Shared responsibility. Throughout the University of Maine System, we handle a great deal of information that requires protection. Students and others entrust the University with their information and it is our commitment to them that we protect that information against unauthorized access, use, discloser, and distribution.

What type of information needs protection? Compliant Data, which includes personally identifiable information and confidential research information, requires protection under law. Such information includes financial records, bank account numbers, health records, driver’s license numbers, student educational records, and any information which could permit a person to attempt to harm or assume the identity of an individual. Exposure of such information can lead to identity theft and financial loss to those that are affected.

Breach Examples. In addition to hacking, breaches can occur from stolen laptops/thumb drives and mishandled paper documents.

- In June of 2014 an unencrypted laptop containing 20,000 former and current students and faculty members’ was stolen (NOT at the University of Maine System). The information contained on the laptops included names, birth dates and Social Security numbers of individuals.

- In June of 2014 a thumb drive containing 33,702 patient records was stolen from a medical facility. An employee placed the thumb drive in their desk, where the drive was stolen.

What can you do?

1. **Report problems.** If you come across misplaced electronic devices or paper documents containing Compliant Data, take action. Don’t share the data, power down the device if applicable and secure it to protect it from further loss. Report it to your supervisor to involve campus security and campus IT so they can report it to the Office of Information Security.

2. **Don’t be fooled by criminal social engineers.** A criminal social engineer is an attacker that attempts to gain access to protected information by tricking or misleading people. Attackers use social engineering techniques to “con” you into revealing information or letting them into facilities they don’t belong.

3. **Protect your own information.** Beware of criminal social engineers. Phishing email impersonate the sender of an email and direct you to a seemingly legitimate site that may steal your information. Likewise, caller ID can be masked to appear as it is coming from someone else. Keep home computer systems up-to-date with antivirus software. Use strong passwords - at least eight characters with upper and lower case letters augmented with numbers and special characters.