As an Administrative Head you are responsible for ensuring the security of all University Information as it is collected, created or handled by your department, and the security of IT services provided by your department. This handout summarizes four basic management practices that will help your department take precautions to protect the information and IT systems in its care.

**Best Practice #1: Ensure your employees’ information security responsibilities are clearly defined, conveyed and fulfilled.**

a) Direct your managers to integrate relevant information security responsibilities into employee job descriptions, performance plans, business processes and routine communications.

b) Ensure your employees formally acknowledge their responsibilities on a periodic basis.

c) Charge your managers with ensuring your employees have the skills, resources and motivation necessary to fulfill their information security responsibilities.

**Best Practice #2: Ensure the management and use of information systems and IT services within your department comply with all relevant policies, standards, laws and contracts.**

a) 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.

b) Direct your managers to ensure all information systems and IT services provided or administered by their respective areas adhere to the relevant compliance requirements.

c) Assign responsibility to a designated person(s) for periodically reviewing compliance, identifying areas of noncompliance and documenting corrective actions.

**Best Practice #3: Ensure your managers take appropriate precautions to prevent unauthorized physical access to sensitive information in your employee work areas.**

a) Direct your managers to take reasonable precautions to prevent unauthorized physical access to sensitive information in all forms (electronic, printed, and spoken) in all employee work areas.

b) 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.

**Best Practice #4: 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.**

a) Designate a Continuity of Operations (COOP) Coordinator with responsibility for developing your departmental COOP plan.

b) 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.

c) 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.

For more information visit: [http://www.ecu.edu/cs-itcs/security.cfm](http://www.ecu.edu/cs-itcs/security.cfm)