



UNIVERSITY OF
SOUTHERN MAINE

Checklist for Safeguarding Information

Departments throughout USM are responsible for collecting, storing and distributing voluminous amounts of information. Some of the information is federally legislated as private and must be protected in accordance with laws such as Gramm-Leach-Bliley (GLB) for personal financial information, and Family Education Rights and Privacy Act (FERPA) for student records. Other information should be safeguarded because it is considered private or confidential by the commonly understood definition of the words.

The following is a checklist that may be helpful to all University employees who have access to confidential/private information that should be safeguarded.

Information Communicated Orally

Make it a practice not to discuss confidential information outside of the workplace or with anyone who does not have a specific need to know it.

Be aware of the potential of others to overhear communications about sensitive information in offices, on the telephones, and in public places like hallways, restrooms, elevators and restaurants.

Information Stored on Paper

Documents that include confidential information need to be secured during printing, transmission, storage and disposal. Examples include but are not limited to: social security numbers, student education records, loan or financial aid data, scholarship information, medical information, tax information and credit card numbers.

Do not leave paper documents containing sensitive information unattended; protect them from the view of passers-by or office visitors.

When offices are closed store paper documents containing sensitive information in locked files and/or locked work areas.

Keys to locked files should not be left in unlocked desk drawers or other areas accessible to unauthorized personnel.

Credit card slips should not be sent through the regular intercampus mail service.

Paper checks, sent through intercampus mail, should be placed in sealed envelope

Shred confidential paper documents that are no longer needed, and secure such documents until such shredding occurs. Confetti shredders are recommended. If Facilities Management is needed to provide shredding services, ensure that clearly defined security measures are adhered to.

Documents containing confidential information should be retrieved immediately from copy machines, faxes and printers.

When faxing sensitive information double check the recipients fax number before hitting “start”. Do not send a fax to an office that is not open for business.

Include only necessary sensitive information on all outgoing correspondence.

Voice Mail / Phone/Cellular Device Cautions

Limit the use of student social security numbers in e-mail messages. Never put the number in the subject line of the e-mail.

When inviting callers to leave messages on voice mail, limit the requested account information to a full name and last four digits of a student account number.

If it is necessary to take credit card information over the phone in a public area, use caution in verifying the numbers back to the caller.

Be aware that information stored on laptops, cell phones and other mobile devices is susceptible to equipment failure, damage, or theft. Information transmitted via wireless connections is not always secure.

Protect and secure mobile devices from theft at all times.

Outside Vendors

If you deal with vendors or other outside parties who handle USM information that must be safeguarded, be sure that the necessary clauses pertinent to safeguarding responsibilities (available from the USM GLB Coordinator) are included in USM’s contracts with them.

Disposing of Computer Equipment

Make sure that computer hard drives declared as surplus or going out of service are sanitized to ensure that all data is removed and not recoverable. Deleting files, moving files to “trash” and emptying the “trash” file is insufficient because files can still be recovered. Call Property Management at 780-5245 with questions regarding properly discarding computer equipment.

Information Stored Electronically

Use a strong password and keep it a secret.

Do not let another person use your user account.

Use network drives for sensitive or important files.

Lock your computer when away from your desk during the day.

Shutdown your computer when you leave for the day.

Use encryption for viewing and exchanging sensitive data.

Do not install unapproved software.

Think before opening email attachments.

Schedule an antivirus scan of your computer.

Be careful using Internet Explorer.

10 Steps to Data and Network Security, a document written by the Division of Information and Technology staff, contains detailed information regarding information stored electronically. It can be found at <http://www.usm.maine.edu/doi/10SecuritySteps.html>

Where to Go for Help and Additional Information

Questions about safeguarding financial information can be directed to Cindy Quinn, GLB Coordinator, at 780-4888.

If you have questions about safeguarding the privacy of student records contact Steve Rand, Registrar, at 780-5107.

Call the Division of Information and Technology HelpDesk at 780-4029 with questions regarding the safeguarding of electronic information.