As an ECU employee you are responsible for taking reasonable precautions to protect the information in your care from misuse, loss and theft. This handout summarizes five basic information security practices that will help you take these precautions.

Best Practice #1: Stay abreast of your security responsibilities.
   a) Meet with your supervisor to review your responsibilities for information security and to identify the laws, policies, standards and practices that are relevant to your work at ECU.
   b) Consult the appropriate ECU compliance offices as needed on the proper handling of regulated data (e.g., FERPA, HIPAA, and PCI).
   c) Work with your supervisor to identify opportunities to develop the knowledge and skills you need to carry out your information security and compliance responsibilities.

Best Practice #2: Report security issues promptly.
   a) When you encounter a security issue or concern, promptly report it through the appropriate reporting channels.
   b) If you are unsure if an issue should be reported or to whom it should be reported, ask your supervisor for guidance. For additional assistance contact the IT Help Desk at 328-9866.

Best Practice #3: Use mobile devices thoughtfully and securely.
   a) Do NOT store sensitive information on your smartphone or other mobile device without prior approval. Check with your supervisor on the approved uses of mobile devices for your work.
   b) If you store sensitive information on a mobile device, you must ensure the information is encrypted, password protected and transmitted only over secure networks.
   c) Immediately report a lost or stolen device to your supervisor and the IT Help Desk at 328-9866.

Best Practice #4: Remove all ECU data from your devices before disposal or trade in.
   a) Always assume that your devices contain sensitive information. It is almost a certainty that your devices contain information about you or your work that should not be shared with others.
   b) Before you sell, give away or dispose of electronic devices or media, contact the IT Help Desk at 328-9866 for current guidance on data sanitization and device disposal.

Best Practice #5: Use different passwords for ECU and personal accounts, and don’t share them.
   a) Use passwords for your ECU accounts that are different from those for your personal accounts.
   b) Select passphrases (longer passwords, built from word phrases) that are easier to remember, and just as secure as shorter, complex passwords.
   c) Do not share your password with others, even as a favor to a coworker.

Information Security.
It’s not about technology.
It’s about people.

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