

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security

I. General

Information Security is the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional; although Information Security often involves electronic data, hard copy (written or printed) and verbally transmitted information require appropriate safeguards.

This APL covers general information regarding security practices and responsibilities, as well as guidelines for identifying and reporting breaches in security, unauthorized acquisition and disclosure of personal information and identity theft.

A separate APL exists for strong passwords.

RESPONSIBILITIES

Information Security is the responsibility of each individual in the UMS community. Each individual needs to understand and protect Covered Data, and must promptly report any suspected incidents. Supervisors and Department Heads are responsible for ensuring all employees they supervise, who are responsible for or come in contact with Covered Data, are aware of this APL and for complying with all procedures for protecting University collected and preserved data. All employees who use a personal or portable device for University work need to understand the security risks with their usage (see Appendix A for checklist).

Campus and System Information Technology departments and the Controller's Office will assist departments in identifying risks and provide information for educating personnel on issues of Information Security.

GUIDELINES

Covered Data

Covered data is information which requires special protection because the misuse could harm members of the UMS community or compromise the mission of the System and/or any one of the Universities. Covered data includes personally-identifiable information, confidential research information, and information that requires protection under law or agreement such as FERPA (the Family Educational Rights and Privacy Act), GLBA (the Gramm-Leach Bliley Act), HIPAA (the Health Insurance Portability and Accountability Act), FTC "Red Flag Rule", and by the PCI (Payment Card Industry) data security standards. Examples of Covered Data include: financial records, health records, student educational records, and any information which could permit a person to attempt to harm or assume the identity of an individual.

The Maine Data Act

The Notice of Risk to Personal Data Act (the Act) (10 M.R.S.A. § 1346 et.seq.) creates a duty to investigate breaches in the security of an individual's computerized data and an obligation to notify such individual of the breach in specified situations.

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security

A breach is defined as an unauthorized acquisition of data “that compromises [its] security, confidentiality or integrity,” or an authorized acquisition which is then used for an unauthorized disclosure of such Personal Information.

For the purposes of the Act, the data protected is referred to as “Personal Information” stored in a University storage system. That is: An individual’s first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- A. Social security number;
- B. Driver’s license number or state identification card number;
- C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;
- D. Account passwords or personal identification numbers or other access codes; or
- E. Any of the data elements contained in paragraphs A to D when not in connection with the individual’s first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Personal Information does not include “publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.”

Someone “unauthorized” is a person who “does not have authority or permission to access the information... and/or obtains access by fraud, misrepresentation or similar deceptive practices.”

If the University becomes aware of a breach, it must “conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information has been or will be misused.”

If, after the investigation, it is determined that a covered breach has occurred, notice must be given to the person(s) affected. It must contain the date of the breach; the information believed to have been accessed, a summary of the University’s response to the breach and a person they can contact for additional information. The notice must be given as “expediently” as possible and “without unreasonable delay,” consistent with the needs of law enforcement and the need to restore the reasonable integrity, security and confidentiality of the data in the system.

Notification is required when personal information was or is reasonably believed to have been acquired by an unauthorized person...and there is likelihood that it will be misused.

Notice must be in writing (presumably given by U.S. Mail) to the person’s known address unless the cost would exceed \$5,000 or notification has to be given to more than 1,000 people. In these events or if there is no mailing address available “substitute notice” can be given by both e-mail and also placed conspicuously on the University’s website. If substitute notice is given, the statewide media must also be notified.

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security

If a single breach involves notification of more than 1,000 people, notice must also be given “without unreasonable delay” to consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach.

A report must be sent to the State of Maine Attorney General.

Basic Risks and Safeguards

General

- Cross shred spent confidential paper documents.
- Lock desks, file cabinets and office doors containing confidential data when unattended.
- Protect paper documents containing covered data from casual view.
- Store critical paper documents in a fireproof vault.
- If vendors will handle UMS data refer to [APL VII-A Purchasing Procedures](#).
- Restrict data available to vendors and employees to that data necessary to perform their function.
- If in doubt as to whether information is considered covered data, contact the department responsible for that information or University Counsel.

Conversations

- Be aware of who may overhear your conversation.
- Do not discuss covered data with anyone who does not have a need to know.

FAX

- Make arrangements to immediately retrieve or secure sensitive documents that are printed on copy machines, fax machines and printers.
- Make every effort to ensure that a fax reaches only its intended recipient.

Staff Management

- Regularly remind staff and students of the importance of information security.
- During orientation, supervisors will train new employees in:
 - The importance of the confidentiality of covered data.
 - The proper use of IDs and passwords.
 - How to dispose of documents that contain covered data and controls and procedures to prevent employees from providing covered data to an unauthorized individual, including “pretext calling”.
 - How to recognize “red flag” warnings of actual or potential identity theft.

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security

Email and FTP

- Encrypt any email containing covered data. Check with your local IT/computer services department for guidance on how to encrypt email.
- Either do not send or take great care when sending anything by e-mail that you would not want disclosed to someone else. E-mail may be miss-addressed; recipients of your e-mail may forward data or store it on an unsecure machine.

Data Storage and Disposal

- Backup media will be stored in a secure location that will account for protection of covered data.
- When disposing of media (disk drives, removable media or solid state drives) which may contain covered data, simply deleting files is inadequate. Destroy or overwrite the media with software which overwrites previously stored data three times with a predetermined pattern of meaningless information effectively rendering the data unrecoverable. If a disk drive doesn't function, the disks will need to be removed and physically destroyed.

Desktops & other Hardware

- Orient computer screens away from the view of others.
- Set screen savers with password protection to activate after 10 minutes of inactivity.
- Physically secure all data storage devices against theft - especially laptops and removable media.
- Completely shut down the desktop computer at the end of the workday unless you have your supervisor's approval for remote access.
- Limit who can remotely access a computer.
- Maintain the operating system with the latest patches, spy ware and anti-virus tools.
- Do not download and install unknown programs. Downloads may install spy ware which allows others to access a data without your knowledge and to log keystrokes.
- Do not open unexpected e-mail attachments.
- Do not download documents from unknown parties.
- Avoid storing covered data on a device with a web server. Consider whether or not your website should be password protected.
- Contact your Desktop Support Technician or UMS-ITS with any question about security.

Passwords

- Secure your passwords – if you must write them down, lock them up or keep them on you.
- Follow the standards in the [Strong Passwords APL VI-D](#) .

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security

Other Resources & Tools

System and Campus IT departments can direct employees to a number of resources and tools that are available. Awareness videos/presentations and checklists are available online. Computer tools are available that scan PC hard disks for SSN and credit card numbers, encrypt hard disks, or wipe computer data from a computer so it cannot be recovered.

II. Security Incident Response

Loss of covered or other confidential data has serious consequences to the University as well as a possible widespread impact on others. An immediate and thorough response to an Information Security incident including analysis and reporting is required by legislation – including, but not limited to, the Health Insurance Portability and Accountability Act, the Gramm-Leach Bliley Act and the Maine Data Act.

Initial Notification

Known or suspected loss of covered or other confidential data must be reported promptly. An event such as the loss of a portable computer or device which may contain protected data, suspected intrusions, or other suspicious activities needs to be reported promptly.

If a non-IT (paper based) compromise of information is suspected, incidents need to be reported to the department head and up through the chain of command, including the System Director of Finance and Controller, so that an appropriate and timely investigation and reporting of information to Legal and External Affairs can be made. Campus or System IT does not need to be involved in non-IT (paper-based) compromises, but should be notified immediately if there is any suspicion that electronic systems are involved.

For any suspected compromise of information that is stored or transmitted on an electronic system or device, report the breach to the Campus Chief Information Officer (CIO) or IT Director, who will coordinate a response. Campus IT will contact UMS/ITS when the incident involves UMS/ITS managed systems. Likewise, System office employees, who suspect a compromise of information, must notify the UMS-ITS director /associate director. If that director is not available the UMS CIO is to be contacted. If the CIO is not available, the employee shall continue to try to locate a responsible individual by calling the campus Help Desk, the UMS-ITS Help Desk or the UMS Network Operations Center. The UMS CIO or the appropriate UMS/ITS director or associate director will ensure a response is coordinated.

The Campus CIO and/or the UMS CIO will notify the System Director of Finance and Controller regarding any compromise of financially related information or any information that may involve or increase the risk of identity theft.

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security

Initial Notification Message – Content:

1. Brief description of the incident including a description of any information believed to have been accessed.
2. Date and time of the incident or of the discovery/report of the incident.
3. Campus.
4. Name of person making this notification.
5. Email, phone, cell phone or other contact information for a person familiar with the incident who is available to provide more information.

Initial Analysis of the Incident

The IT Director determines if an incident has actually occurred. An incident most likely would involve:

- Any computer fraud.
- A compromise which may have resulted in the leakage of personal information (data theft).
- A successful denial of service attack.
- A natural disaster which compromises access to the information systems.
- An adverse event that threatens the confidentiality, integrity or availability of University information assets, information systems, or the networks that deliver the information.
- Damage to data or unauthorized data modification.
- Unauthorized access to a system of unknown origin.
- Unusual, unexplainable system behavior.

Events which in themselves are not an incident:

- Port scans.
- Equipment failure or software failure.
- Routine detection and remediation of a virus or mal-ware.

Response to Incident

After determining that an incident has occurred, the IT director will form and direct a Computer Incident Response Team (CIRT). The IT Director will immediately notify the UMS CIO, the UMS Network Operations Center, External Affairs, University Counsel, and the Director of Finance and Controller and will keep these individuals apprised of the status of the incident.

The CIRT will take the following actions as appropriate to investigate the incident, contain the compromise, and make proper notifications.

- Follow the provisions of the Maine Data Act as enumerated above.
- Determine how the incident occurred.

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security

- Conduct interviews.
- Preserve evidence.
- Protect or copy any logs which may relate to the incident.
- Maintain a response log including date, time, action taken and individuals contacted.
- Step back and analyze the scope (i.e. is more involved than initially suspected?).
- Seize, segregate and preserve hardware for possible forensic analysis.
- Disable the compromised hardware or software.
- Take steps to prevent proliferation of the incident.
- Contain the incident; reduce the incident impact with a plan to restore functionality.

Notify any known individuals who may be harmed by this incident.

- Notify the help desks to consider and report related events to avoid duplicate effort.
- Notify campus police and law enforcement if appropriate.
- Notify and coordinate with hardware or software vendors.
- Coordinate regulatory reporting and notice to other members of the University community.

After resolution, prepare a report of the incident including cause, action taken, cost to the organization, resources needed to fully recover, recommendations to improve security and prevent similar incidents and recommendations for future incident response. Issue a copy to all individuals who were initially notified.

APPROVED:

Vice Chancellor for Finance and Administration

Note: Official copy on file in the Office of Finance and Administration at the University of Maine System

Related Documents:

[APL VI-D Strong Passwords](#)

[APL VII-A.2 Purchasing Procedures](#)

Maine Revised Statute Title 10, Chapter 210-B: Notice of Risk to Personal Data

<http://www.mainelegislature.org/legis/statutes/10/title10ch210-Bsec0.html>

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security

APPENDIX A

Checklist for the Protection of Covered Data When Using Portable University-Owned and All Non-University Devices

Employees who telecommute will complete this checklist as part of their telecommuting agreement. Supervisors will ensure that any employee who is issued a University portable device also completes this checklist. Based on the employee’s contact with covered data, a supervisor may require this checklist be completed by an employee who works at home or uses a personal device for University work.

Covered data is information which requires special protection because the misuse could harm members of the University community or compromise the mission of the University of Maine System and/or any one of the Universities. Covered data includes personally-identifiable information, confidential research information, and information that requires protection under law or agreement such as FERPA (the Family Educational Rights and Privacy Act), GLBA (the Gramm-Leach Bliley Act), HIPAA (the Health Insurance Portability and Accountability Act), and by the PCI (Payment Card Industry) standards. Examples of covered data include: financial records, health records, student educational records, and any information which could permit a person to attempt to harm or assume the identity of an individual such as an individual's name in combination with a Social Security, credit card or bank account number.

Complete the entire checklist that follows. For each “YES”, provide a response to the appropriate measures. If you have arranged an exception or alternate to any measure with IT/computer services, annotate the measure with an asterisk (*) and note the alternate measure at the bottom.

1. University Laptop

YES NO I use a University laptop.

↳ If YES (check one of the following):

- I store Covered Data, access Covered Data with software other than MaineStreet, or send/receive Covered Data via email; and I have worked with my IT/ computer services department to have an area of the laptop’s hard drive encrypted for storage of Covered-Data.
- I will not store Covered Data, access Covered Data with software other than MaineStreet, or send/receive Covered Data via email.

2. Personally-Owned Computer

YES NO I use a personally-owned computer for work at home or to telecommute, even if only for University email.

↳ If YES (check as applicable):

- I agree that Covered Data may never be stored on my personally-owned computer.
- I agree that I will install virus protection on the computer which I use to access University systems. One copy of virus protection will be provided by the University.
- I agree that, in the case of a suspected breach, I may be required to provide access to my personally-owned computer to UMS staff.

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security

- I access MaineStreet Covered Data from my personally-owned computer or device for more than my own personal information and I agree not to download and save Covered Data from MaineStreet to my personally-owned computer or device.
- I use remote access services (such as Remote Desktop Protocol or VPN) to connect to an office computer and I agree to not transfer files with Covered Data to my personally-owned computer.
- I send/receive Covered Data via email, and I will use secure (https) webmail that will not cache or save email/files. I will work with my IT/computer services department if I need help with using appropriate email.
- I agree to not open Covered Data email attachments on my personally-owned computer because doing so would automatically copy the attachment to my computer's drive.

3. Portable Handheld Devices such as Smart Phones

YES NO I use a University provided or personally-owned handheld device to access University email or connect to University data.

↳ If YES (check as applicable):

- I access Covered Data, or send/receive Covered Data via email from my handheld device and have completed all of the following measures.
 - I have worked with my IT/ computer services department to ensure encryption is available and turned on for the device.
 - I have enabled the requirement to use a password to access email.
 - I agree that in the case of a suspected breach, I may be required to provide access to my personally-owned device to UMS staff.
- I will not access Covered Data, or send/receive Covered Data via email from my handheld device.

4. USB drives or other portable storage

YES NO I use a USB drive (e.g., pen drive, memory stick, etc.).

↳ If YES (check one of the following):

- I move or store Covered Data with a USB drive; and I have worked with my IT/ computer services department to encrypt the Covered Data storage area.
- I will not move or store Covered Data with a USB drive.

5. Home Wireless

YES NO I have a wireless network at home even if the computer I use is hardwired and I might access Covered Data.

↳ If YES (check one of the following):

- I have secured my wireless access point to prevent a wireless intrusion to my network which would allow an intrusion into a wireless or wired computer.
- I will turn off wireless access while I work at home.

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security

6. Other Situations and Alternate Measures or Exceptions.

YES NO I access, store or transmit Covered Data in a manner that isn't listed here and I have worked with my supervisor and IT /computer services department to implement the following measures:

YES NO I am implementing the following alternate measures or exceptions to the requirements above with my supervisor's and the IT / computer services department approval:

7. Required Conditions

I agree that if any conditions change regarding access or storage of Covered Data, to include receiving an email with Covered Data, I will notify my supervisor and work with my IT /computer services department to ensure proper actions are taken to secure the data and employ the appropriate protections.

I agree that if any Covered Data is accessed or stored on a University or personally-owned device to include receiving email with Covered Data, without the proper measures taken, I will treat this as an urgent security incident. I will notify my supervisor and work with my IT /computer services department to ensure prompt proper actions are taken to secure the data and employ the appropriate protections. I understand that swift actions are needed to prevent unauthorized access to Covered Data.

Employee's Signature: _____ Date: _____

Supervisor's Signature: _____ Date: _____