Best Practices in Information Security for

Administrative Heads

(Department Directors)

Protecting the Information in the Care of Your Department

East Carolina University

October 16, 2015
Contents

Introduction ........................................................................................................................................... 3
Definitions ............................................................................................................................................... 4
Information Security Practices for Administrative Heads ................................................................. 5
  Management Practice #1: Employee awareness, acknowledgements and responsibilities .......... 5
  Management Practice #2: Information system compliance ............................................................ 6
  Management Practice #3: Physical security of employee work areas ............................................. 7
  Management Practice #4: Continuity of operations (COOP) planning ......................................... 9
Reference: ECU Information Security Standards for Administrative Heads ..................................... 11
Resources ............................................................................................................................................... 15
Introduction

The best practices in this guide are designed to help you—as the Administrative Head of your department—fulfill your responsibilities for protecting the information and IT Systems in the care of your employees. For the purposes of this guide an “Administrative Head” is defined as:

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

Best practices and standards

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

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

Baseline requirements

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

Alternative controls

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

Higher education environment

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

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

- **Employee**: A person employed by the University or who serves as a University volunteer. This includes anyone performing work on behalf of the University, such as staff and faculty members, student workers, contractors, and unpaid volunteers.

- **Administrative Head**: The administrative director of a University department, such as an academic department chair, administrative department director or college dean. Administrative Heads direct departmental operations and the use of university resources within the department.

- **IT Support**: an employee who provides technical or end user support of a university owned or managed IT system or service to other persons, regardless of their affiliation with the university.

For guidance on your responsibilities for regulatory compliance, contact the relevant ECU compliance office. If you have questions about the ECU best practices and standards in information security, contact the IT Help Desk at 252-328-9866 for assistance.

**Definitions**

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

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

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

Management Practice #1: Employee awareness, acknowledgements and responsibilities

The Best Practice
Ensure your employees’ information security responsibilities are clearly defined, conveyed and fulfilled.

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

Guidance
Information security is about people, not technology
Information security is far more about people than it is about technology. Any employee can circumvent our security technologies and place ECU and the people we serve at risk. Such actions can disrupt university operations; create compliance failures and financial penalties; and breach the privacy of our students, employees, and healthcare patients who entrusted us with their personal information.

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

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

Periodic employee acknowledgements
Employee acknowledgements benefit both the employee and the University. A good acknowledgement statement not only provides a clear statement of responsibilities to the employee, it also documents the employee’s receipt and understanding of this information for the University. In short, a signed acknowledgement statement allows our employees to confirm that they are aware of and understand their information security responsibilities.
Periodic employee acknowledgements provide greater assurance that your employees are up to date on the latest risks to ECU information, as well as any corresponding adjustments to their responsibilities. Fortunately, you can take advantage of existing acknowledgement processes that are administered centrally, such as those provided by ITCS when employees access various IT services. However, your managers should also integrate employee-specific information security responsibilities into formal job descriptions and performance management plans, where they are reviewed and signed periodically by your employees.

**Employee skills, resources and motivation**

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

*If your employees work with regulated information, such as patient treatment information or student educational records, your managers should ensure your employees participate in the appropriate compliance training.* For guidance on employee awareness and training contact the appropriate compliance office or the Information Security Office at 328-9866.

In addition to ensuring your employees have the necessary skills and resources, *your managers must ensure your employees have the motivation to fulfill their responsibilities.* A common approach is to formally integrate information security responsibilities into job descriptions and performance management plans. This ensures that your employees are aware that they are accountable for fulfilling their information security responsibilities, just as they are for any work responsibility.

**Relevant ECU Information Security Standards**

- ECU Information Security Standard 2.1.1
- ECU Information Security Standard 2.2.1 – 2.2.2

**Management Practice #2: Information system compliance**

**The Best Practice**

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

**Your Activities**

- Assign responsibility to a designated person(s) for documenting the policy, legal and contract requirements that are relevant to your departmental information systems and IT services.
- Direct your managers to ensure all information systems and IT services provided or administered by their respective areas adhere to the relevant compliance requirements.
• Assign responsibility to a designated person(s) for periodically reviewing compliance, identifying areas of noncompliance and documenting corrective actions.

**Guidance**

*Begin with ECU policies and standards*

ECU information security policies and standards are based on the same basic security practices as many regulations, laws, and industry standards. You will find that by complying with University policies and standards you will have a head start on complying with many of the external requirements that apply to your department’s activities.

*Assign responsibility for compliance management and reporting*

It is important that you assign responsibility to a person or persons within your department for periodically assessing your compliance efforts, identifying compliance gaps, and developing remediation plans. This will allow you to review your compliance levels on a moment’s notice and be prepared to take advantage of opportunities for improvement as they arise.

*Third-party (outsourced) IT services*

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

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

**Relevant Standards**

- ECU Information Security Standard 4.1.1 – 4.1.2
- ECU Information Security Standard 4.2.1 – 4.2.2

**Management Practice #3: Physical security of employee work areas**

*The Best Practice*

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

*Your Activities*

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

**Guidance**

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

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

**Physical security in layers**

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

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

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

**Third party service personnel**

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

**Protect your data backups**

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

As an alternative to removable backup media, which are highly susceptible to theft and loss, consider backing up your data directly to an ECU departmental Piratedrive. The ECU Piratedrive system is located in a secure data center and is well protected from unauthorized access. For assistance with establishing a departmental Piratedrive contact the IT Help Desk at 328-9866.
Relevant Standards

ECU Information and Security Standard 2.3.1

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

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

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

Guidance

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

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

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

**Disaster recovery planning versus business continuity planning**

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

**Protect University information during business continuity and recovery activities**

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

**Relevant Standards**

ECU Information Security Standard 3.1.1 – 3.1.2
ECU Information Security Standard 3.2.1 – 3.2.2
ECU Information Security Standards for Administrative Heads

2.1 Information education and awareness

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

*Standards*
2.1.1 All employees with access to university information resources shall be:
   a) informed of their information security responsibilities as appropriate to their job duties and responsibilities
   b) trained in information security practices that are relevant to their information security responsibilities
   c) periodically reminded of information security policy, statutory, and regulatory requirements that are relevant to their job duties and responsibilities

*ISO 27002 References*
  6.1.3 Allocation of information security responsibilities
  8.1.3 Terms and conditions of employment
  8.2.1 Management responsibilities
  8.2.2 Information security awareness, education, and training

2.2 Acknowledgments of responsibility

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

*Standards*
2.2.1 The information security responsibilities of all employees with access to university information resources shall be formally documented as appropriate to their roles and responsibilities with the university.
2.2.2 Employees shall formally acknowledge their information security responsibilities. The acknowledgements shall be:
   a) obtained prior to gaining access to university information resources or as soon afterward as is practical
   b) renewed on a periodic basis
   c) documented for reporting and assurance purposes
ISO 27002 References
8.1.1 Roles and responsibilities
8.1.3 Terms and conditions of employment
8.2.1 Management responsibilities

2.3 Securing office and work areas

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

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

ISO 27002 References
9.1.3 Securing offices, rooms, and facilities

3.1 Business continuity management

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

Standards
3.1.1 All ECU mission essential functions and critical departmental functions shall be covered by business continuity plans to ensure such functions will continue in the event of a disaster, service outage, human error or other disruptive event.
3.1.2 Business continuity and disaster recovery plans shall address all relevant information security requirements to ensure the protection of information resources during business continuity and disaster recovery activities.

ISO 27002 References
14.1.1 Including information security in the business continuity management process
14.1.2 Business continuity and risk assessment
14.1.3 Developing and implementing continuity plans including information security

3.2 Business continuity plan maintenance

Purpose
To ensure that business continuity and recovery plans remain effective and relevant as changes in the business or threat environments occur.
Standards
3.2.1 Business continuity plans and disaster recovery plans shall be reviewed annually and whenever there is a significant change in the business environment. The reviews and their results shall be documented.
3.2.2 Business continuity plans and disaster recovery plans shall be tested annually and whenever there is a significant change in the business environment. The tests and their results shall be documented.

ISO 27002 References
14.1.4 Business continuity planning framework
14.1.5 Testing, maintaining and re-assessing business continuity plans

4.1 Legal, regulatory and contractual compliance

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

Standards
4.1.1 All information stored or processed by an information system shall be protected from loss, destruction or misuse in accordance with applicable legal, regulatory and contractual requirements.
4.1.2 All legal, regulatory and contractual requirements applicable to an information system shall be documented and made available to the appropriate management authority.

ISO 27002 References
15.1.1 Identification of applicable legislation
15.1.3 Protection of organizational records
15.1.4 Data protection and privacy of personal information

4.2 Policy and standards compliance

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

Standards
4.2.1 Information systems shall be regularly assessed for compliance with university information security standards and requirements.
4.2.2 All operational processes involving the use of sensitive information shall be regularly reviewed for compliance with university information security policies, standards, and guidance.
4.2.3 Areas of noncompliance shall be evaluated to identify the causes of noncompliance and document corrective actions.

**ISO 27002 References**

15.2.1 Compliance with security policies and standards
15.2.2 Technical compliance checking
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](http://www.ecu.edu/itcs)
ECU IT Security: [www.ecu.edu/itcs/security.cfm](http://www.ecu.edu/itcs/security.cfm)