenance

The Best Practice

Where feasible maintain your software applications and operating systems at version levels supported by your software providers.

Your Activities

- Establish a software "patch strategy" for your information systems that achieves an appropriate balance between system stability, data security and service availability to your clients.
- Stay informed of new software and system updates by monitoring product release notices.
- Analyze product release notices to determine whether an update should be implemented in accordance with your patch strategy and to establish an implementation plan.
- Where it is not feasible to implement an update or maintain a supportable product version, implement alternative controls to provide a suitable level of security and notify your supervisor of the decision to do so.

Guidance

Updates are essential, but problematic

There are many reasons for software maintenance. Software updates provide new features, fix application problems, resolve security weaknesses and ensure the continued support of a software provider. However, software updates often come at a cost and may not always be practical.

For example, you may find that a software update undermines the security or stability of your system and may even disrupt a business process. Consequently, it is important that you weigh the benefits of a software update against its potential harm. You can assess the potential harm by testing the updates in an isolated operating environment or by monitoring the results of installations at other sites.

When you cannot maintain your software at a level supported by the software provider, it is important that you routinely assess the security of the software and address the risks. This is necessary, because the risks associated with any software vulnerabilities will change as the operating environment changes.

It is important that you define a "patch strategy" for managing the software updates to your information systems. Your patch strategy will serve as a decision guide, reducing the analysis needed for individual updates and will yield greater consistency in how the system updates are handled.

Relevant Standards

ECU Information Security Standard 5.8

IT Services Practice #9: Information system inventories

The Best Practice

Maintain an inventory of your information systems to support the needs of your department and the University for business continuity, disaster recovery and compliance.

Your Activities

- In collaboration with your supervisor, identify the information systems in your area that are mission critical or that handle sensitive information covered by a University policy, federal regulation or state law.
- Document each of the identified information systems as needed for business continuity, disaster recovery and compliance. At a minimum, document the system name, owner and purpose, as well as the information handled by the system.
- Inventory the hardware associated with the system where needed for asset management and tracking.

Guidance

Critical information systems

Critical information systems are those that are essential to the ongoing operation of the University and must continue to function in the event of a disaster. Review your business continuity and disaster recovery plans with your supervisor to confirm which of your systems are deemed critical and should be documented in an inventory.

It is important that you have a disaster preparedness plan for your critical information systems. The disaster preparedness plan should identify the fundamental hardware and software information needed to rebuild your system after a system failure, fire or other adverse event. In addition, the departments that depend on your critical information system should have business continuity plans that describe how they will continue their operations whenever your information system is unavailable for any reason.

Sensitive information systems

Sensitive information systems are those that collect, store or process sensitive information–and if compromised, could lead to an unauthorized data disclosure. *Sensitive information* is a broadly defined term that covers practically any information that, when disclosed, can cause harm to individuals or the University. Consult with your supervisor to identify which of your systems are deemed sensitive and should be documented in an inventory.

If you have determined that your system handles sensitive data, you must also determine the nature of that data. Sensitive data is likely to be subject to a university policy, federal regulation, state law or a contractual requirement. Any of these may give rise to additional system administrative duties that are necessary for ensuring your systems comply with all policy, legal, regulatory or contractual requirements.

Simplify your inventory by grouping your systems

You may have a number of similar information systems or systems that are composed of many components that together serve a single purpose. For these you may find it helpful to group the systems or components to simplify inventory tracking and documentation.

Using existing inventories

When the system information needed is already available from existing sources, you may find that it is not necessary to create a separate inventory. However, if you must gather information from multiple sources before it may be used, you may wish to consolidate the information into a single inventory so that you can quickly provide it to those responding to disasters, service outages, security events or compliance requirements.

Relevant Standards

ECU Information Security Standard 6.1

IT Services Practice #10: Documented operating procedures

The Best Practice

Document your system operating procedures and periodically review them to keep them current and relevant.

Your Activities

- Identify the support and maintenance processes that are essential to ensuring the secure and reliable operation of your information systems.
- Document each of the essential processes and periodically review to keep them current and relevant.
- Place the procedures in a location readily available to anyone who may need them.

Guidance

Why document?

Although *you* may not need a written procedure for your daily activities, you may not always be the person who must carry out those activities. If you are unavailable for any reason, another person will need a written procedure to follow to ensure your information systems continue to operate reliably and securely. To facilitate the transition of duties (either temporarily or permanently) document the steps for providing others with access to the needed resources and development/working environments.

You will also find that a written procedure is an invaluable reference for those non-routine tasks that you carry out infrequently. Here, a written procedure will save you time and eliminate costly mistakes that can occur when you are re-learning such tasks.

Procedure maintenance

To ensure that your information systems are operating properly, it is important that you review your written procedures at least once a year and whenever changes occur to an information system or its operating environment. Examples of changes that may warrant a procedure review includes those that may occur in operating system software, applications, hardware, data backup requirements, business processes or electronic communications with other systems.

Documented reviews

You should document the reviews of your procedures. At a minimum your documentation should include the date of the review, the person conducting the review, and a description of any notable changes to the procedure.

Procedure approvals

Any procedure changes should be formally approved by an appropriate management authority. This may be carried out by way of a signed paper copy, a confirmation email or another means of showing evidence of the approval. The appropriate management authority will depend on the situation and may be a direct supervisor, an area manager, or a departmental director.

Where are the procedures?

Make your operating procedures readily available to all persons who need them. Avoid situations where you must be personally available at the moment others need access to a procedure. If you are unavailable to carry out an operating process, you are also unavailable to locate or grant electronic access to a procedure.

Relevant Standards

ECU Information Security Standard 6.2

IT Services Practice #11: Physical Security

The Best Practice

Take precautions to protect your sensitive and critical information systems from physical and environmental threats, such as equipment theft and damage, fire and flood, excess heat and humidity and power failures.

Your Activities

- Identify the information systems in your area that are mission critical or that handle sensitive information covered by a University policy, federal regulation, state law or contractual requirements.
- Periodically review the physical security controls for your sensitive information systems to identify areas in need of improvement.
- Develop a plan for implementing controls for the areas of greatest risk.

Guidance

Simple and intuitive

Compared to the complexity of technical security measures, physical security is a much simpler affair and something that we already understand quite well. When you review the physical security of your systems, you may find that the necessary door locks are already in place and that creating a reception area is a simple matter of rearranging desks. The goal is to restrict physical access to your critical and sensitive information systems to only those persons with a business need to do so. Where practical and appropriate, consider additional controls for added security, such as:

- Escorting visitors and recording their identity, purpose of visit and entry/exit times
- Using access control cards and monitoring cameras to protect access to secure areas

Environmental dangers

Physical security is not limited to preventing unauthorized human access. It also encompasses disruptive events such as a fire or flood, which can cause serious damage. Locate your information systems and equipment so that are protected from physical and environmental threats.

Example safeguards include:

- A separate heating, ventilation and air conditioning (HVAC) unit to protect from temperature and humidity extremes and to filter out dust and other particulates
- An uninterruptible power supply (UPS) to protect against power failures, surges and line noise
- A raised floor or cushioned equipment mountings to guard against excessive vibration
- Clearly labeled and documented equipment and wiring to facilitate rapid resolution of cable failures and reduce patching errors

Where are you located?

Although it is difficult to conceal the locations of your sensitive or critical information systems, avoid signage or other public announcements. Limiting public awareness reduces the likelihood of a spontaneous attack or other disruptive event.

Relevant Standards

ECU Information Security Standard 6.3

IT Services Practice #12: Data backup

The Best Practice

Back up your data and software in accordance with your business continuity and disaster recovery needs.

Your Activities

- Be familiar with the types of data stored on your information systems, the frequency at which the data changes and its importance to your clients.

- Based on the nature of the data and its importance to your clients, establish a backup strategy for your information systems.
- Periodically review the data backup requirements of any applicable business continuity and disaster recovery plans and adjust your written data backup schedule as appropriate.
- Store your data backups in secure locations to prevent loss, damage or unauthorized access.

Guidance

Ensuring your data is available when needed

The purpose of a data backup is to ensure that the data is available in the aftermath of a system failure, data loss from human error, utility outage, disaster, or other disruptive event. Also, store your backups at a secure location that is unlikely to be affected by the same events that impact your information systems.

Review your business continuity and disaster recovery plans to determine the frequency and retention cycles for your data backups. If you are unable to meet your continuity or recovery objectives, inform the persons responsible for those planning efforts. They may adjust their plans or help you acquire the resources necessary to meet the continuity and recovery data backup needs. Document the resulting data backup schedule for future reference.

An unpleasant surprise

There are few things more frustrating than dutifully backing up your data month after month, only to find that your backup data cannot be restored after a system failure. There are a number of reasons why this can occur. The physical media degrades over time and fails; the backup software is misconfigured and does not capture all of the data; and an equipment failure sends corrupted the data to the backup media. These are good reasons for routinely test your backup media.

In general, it is too resource intensive to test the restoration of all of your backups. So, the general practice is to periodically restore a sampling of your data backups to ensure they are viable and contain the data you need.

Relevant Standards

ECU Information Security Standard 6.4

IT Services Practice #13: Technical vulnerability management

The Best Practice

Proactively manage the technical vulnerabilities of your information systems (e.g., software applications and operating systems) to minimize the risks of system compromises, data disclosures and business disruptions.

Your Activities

- Routinely identify and evaluate the technical vulnerabilities of your information systems and remediate those vulnerabilities in a timely, effective and systematic manner.
- Where practical, test and evaluate critical system patches to identify and resolve any problems prior to implementation. Where testing is impractical, analyze the implementation results at other sites to determine how they may apply to your information systems.
- Where system patches are not available for high risk vulnerabilities, implement alternative measures that achieve an acceptable level of risk.

Guidance

Patch it quick, but not too quick

Vulnerability patches are often released in short order to help you quickly resolve your system's vulnerabilities. However, in an effort to ensure you are quickly informed of a recently discovered vulnerability, patches are often released before their impacts to system stability and security are fully understood. Therefore, you should test and evaluate system patches before installing them on your systems.

When evaluating the potential impacts of a system vulnerability consider not only the primary system involved, but also other systems and networks to which it is connected. An attack may exploit vulnerabilities on one system and use that as a springboard to gain access to other systems.

When testing is not feasible

If it is not feasible to test a system patch, you should monitor and review the test results at similar sites. While test results from other sites may not be as relevant as those from your own environment, they are valuable nonetheless for identifying and evaluating the potential impacts to your systems.

When no patches are available

There are times when there are no system patches immediately available for a reported vulnerability. In such cases, minimize the risks to your systems by implementing alternate controls, such as turning off the affected service or switching to more secure technologies or processes. While alternative controls may not be the preferred approach, they are often a necessary part of due diligence for managing the security of your systems.

Relevant Standards

ECU Information Security Standard 6.5

IT Services Practice #14: Malicious code protection

The Best Practice

Use automated protection against malicious code and supplement with alternative controls where appropriate.

Your Activities

- Adopt a multilayer strategy to protect your systems from malicious code infections. Your strategy may include automated malicious code detection, code isolation, and signature updates.
- If your malware protection software is insufficient, implement alternative controls, such as firewall restrictions, system log reviews, and infected system isolations.

Guidance

Automation, replication, consternation

Malicious code (i.e., viruses, worms, Trojan horses) is of great concern to IT support staff, because it automates the exploitation of your system vulnerabilities and can do so on a grand scale. One moment your system is functioning at peak efficiency, and the next it is struggling to keep up with the processing demands of a rapidly replicating virus.

Malicious code is so prevalent in today's computing environment and changes so frequently, that protecting against malicious code infections is an arms race. As soon as you implement protections from one virus, two more are released into the wild. Consequently, it is impossible today to protect your systems from malicious code without automation.

Automated countermeasures

Your best countermeasure against malicious code is to utilize an automated malware detection and prevention system that programmatically updates its detection signatures. The protection software should also be capable of isolating malicious code and repairing damage to limit the spread and impact of an infection.

Compensating controls

Where automated malware protections are unavailable it is important that you employ compensating controls. These include network segmentation, firewall filtering, and system log reviews. Even when you have suitable malware protection, you may find it helpful to adopt such controls to enhance your ability to manage malware threats.

Relevant Standards

ECU Information Security Standard 6.6

IT Services Practice #15: Information system monitoring

The Best Practice

Regularly monitor your information systems so that you may detect and act on events that impact system performance, security and compliance.

Your Activities

- Stay current on the logging solutions that are available for your information systems.
- Configure your systems so that all events applicable to system performance, security and compliance are recorded in your system logs for review and action.
- Regularly review your system logs to identify events that require attention or corrective action.
- Retain your system logs as appropriate to support system maintenance, security reviews, incident investigations, and compliance assessments.

Guidance

Early detection is the key

While vulnerability management and malware protection may catch a large number of problem events, there are other system events that can only be detected through log review and analysis. Early detection of these events can mean the difference between a temporary inconvenience and a full scale system breach. For example, pay special attention to security-related events such as account login failures that may indicate a brute force attack on the system's user accounts. Also pay attention to successful logins that are logged outside of normal work hours and may indicate a compromised account.

Logs, logs, and more logs

As part of your log management process, you should define log retention cycles, storage needs, event escalation procedures and an approach to automating system log reviews. Keep in mind that logs can generate a tremendous amount of information, overrunning your storage systems and your capability to review them. Automating the log review and event escalation process (e.g., automated alerts for specific events or thresholds) ensures that important events are detected—and reported in a timely manner.

Your audit logs should contain—where appropriate—user account name, network names and addresses, and information on key events. Examples of key events include attempted and successful logins, system faults and configuration changes and the use of privileged accounts and utilities.

Relevant Standards

ECU Information Security Standard 6.7

IT Services Practice #16: Tech compliance reviews

The Best Practice

Arrange for regular reviews of your information systems to assess their technical compliance with information security standards and requirements.

Your Activities

- Identify the persons and resources needed to conduct technical compliance reviews of your information systems for all applicable standards, regulations, laws, policies and contractual requirements.

- Establish and oversee a technical compliance review schedule for your information systems.
- Report the results of the reviews to the appropriate University management areas.

Guidance

So many requirements

You will probably find that the technical compliance requirements for your information systems are many and complex. That is because the requirements arise from a patchwork of different compliance sources, such as policies, standards, regulations, laws and contracts. Given the breadth and depth of these requirements, you will find it helpful to enlist the help of others with the knowledge and skills necessary to assess your systems in each of the compliance areas.

It is important that your technical compliance reviews be documented and reported to the appropriate compliance areas. At a minimum, the review documentation should provide the date of the review, the identity of the reviewer and the findings of the review.

Compliance review schedule

To help you manage your technical compliance reviews and demonstrate ongoing compliance, establish a regular review schedule. This will ensure a reasonable level of compliance even as changes occur in your information systems, the technical environments in which they operate and the compliance requirements themselves.

Relevant Standards

ECU Information Security Standard 6.8

IT Services Practice #17: Network Security

The Best Practice

Actively manage network security to ensure the protection of the network infrastructure, connected information systems and applications, and University information in transit on the network.

Your Activities

- Conduct periodic reviews of network security controls to ensure the security of University information and information systems on the University network.
- Establish special controls for information and information systems that use wireless or public network services provided or procured by the University.
- Coordinate network management with other service areas to ensure a consistent level of security throughout the University computing infrastructure.
- Establish processes and tools for detecting, analyzing, and acting on relevant security events.
- Ensure third party network services and contracts adhere to all relevant University security requirements.

Guidance

Network security

The University network is the backbone of an institution's electronic communication services, which connects every student, employee, administrative office and academic function. The network has proven to be an incredibly valuable asset that allows us to deliver information to anyone at any time and any place.

However, our dependence on network communications presents certain risks to University business. For example, a single, compromised laptop can place the University at risk of data disclosure, operational disruption and compliance failure. Consequently, the University network should be treated as the first line of defense against network-based threats to University information and information systems and must be closely monitored.

It is also important that periodic reviews of network security controls are performed to identify security weaknesses and opportunities for improvement. Because the electronic communications environment is constantly changing, network controls review should be performed periodically and whenever there is a notable change in the technical or threat environment.

Public and wireless services

Public and wireless networks are inherently less secure than traditional wired networks and require just as much attention to security as the University's internal network services. If you provide technical or user support for public or wireless network services, consider employing additional measures to limit unauthorized access to University information systems. For example, you may block public network access to critical University systems at the router or firewall.

Third party network services

The use of third party network services requires the same level of attention to security as the University network. If you are involved in outsourcing a network service to a third party, it is important that you ensure the service adheres to all relevant University requirements. This is best accomplished by addressing those requirements in the contract language and managing the contract to ensure those requirements are met as the services are delivered.

Relevant Standards

ECU Information Security Standard 6.9

IT Services Practice #18: Information security incident management

The Best Practice

Report information security incidents promptly and in accordance with an established response process.

Information security incidents shall be reported by technical support personnel to allow for timely action by university administration, legal affairs, privacy officers, compliance functions, and other responsible parties.

Your Activities

- Review the incident response procedures for your area to determine your responsibilities for reporting and responding to security events.
- If your incident response responsibilities are not clearly defined, work with your supervisor to define and document your responsibilities for incident response.
- Ensure incident response procedures require the timely reporting of incidents so that other University functions (e.g., compliance, legal, privacy and senior administrators) can respond promptly to all University obligations.
- If you are responsible for maintaining an incident response procedure, conduct after-incident reviews to identify areas for improvement.

Guidance

When to report a possible incident

You may find it difficult at times to know *when* you should report a *potential* incident. As part of your duties you may routinely investigate system errors and anomalies—any of which may be symptoms of an incident. The problem is that the cause of the error or anomaly may not be apparent until your investigation is well underway. Even then, you may not be able to confirm that the event is a security incident. Thus, it can be difficult to determine when the probability of an incident is sufficient to report.

To complicate matters, if you report a potential event too early, it can lead to inaccurate assumptions and flawed response actions. On the other hand, if you report an incident after you've concluded your investigation and confirmed your findings, the opportunities to contain the incident and mitigate damages will be lost. The solution to this dilemma falls in between the two.

Report in stages

One approach to reporting security incidents is to do so in stages and deliver the information as a series of status reports. As details emerge and a better understanding of the event emerges, you can distribute reports more widely and with more information.

The information included in a status report is as important as the information that is not included. Stick with what is known. Avoid speculation. Speculations are like rumors—they spread quickly, are taken as fact and are sometimes acted upon with unfortunate repercussions.

When reporting on the status of an incident, be clear about what has been confirmed and what has NOT been confirmed. For example, be careful of reporting that the system owner stated no sensitive data was stored on the compromised system without also reporting that the hard drive analysis has not yet confirmed this. Otherwise people will assume that no data was involved, and you will be left to explain

the discrepancy in your reporting when the analysis reveals a cache of data containing sensitive information.

Forensics

If you are not trained in the rules of evidence or do not have the required tools to conduct a valid forensic investigation, do not attempt to gather evidence. This is likely to render all evidence unusable for legal and human resource actions. Contact the IT Help Desk for guidance.

Relevant Standards

ECU Information Security Standard 6.10

IT Services Practice #19: User account management

The Best Practice

Establish and follow a clearly defined process for authorizing, provisioning and managing user account access.

Your Activities

- If you do not have an access authorization process, work with your supervisor to identify the persons with decision authority for approving access to your information systems and create a simple, repeatable authorization process.
- Establish a process for provisioning user access according to authorized access rights.
- Establish a process for periodically reviewing and modifying access rights as authorized rights change. This occurs when an employee changes position, takes on new duties, transfers to another department or separates from the University.
- Request the weekly Human Resources report of employee terminations. Use this report as a safety net to ensure you revoke the accounts of all separating employees.

Guidance

User account management

Do not allow user access to your information systems to exceed what is reasonably needed for business purposes. Excess privileges often result in unauthorized data access and changes. This is why it is important that you have a formal authorization process.

Access rights - a moving target

One of the biggest challenges you will face is keeping users' access rights aligned with their *authorized* access rights as their job duties change. This can occur when a person takes on new duties within the same position or transfers to another University position. To manage user access rights you should:

1) Periodically review your users' access rights and resolve any discrepancies.

2) Remind supervisors in your area to notify you whenever their staff members change duties, positions, or leave the employ of the University.
3) Sign up for the weekly employee termination report from Human Resources.

Shared accounts

The need for shared user accounts may arise when using a software application with a rudimentary user account structure. For example, a single 'administrator' account is provided for use by multiple people. Regardless of the reason for using shared accounts, you should take steps to associate the activities of the shared account with specific individuals. This may be as simple as keeping an account use log, which documents the employee, times of use, etc.

Special service accounts

Service accounts are a special type of account, often used to programmatically run a specific application or service without user interaction. To ensure that an unauthorized user cannot assume control of one of these accounts, you should employ additional controls, such as limiting the locations from where the account can be accessed and limiting the account's privileges to a specific program service or task.

Relevant Standards

ECU Information Security Standard 7.1

IT Services Practice #20: Privileged access management

The Best Practice

Regularly monitor privileged account use and review privileged access rights to ensure your staff members have only the access they need to carry out their support duties.

Your Activities

- Limit privileged access rights to your information systems to that which is specifically required for technology support services.
- Regularly review and document the privileged access rights to your systems.
- Promptly revise privileged access rights when such rights are no longer needed.
- Log the activities of privileged access sessions as needed for security reviews, incident investigations and compliance requirements.

Guidance

The power of privileged access

Privileged accounts are essential to maintaining the health and performance of our information systems. By their nature privileged accounts require access rights that far exceed those of normal users. Such access rights enable the support staff to configure, repair and change the basic operation of an information system and even change production data.

However, privileged access can create serious problems. Critical system services may be accidently misconfigured or shutdown and valuable data may be altered or destroyed. Minimize the potential for harm by limiting your staff members' privileged access to that which is specifically required for technology support purposes.

Privileged access on an as needed basis

Grant privileged access on an as needed basis and promptly revoke the access when it is no longer needed. To reduce the window of exposure, grant privileged access for specific times that coincide with a particular task schedule and revoke the access afterward.

Privileged access on normal accounts

Wherever feasible, do not provide normal user accounts with privileged access rights. A technical support person, who is using a normal account with elevated privileges, may inadvertently cause harm to an information system while performing routine user tasks. Thus, it is important to limit the use of normal user accounts with elevated access privileges. Where it is not feasible to separate normal user accounts and privileged access, implement other controls to monitor use and limit access as much as is practical.

Documenting access rights

To help you track the assignment of privileged access rights, document them in a form that is easy to maintain. This may be as simple as keeping a list of authorized personnel and a description of their access rights. Consider the including the following information in your documentation:

- user IDs
- date, time and nature of key events
- programs and utilities used
- system start-ups and shut downs
- I/O device attachments and uses

Monitoring privileged account activity

Regularly review the activity logs for your privileged access sessions. Promptly investigate any potential violations of authorized access rights, system security or University policy and respond accordingly. It is important that you respond promptly to contain the event and limit the potential impacts of a misuse of privileged access rights. In situations where you do not have the means to log privileged access activities, implement other measures to track and control the use of your privileged accounts. This could involve manual signups for account usage, limiting access from specific locations, etc.

Relevant Standards

ECU Information Security Standard 7.2

IT Services Practice #21: Passphrase security

The Best Practice

Control the selection and use of passphrases (passwords) on your information systems to limit opportunities for unauthorized account use.

Your Activities

- Configure your information systems to enforce University passphrase requirements at user login for password length, complexity, expiration and reuse. If your information system is not able to do so, contact the IT Help Desk for guidance.
- Establish a process for securely communicating new and temporary passphrases to users.
- Promptly change default product and vendor account passphrases to prevent unauthorized access.

Guidance

The official passphrase requirements

You will find the official University passphrase requirements in *ECU Information Security Standards* document (see Reference section). The requirements provided here are for illustrative purposes only and should not be relied on as official requirements.

Enforcement at login

Configure your information systems to enforce the ECU passphrase requirements at login:

- Passphrases shall be at least 8 characters in length.
- Passphrases shall contain characters from at least 3 of the 4 character classes: numeral, upper case letter, lower case letter, and special characters (!, @, #, *, ?).
- Passphrases shall be changed at a minimum of once every 90 days and shall not use any of the user account's previous 6 passwords

Alternative controls

If your information systems cannot meet University passwords requirements, you must implement alternative controls to provide an *equivalent* level of access control security. Unfortunately, it is not uncommon to find that a product lacks the necessary enforcement controls. For example, a specialized software application may limit passwords to 6 characters or less, which prevents users from selecting passwords that meet University requirements for minimum password length. Examples of alternative controls include: using highly complex passwords (when password length is an issue), working with the software provider to provide a fix that allows strong passwords, switching to a different product altogether, limiting access to the product from specific end user devices, and so on.

Legacy password systems tend to focus primarily on password complexity and less so on password length. Because password strength is based primarily on complexity and length, legacy systems often result in short, complex passwords that are difficult to crack and difficult to remember. Fortunately,

within this framework we can also use a different type of password, known as the *passphrase, which is easier to remember and just as secure.*

A passphrase is a longer version of the password and relies more on length than complexity. You can create a passphrase from a word phrase or sentence, yielding a passphrase of 10 characters or more in length. By using mixed-case characters and adding a numeral or special character, a passphrase can be easy to remember, yet very difficult to crack.

New account passwords and password resets

You should also implement controls over assigning "new" or "reset" passwords (to new users or those who forget their password, respectively) to guard against that password being disclosed. These measures include authenticating the requesting user's identity, selecting a password that is difficult to guess, communicating the password in a secure manner and requiring the password be changed at the user's first login.

Default and vendor account passphrases

Default product and vendor accounts and default passphrases are well known and frequently sought out as a simple means to gain unauthorized access to an information system and possibly an institution's network. Therefore, it is important that you disable default accounts and change default passphrases at the earliest possible moment during implementation or maintenance.

Relevant Standards

ECU Information Security Standard 7.3
Link to Passphrase Standards

Reference - ECU Information Security Standards for IT Support Staff

5. Information System Acquisition, Development, and Maintenance

Information security requirements must be integrated into the business specifications that drive the selection, development, and maintenance of information systems.

5.1 Security requirements for information systems

Purpose

To ensure that security requirements are included in the business requirements for new information systems and changes to existing information systems.

Standards

5.1.1 Information security requirements shall be documented and integrated into the business requirements for new information systems and for changes to existing information systems.

5.1.2 New information systems and changes to existing information systems shall be tested or otherwise confirmed to meet security requirements prior to placement into production.

ISO 27002 References

- 12.1.1 Security requirements of information systems

5.2 Application data security

Purpose

To ensure that applications developed by or on behalf of the University have adequate controls to ensure the integrity of university information on data input, processing, output, and reporting.

Standards

5.2.1 Data shall be validated for correctness and appropriateness before it is processed by an application.

5.2.2 Data created or processed by an application shall be confirmed to be correct and appropriate before distributed for use.

5.2.3 Procedures for validating data and resolving data errors shall be established and maintained.

ISO 27002 References

- 12.2.1 Input data validation
- 12.2.2 Control of internal processing
- 12.2.4 Output data validation

5.3 Protection of test data

Purpose

To ensure the use of sensitive data for testing purposes is appropriately authorized, secured, and managed.

Standards

5.3.1 Test data shall not include sensitive information, unless it is essential to the testing process and its use is approved by the appropriate management authority.

5.3.2 Test data containing sensitive information shall have adequate controls in place to prevent unauthorized access, use and disclosure.

5.3.3 Live production data (as compared to a copy of production data) shall not be used for testing purposes. Controls shall be in place to prevent information system development processes from modifying live production data.

5.3.4 Where practical, sensitive test data shall be removed when no longer needed for testing or business purposes.

ISO 27002 References

- 12.4.2 Protection of system test data

5.4 Protection of program source code

Purpose

To prevent unauthorized and unintentional functional changes to program source code.

Standards

5.4.1 Access to program source code and related items, such as application specifications, shall be controlled to prevent unauthorized access and source code changes.

ISO 27002 References

- 12.4.3 Access control to program source code

5.5 Third party source code development

Purpose

To ensure that outsourced software development adequately protects the University's intellectual property rights, meets functional and security specifications, and fulfills contractual requirements.

Standards

5.5.1 Outsourced software development work shall be supervised to ensure that:

a) Intellectual property rights, source code ownership, licensing agreements, and rights to audit are clearly established and documented before start of work.

b) The work is tested to identify any security issues and concerns, such as weak data controls or known security vulnerabilities.
c) The work is confirmed to meet contract requirements.

ISO 27002 References

- 12.5.5 Outsourced software development

5.6 Change management

Purpose

To ensure that changes to information systems do not compromise the security of university information and information systems.

Standards

5.6.1 The introduction of new information systems and changes to existing information systems shall be controlled through formal change management processes.

ISO 27002 References

- 12.5.1 Change control procedures

5.7 Separation of development, test, and production environments

Purpose

To reduce the risk of accidental or unauthorized misuse of production information systems that may arise from an insufficient separation of development, test, and production environments.

Standards

5.7.1 Development, test, and production systems shall be sufficiently separated to prevent unauthorized access and changes to production systems and data.

5.7.2 Where practical, a segregation of technical support duties shall be maintained to limit opportunities for the accidental or unauthorized misuse of university information and information systems.

ISO 27002 References

- 10.1.3 Segregation of duties
- 10.1.4 Separation of development, test, and operational facilities

5.8 Maintenance of operating system and application software

Purpose

To ensure that operating system, application, and other software are maintained in accordance to business, technology and security needs.

Standards

5.8.1 Where practical and appropriate, software (e.g., operating systems and applications) software shall be maintained at a version level supported by the software provider.

ISO 27002 References

- 12.4.1 Control of operational software

6. Information Technology Security

The provisioning and management of information technology services have considerable impact on the security of university information systems and the information the systems process, store, or transmit. Many of the standards in this section provide are closely aligned with best practices in information technology management.

6.1 Information system inventory

Purpose

To ensure that all information systems are documented and have designated owners with oversight responsibility for information system management, security, and compliance.

Standards

6.1.1 All sensitive or critical information systems shall be inventoried in a manner that meets the needs of business continuity, disaster recovery, incident response, and compliance processes. The inventory shall include the following at a minimum:

a) description of the information system
b) description of the information collected, processed or stored by the system
c) the technical contact person for the information system
d) the owner of the information system

ISO 27002 References

- 7.1.1 Inventory of assets

6.2 Documented operating procedures

Purpose

To ensure the secure and reliable operation of university information systems.

Standards

6.2.1 Operating procedures for university information systems shall be documented and made available to all persons who need them.

6.2.2 Operating procedures shall be reviewed annually to ensure they remain current and relevant.

6.2.3 The review of operating procedures shall be documented to indicate the:

a) date of review

b) name of the person(s) conducting the review

ISO 27002 References

- 10.1.1 Documented operating procedures

6.3 Physical security

Purpose

To prevent unauthorized physical access to university information systems.

Standards

6.3.1 Physical access to critical and sensitive information systems shall be controlled and limited to authorized personnel only.

6.3.2 Critical and sensitive information systems shall be physically protected from disruptive events, such as fires, floods, civil disorders, and hazardous material contaminations.

6.3.3 Information system equipment shall be located to provide protection from physical threats, such as excess heat and humidity, power failures, and equipment damages and thefts.

ISO 27002 References

- 9.1.1 Physical security perimeter
- 9.1.2 Physical entry controls
- 9.1.3 Securing offices, rooms, and facilities
- 9.1.4 Protecting against external and environmental threats
- 9.1.6 Public access, delivery, and loading areas
- 9.2.1 Equipment siting and security
- 9.2.2 Support utilities
- 9.2.3 Cabling security

6.4 Information backup

Purpose

To ensure that information and software essential to critical university operations remain available.

Standards

6.4.1 Backups of information and software essential to university operations shall be taken regularly and in accordance with disaster recovery and business continuity objectives.

6.4.2 Information and software backups shall be stored in secure locations to prevent loss, damage, and unauthorized access.

ISO 27002 References

- 10.5.1 Information back-up

6.5 Technical vulnerability management

Purpose

To ensure that technical vulnerabilities of University information systems (e.g., software applications and operating systems) are managed to minimize the risks of system compromises, data disclosures, and business disruptions.

Standards

6.5.1 Technical vulnerabilities of information systems shall be identified, evaluated, and appropriate measures implemented in a timely, effective, and systematic manner.

6.5.2 Where practical, critical software patches shall be tested and evaluated to identify and resolve any problems prior to implementation. Where testing is impractical, implementation plans shall consider the implementation results of other sites.

6.5.3 Where software patches are not available, alternative measures (e.g., turning off affected services) shall be taken to mitigate risks.

ISO 27002 References

- 12.6.1 Control of technical vulnerabilities

6.6 Protection against malicious code

Purpose

To ensure that university information resources are adequately protected from malicious code.

Standards

6.6.1 Information systems shall be protected against malicious code infections and attacks. Where technical limitations prevent the use of commonly available software and tools, alternative controls shall be implemented to provide a similar level of protection.

ISO 27002 References

- 10.4.1 Controls against malicious code

6.7 Information system monitoring

Purpose

To ensure that unauthorized activities and unexpected events on information systems are detected and acted upon in accordance with university policy, relevant legal requirements, and information system performance needs.

Standards

6.7.1 All applicable events shall be recorded in audit logs as necessary for the effective management of user access, system performance, and system security.

6.7.2 System audit logs shall be:

a) retained for access control management, system maintenance, and security investigations
b) protected from unauthorized modification, loss, or destruction
c) reviewed to identify events in need of attention or corrective action

ISO 27002 References

- 10.10.1 Audit logging
- 10.10.2 Monitoring system use
- 10.10.3 Protection of log information
- 10.10.4 Administrator and operator logs
- 10.10.5 Fault logging

6.8 Technical compliance reviews

Purpose

To ensure that university information systems are regularly reviewed for technical compliance with information security standards and requirements.

Standards

6.8.1 Information systems shall be regularly reviewed for technical compliance with all applicable standards, regulations, laws, policies, and contractual requirements.

6.8.2 Information system compliance reviews shall be performed by or under the supervision of persons with the requisite knowledge and skills.

6.8.3 Information compliance reviews shall be documented, submitted to the appropriate management authority, and shall include the:

a) date of the review
b) name of the person(s) conducting the review
c) findings of the review

ISO 27002 References

- 15.2.2 Technical compliance checking

6.9 Network security

Purpose

To ensure the security of the university network infrastructure is managed in a way that protects the network, the information it contains, and the information systems that use it.

Standards

6.9.1 The security of the university network infrastructure shall be managed to ensure that information systems using the university network and the information flowing within the network are appropriately protected.

6.9.2 Third party network services and contracts, such as Internet connectivity services, shall adhere to the security requirements of the University. In situations where the University does not directly manage a network services contract, the persons managing the contract shall be notified of the requirements.

ISO 27002 References

- 10.6.1 Network controls
- 10.6.2 Security of network services

6.10 Information security incident management

Purpose

To ensure information security incidents are reported and managed in a timely and effective manner by technical support functions.

Standards

6.10.1 Information security incidents shall be reported by technical support personnel to allow for timely action by university administration, legal affairs, privacy officers, compliance functions, and other responsible parties.

6.10.2 Incident management responsibilities shall be defined and documented to ensure an orderly and effective response to information security incidents.

ISO 27002 References

- 13.1.1 Reporting information security events
- 13.1.2 Reporting security weaknesses
- 13.2.1 Responsibilities and procedures
- 13.2.2 Learning from information security incidents
- 13.2.3 Collection of evidence

7. Access Management

The underlying principle behind access management is that of avoiding unnecessary security risks by restricting user access to that which is specifically needed for business purposes. This involves managing access throughout the user account lifecycle.

7.1 User account management

Purpose

To ensure that access to university information systems is provisioned and managed in accordance with authorized access rights.

Standards

7.1.1 Access to university information resources shall be controlled and managed to prevent unauthorized access and use.

a) Access rights shall be authorized by the appropriate management authority prior to granting user access to university information resources.

b) Unique user accounts shall be used wherever possible so that user account activities may be associated with specific individuals. When shared user accounts are necessary, they shall be approved by the appropriate management authority.

c) Access rights shall be reviewed periodically and as soon as is practical after changes occur in an individual's roles, responsibilities, or relationship with the University.

ISO 27002 References

- 11.2.1 User registration
- 11.2.4 Review of user access rights
- 11.5.2 User identification and authentication

7.2 Privileged access management

Purpose

To ensure that privileged access is controlled so that such access is limited to that which is specifically required for technology support purposes.

Standards

7.2.1 Privileged access to university information systems shall be limited to that which is specifically required for technology support services.

7.2.2 The activities of privileged access sessions shall be logged as needed for information security management, incident investigations, and compliance requirements.

7.2.3 Privileged access rights shall be documented and reviewed regularly.

ISO 27002 References

- 10.10.2 Monitoring system use
- 11.2.2 Privilege management
- 11.2.4 Review of user access rights
- 11.5.1 Secure log-on procedures
- 11.5.2 User identification and authentication
- 11.5.3 Password management system

7.3 Passphrase security

Purpose

To ensure strong passphrases (passwords) are selected, managed, and protected from unauthorized use.

Standards

7.3.1 Passphrases used to provide access to university information resources shall adhere to the following minimum requirements:

a) Passphrases shall be at least 8 characters in length.

b) Passphrases shall contain characters from 3 of the 4 character classes:

- Numeral
- Upper case letter
- Lower case letter
- Special character (e.g., !, @, #, *, ?)

c) Passphrases shall be changed at a minimum of once every 90 days and shall not use any of the user account's previous 6 passwords.

7.3.2 New user account passphrases and temporary passphrases shall be controlled to prevent disclosure to unauthorized persons. This shall include:

a) authenticating a person's identity before providing a new or temporary passphrase

b) providing new or temporary passphrases that are difficult to guess by others

c) delivering new and temporary passphrases securely, and in a separate communication from new account notifications

d) requiring temporary passphrases to be changed upon login

7.3.3 Default product and vendor account passphrases shall be secured to prevent unauthorized access. Where technically feasible this shall include:

a) changing the default vendor passphrase immediately after account activation

b) disabling the account when it is no longer needed or between maintenance sessions

ISO 27002 References

- 11.2.3 User password management
- 11.5.2 User identification and authentication
- 11.5.3 Password management system

Resources

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

Information Technology & Computing Services (ITCS): www.ecu.edu/itcs
ECU IT Security: www.ecu.edu/itcs/help/security.