University of Maine System

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Employee Protection of Data

PURPOSE AND SCOPE

All individuals working on behalf of the University have a responsibility for protecting University data and data that is entrusted to the University. The Board of Trustees Information Security Policy specifies that this requirement applies to all UMS faculty, staff, employees, contractors, consultants, business partners or anyone who accesses or possesses such data. This APL focuses on appropriate precautions that faculty, staff and student workers are expected to take commensurate with the sensitivity, volume, and value of the data they handle. The overarching goal of protecting data is to reduce the risk associated with unauthorized access, loss or theft of data whether the data is in paper or electronic form. Included in protection is awareness of what data is under an individual's control so that appropriate actions can be taken if data is lost.

DEFINITIONS

Compliant Data – Information which has specified requirements for the control of confidentiality, integrity, or availability of the data due to statute or contract or other law or agreement. Compliant 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. Compliant data includes, but is not limited to, personally-identifiable information, confidential research information, and information that requires protection under law or agreement. (e.g., Maine Data Act, FERPA, GLBA, HIPAA, FTC "Red Flag Rule", by the PCI data security standards, and data placed on legal hold in accordance with e-discovery). Examples of Compliant Data include: financial records, health records, student education records, and any information which could permit a person to attempt to harm or assume the identity of an individual.

In the previous Information Security APL VI-C, Compliant Data was labeled as Covered Data.

Business Sensitive Data – Information that is not the subject of statutory or contractual controls, but where the compromise of the confidentiality, integrity, or availability of the information would result in damage or loss to UMS.
Computing Device - A Computing device is specifically a single user machine such as a desktop computer, laptop computer, tablet, smart phone, or other mobile device that is used for University work, whether provided by the university or not.

Unauthorized Access - Viewing or possessing something without authorization. This may be deliberate or accidental. The access may be to a system, network or data. Any lost or stolen paper or device which contains compliant or business sensitive data should be assumed to have resulted in unauthorized access.

University Data - For the purposes of this APL, University data is information that is either wholly or partially owned by UMS, or that has been entrusted to UMS. The UMS Policies and Standards define this data as Compliant, Business Sensitive, or Unclassified.

RESPONSIBILITIES

Protection of University data is the responsibility of everyone who accesses, stores, transmits or processes such data. This section describes the responsibilities that pertain to individuals (e.g. faculty, staff, and student workers) as well as managers and supervisors, and supporting Information Technology offices.

Individuals

Each individual shall:

1. Understand the requirements for protecting University data and the risk associated with using devices to access, process or store information. A list of permitted and restricted systems for compliant data is located in APPENDIX C and a list of specific data elements is located in APPENDIX D.
2. Be accountable for the Compliant Data in his or her control or possession to include data on devices whether provided by the University or not.
3. Limit the amount of Compliant Data that is in his or her control or possession and handle only the amount of data which is necessary to complete the job.
4. Back-up University data stored on computing devices under the individual's control when the data is the original or master copy.
5. Promptly report any suspected incident including loss or theft of a device that may contain University data to Campus or System IT. Further response shall be in accordance with the Information Security Incident Response APL (APL VI-B).
6. Follow the checklist referenced in APPENDIX A when using non-University devices or networks. Create strong passwords, ensuring they contain at least one upper and one lowercase alphabetic character, one numeric or special character and have a length of at least eight characters.
7. Send business or compliant data to other departments or third parties only when the recipient is authorized to receive such data. Check with supervisor or manager if uncertain who is authorized.

Managers/Supervisors

Each Manager and Supervisor shall:

1. Ensure individuals receive security awareness training and are familiar with the requirements of this APL.
2. Require individuals to sign a confidentiality agreement if the individual has access to a significant amount of compliant or business sensitive data. A template is in APPENDIX B. This template may be administered electronically.
3. Evaluate the amount and sensitivity of data handled by each individual, authorize the minimum access required to perform assigned duties according to a "need to know" basis, and determine whether a separation of duties should be used to prevent negligent or deliberate misuse of data.
4. Grant authorization to an individual to remove equipment from the University prior to that individual taking University-owned equipment off site. This authorization may be one time and need not be in writing.
5. Emphasize the need for individuals to protect Compliant or Business Sensitive Data when transporting it outside of UMS's physical boundaries. Ensure that individuals who telecommute or work at home understand and acknowledge that they will follow the actions contained in APPENDIX A.
6. Prohibit sharing of passwords and require individuals to report incidents where they were asked for their passwords from someone who is believed to be a University employee. Supervisors shall report such incidents to Campus IT or UMS ITS.
7. Ensure each individual is handling UMS records in accordance with the Records Retention APL.

8. Hold employees accountable for proper Information Security practices. Misuse of Compliant Data or Business Sensitive Data and breach of the Information Security Policy is subject to normal UMS disciplinary processes.

Campus and System Information Technology

IT offices shall:

1. Assist individuals with applying technology to reduce risk of unauthorized access and to protect electronic data on University-issued devices. Such protections include storage encryption, antivirus, and secure file removal utilities, and other actions as required by the Information Security Policy and Standards.
2. With cooperation from Information Owners, complete Risk Assessments on internal and external systems provided by the IT office to understand and relay the level of sensitive data that is permitted to be stored on such systems. Reference APPENDIX C.

GUIDELINES

Basic Risks and Safeguards

The UMS Information Policy and Standards identify a number of controls to be employed to safeguard data. The following are some basic practices.

1. Make a concerted effort to understand what Compliant Data is in your control and possession at all times.
2. Share Compliant Data only with those who have a need to know. This includes limiting voice discussions, orienting computer screens away from those not authorized and quickly retrieving documents that are printed on copy machines, fax machines and printers.
3. Either do not send or take great care when sending anything by email or fax that you would not want disclosed to someone else. Be careful to address email to authorized recipients and be aware that the email may land on an unsecured device.
4. Use extreme caution when handling certain types of Compliant Data as some data is highly targeted for theft and its loss could severely impact the University. Examples of such data are social security numbers, driver's license numbers, bank account numbers, and credit card numbers. This type of data must be encrypted when stored on a computing device, and only stored on such a device with department head approval.
5. Use cross-cut shredders to destroy compliant documents. For electronic documents, typical file deletion does not erase data from a computer hard drive. There are secure file deletion tools that overwrite disk space to render electronic files unreadable.
6. To prevent malware from being installed on a computer, do not download or install unknown programs, do not, open unexpected email attachments, and do not download documents or open attachments from unknown individuals.

Supplemental Instructions

For individuals who want guidance on how to implement or perform technical aspects of this APL, such guidance can be found at the Office of Information Security web site, www.infosecurity.maine.edu.

Prepare for the Worst - Loss or Theft of a Device

Whether a device is University owned or not, individuals need to take precautions if University data is on the device. Mobile devices are more likely to be lost or stolen than other equipment. Even though a device may be stolen for the equipment value, the data on the device will be considered compromised unless it is encrypted. Devices containing sensitive data should not be left unattended and where possible, should be physically locked or stored away. A user/owner may have to relinquish control and possession of a device in the event it is needed for evidence for legal actions.
Taking the following steps will reduce the risk associated with lost data.

1. Record what University data (especially Compliant Data) is stored on the device. This will provide a basis to report lost data, if needed, as well as help to reduce or eliminate unessential data. A backup of files provides a good record.
2. Configure the device appropriately for the type of data being stored or accessed. Any or all of the following configurations may be required:
   i) Password protect the device using a strong password.
   ii) Enable system locks on devices so that the device will lock after a set time. This is usually 5-30 minutes depending on the device type, location of use and type of data accessed or stored.
   iii) Configure the web browser so that passwords associated with email or other programs are not saved.
   iv) Configure the device so that Compliant Data is not downloaded unbeknownst to the user/owner. For example, know when email is cached/stored on the device and if appropriate, avoid caching. On unencrypted laptops and personally owned computers, use browser-based email.
   v) Encrypt the device.
3. For retrieval purposes, document the device's serial number for personally owned devices.
4. Ensure data files that contain the original or master copies are backed-up.

APPROVED

Official signature on file in the Finance Office
of the University of Maine System

Vice Chancellor of Finance and Administration

APPENDIX A: Protection of Compliant Data when using non-University Devices or Networks

Employees who work at home or at non-University locations and employees who use non-University devices will follow the measures below. Employees who telecommute will also follow these measures as part of their telecommuting agreement.

Compliant data includes personally identifiable information, confidential research information, and information that requires protection under law or agreement. Examples of compliant 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.

1. University-owned Device

An employee who stores, accesses, or emails Compliant Data, other than limited student data as it pertains to particular course (such as faculty records of student activity in a course) will work with Campus IT to ensure the necessary precautions are taken and have encryption enabled on the device. Accessing Compliant Data through MaineStreet does not require working with Campus IT.

2. Non-University-owned Devices

An employee who uses a non-University owned device for work, even if only for University email, agrees to:

- Never store Compliant Data other than student course information on a non-University-owned device. For example faculty may store student data to include class lists and information about current students.
- University data, including email attachments, should never be stored, downloaded or cached on public computers such as those in public libraries or computer cafes.
- Install virus protection software on a computer which is used to access University systems and will manage the system in such a way that the system is monitored and virus signatures are kept current.
- Have disabled web browser's option to store passwords to University systems.
- In the case of a suspected breach, report it to campus IT and, if required, provide access to his or her personally-owned device to UMS staff.

3. Portable Storage Devices

An employee who uses a portable storage device (e.g., portable HDD, memory stick, thumb drive, etc.) agrees that if he or she moves or stores Compliant Data, other than student course information, with a portable storage device, the employee will work with Campus IT to encrypt the Compliant Data storage area and securely erase the device or files when finished using the device for Compliant Data storage.

4. Non-University Network

An employee who has a wireless network at home and might access Compliant Data must secure the wireless network with encryption even if the computer being used is hardwired. An employee who uses non-University networks to access Compliant or Business Sensitive data, will use be sure the connection is secure (for example through https).

APPENDIX B: Confidentiality Agreement Template

UNIVERSITY OF MAINE SYSTEM
EMPLOYEE CONFIDENTIALITY AGREEMENT

As an employee of University of_________________________________, I may be provided with access to Compliant or Business Sensitive Data. Such data, including personal or private information concerning faculty, staff, students, or others associated with the University will be referred to herein as “confidential” information.

I will use my access to confidential information for the sole purpose of conducting permitted University business and understand that the use of confidential information for personal or other unauthorized purposes is prohibited. As an employee of the University of Maine System, I am entrusted to protect sensitive information, whether or not it is labeled or identified as such and agree to abide by the following requirements:

a. I will NOT access or attempt to access information that I am not authorized to access;

b. I will NOT make unauthorized use of, or seek personal benefit from, any confidential information to which I have access;

c. I will NOT disclose or provide access to confidential information to any person who is unauthorized to view such information.

I understand that my access to confidential information is often facilitated by electronic information systems. I will not give unauthorized access to such systems and I will keep all related passwords secure. If any circumstance requires me to share a password, I will immediately reset it once the situation is resolved. Likewise, if a University employee shares a password with me for emergency purposes, I will advise the employee to immediately reset the password once the situation is resolved.

I will process and store confidential information in a secure way. When no longer needed, papers containing confidential information will be shredded and electronic files that contain confidential information will be securely deleted in accordance with records retention policy.

I understand that this statement and additional guidance relating to securing information can be found within the University of Maine System Information Security Policy and Security Standards and Administrative Practice Letter (APL VI-C [this APL]. I also understand that student education records are specifically protected under the Family Educational Rights and Privacy Act (FERPA), and I will seek guidance from the Registrar’s Office if I am unsure about appropriate disclosure of such information. I further understand that certain departments or units within the University perform health care or health plan functions and are bound by privacy and security related policies and procedures created under the Health Insurance Portability and Accountability Act (HIPAA).

By signing and dating this agreement, I understand the permissions and authorizations I have been given to confidential information, agree to these terms, and acknowledge that failure to do so may result in disciplinary action. I also understand that this agreement remains in effect continuously for the duration of my employment by the University of Maine System.

Employee Signature ____ Date: __________________________
Printed Employee Name: ____ Employee ID: ____________________
Employee Title: ____
Department: ____

APPENDIX C: Permitted and Restricted Systems for Compliant Data

Table 1: Internally Hosted Services

DATA TYPE	MaineStreet	ImageNow	Data Warehouse	Advance	Blackboard	Local Email	Local Servers
Student Educational Records (FERPA)	✓	✓	✓	✓	✓	✓	✓
Protected Health Information (HIPAA)	✓	✓	✖	✖	✖	✖	⚠[1]
Banking Information to include student financials (GLBA)	✓	✓	✓	✖	✖	✖	✓
Payment Card Information (PCI)	✖	✖	✖	✖	✖	✖	⚠[2]
Export Control Research (ITAR, EAR)	✖	✖	✖	✖	✖	✖	⚠[3]
Social Security Numbers and Driver's License/ State ID Numbers (Maine Data Act)	✓	✓	✖	✖	✖	✖	⚠[1]

✓Permitted ⚠Not Permitted without Exception or Specific Approval ✖Not Permitted

Notes:
1. Only on approved servers. Check with the server administrator or Campus IT.
2. Only on approved servers or computers placed on the PCI network in accordance with PCI DSS.
3. Only on approved research systems meeting ITAR and EAR requirements.

Table 2: Externally Hosted Services

DATA TYPE	UMS Gmail and Calendar	UMS Google Apps (Google Drive)	Additional Google Services (Blogger, Picasa, YouTube, etc.)	Other Cloud Services
Student Educational Records (FERPA)	✓	✓	✗	⚠[4]
Protected Health Information (HIPAA)	✗	✗	✗	⚠[4]
Banking Information to include student financials (GLBA)	✗	✗	✗	⚠[4]
Payment Card Information (PCI)	✗	✗	✗	⚠[4]
Export Control Research (ITAR, EAR)	✗	✗	✗	⚠[4]
Social Security Numbers and Driver's License/ State ID Numbers (Maine Data Act)	✗	✗	✗	⚠[4]

✓Permitted ⚠Not Permitted without Exception or Specific Approval ✗Not Permitted

Notes:

4. Only on systems approved by the UMS CIO for storage of this particular type of data. A list of approved cloud services will be published on-line.

Table 3: End-user Computing Devices

DATA TYPE	UMS Devices	Encrypted UMS Devices	Non – UMS Devices (e.g. phones/tablet)	Removable Media
Student Educational Records (FERPA)	✓	✓	✓	✓
Protected Health Information (HIPAA)	✖	⚠[5]	✖	⚠[6]
Banking Information to include student financials (GLBA)	✖	⚠[5]	✖	⚠[6]
Payment Card Information (PCI)	⚠[2]	⚠[2]	✖	✖
Export Control Research (ITAR, EAR)	✖	⚠[5]	✖	✖
Social Security Numbers and Driver's License/ State ID Numbers (Maine Data Act)	✖	⚠[5]	✖	⚠[6]

✓Permitted ⚠Not Permitted without Exception or Specific Approval ✖Not Permitted

Notes:
2. Only on approved servers or computers placed on the PCI network in accordance with PCI DSS.
5. Only when approved by Department Head.
6. Only when encrypted and approved by Department Head.

APPENDIX D: Protection of Common Data Elements.

University data is often characterized by category or use of the data and then classified in accordance with the legal or contractual controls placed on it. However, data elements within each category often warrant different levels of protection. While some data elements offer little risk and require no special protection, inappropriate handling of other data elements might result in criminal or civil penalties, identity theft, and/or personal or organizational loss.

This table identifies some common data elements by category, the associated classification, and the degree of protection that each requires. The protection factor is based on the threats to that type of data together (e.g. identity or credit threat targets) with the impact if lost (to the University or to affected individuals). When using this table consider:

1. Not all data elements are listed. Absence of a data element does not mean that it requires no protection.
2. Quantity/amount of data must be considered. One thousand records of one data element may have more value together than one record of an element with a seemingly higher protection factor.
3. Combination of data elements can increase the value. For example FERPA identifies Personally Identifiable Information (PII) as information that can identify a person even though the name may not be given.

Use the following protections when storing, processing or transmitting data for each protection factor:

Critical - Use extreme caution as this information is highly targeted for theft and loss of this data could severely impact the University. Must be encrypted when stored on a computing device, and only stored on such a device with department head approval.
High - Use caution as this information is targeted for theft. Limit use and protect according to quantity and value.
Medium - This data has some value, especially in quantity. Limit storage on computing devices
Low - There is a low threat to this data which has little value. Releasable through official channels only.

Personnel Information Elements (HR)	Information Classification	Protection Factor
Social Security Number Driver’s License number State Identification Number	Compliant - Maine Data Act (when combined with a name or other uniquely identifiable personal information).	Critical
Genetic Information	Compliant – Genetic Information Nondiscrimination Act (GINA). Information must be safeguarded as health information in accordance with HIPAA	Critical
Disability Status Military Disability Status Ethnicity/Race Gender Status	Compliant	High
Name Date of Birth	Business Sensitive	High
Employee Identification Number (EMPLID)	Business Sensitive - An EMPLID is not considered Compliant Data, and is not afforded special protection and confidentiality.	Medium

	EMPLIDs uniquely identify staff and faculty members without using Compliant Data such as SSNs. Routine shared use of EMPLIDs is sometimes necessary for University functions. Share EMPLIDs only with those who have a reason to use it. Combinations of information increase the value of data. EMPLIDs when used in combination with name or DOB increase the security risk.	
Home Address Home Phone Number	Unclassified - Not protected by any legal or contractual controls and is provided only to those with a "need to know" or public only through official channels.	Medium
Work Address Work Phone Number Business Email Address	Unclassified - Not protected by any legal or contractual controls and is public information.	Low
Payroll Information Elements	**Information Classification**	**Protection Factor**
Social Security Number Bank Information (routing/Acct #)	Compliant - Maine Data Act & GLBA	Critical
Salaries	Not Protected - Not protected and is public only through official channels.	Low
Work Study Awards	Business Sensitive - Protect this information as is indicative of financial need. Some work study is non-need based and does not require protection.	Medium
Employee Verification (i.e., salaries)	Not Protected HR will only verify what the Bank or Third Party was told by employee	Low
Protected Health Information (PHI) Elements	**Information Classification**	**Protection Factor**
Past, present, or future physical or mental health or condition of an individual. Provision of health care to an individual Past, present, or future payment for the provision of health care to an individual.	Compliant - HIPAA - If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information. The HIPAA privacy rule lists 18 identifiers that are not to be used with a health record.	Critical
Identifiers - 18 specific identified by HIPAA	Compliant - HIPAA	High

Privacy Rule (includes such information as name, geographic information, dates, contact information, medical record and account numbers, biometric identifiers, photos, and other uniquely identifying number, characteristic or code)	Those working with protected health information need to be familiar with the identifiers as listed by the HIPAA Privacy Rule and protect them accordingly. These identifiers by themselves may not be compliant data, but when associated in any way with the Personal Health Information elements listed above are compliant under HIPAA.	
Student Data Elements (Registrars)	**Information Classification**	**Protection Factor**
Social Security Number (including historical student ID number when it was SSN) Driver's License Number State Identification Number	Compliant - Maine Data Act & FERPA (When combined with a name or other uniquely identifiable personal information).	Critical
The following elements are considered Directory information: Name Address Phone Number Date of Birth Class Level Dates of Attendance Degree Awarded Status Enrollment Status (full or part-time) Honors and Awards Program of Study Most recent previous educational institution attended Participation in sports and activities Appropriate personal athletic statistical data	Compliant or Unclassified - FERPA - This is not protected and can be openly shared UNLESS ASKED BY THE STUDENT TO BE SUPPRESSED. Therefore, prior to any disclosure, one must check each student's FERPA election to determine whether the student data may be disclosed.	Medium
Academic Standing (i.e., probation, suspension, etc.) Class Schedule Degree Audit (including courses remaining to complete a degree) GPA Grades Transcript Email Address	Compliant – FERPA Note: Students' entire educational record is considered protected information under FERPA. For example, a class schedule includes information about any student taking a course.	Medium
Student Identification Number (EMPLID)	Compliant - FERPA - Unlike a staff and faculty member EMPLID, a student ID number is Compliant Data and requires protection	Medium

	under FERPA. When a student worker's EMPLID is used for employment, this EMPLID remains protected by FERPA. - This ID number is not a personal identification number under the Maine Data Act and is not protected by that law.	
Information on former students - Student records not to include SSN or Driver's License/State Identification Number	Compliant – FERPA - Educational Records collected when an individual was a student is protected in accordance with FERPA, for the life of the record. Compliant FERPA or Unclassified - Information that was collected as directory information when an individual was a student is not protected unless asked by the student for it to be suppressed, while the individual was a student. Not classified by FERPA - Information about a former student (i.e. alumni information) collected *after* the student graduated is not considered an educational record.	Medium

Donor Information Elements	**Information Classification**	**Protection Factor**
Social Security Number Bank Account Number	Compliant - Maine Data Act & GLBA	Critical
Financial Account Information	Compliant - GLBA or PCI - Not to be stored without specific permission. Credit Card transactions must be in accordance with the Credit/Debit Card Standards APL	Critical
Name Giving History (Amount/what donated)	Business Sensitive - When associated with donation(s)	High
Address Telephone/Fax Numbers Email Employment Information Family Information	Business Sensitive	Medium

Interests, Affiliations or Sports		
Other donor info (e.g. Age, Sex, Degree Information)	Unclassified	Low
Payment Card Elements	**Information Classification**	**Protection Factor**
Credit/Debit Card Number (Primary Account Number - PAN) Cardholder Name Expiration Date Service Code	Compliant - PCI-DSS & Maine Data Act - See Credit/Debit Card Standards APL for storage requirements	Critical
Authentication data (CAV2/CVC2/CVV2/CID) Number PIN/PIN Block Full Magnetic Stripe Data	Compliant - PCI-DSS - Never to be stored. See Credit/Debit Card Standards APL.	Critical
Masked Credit/Debit Card Number (no more than first 6 and last 4 digits)	Unclassified - See Credit/Debit Card Standards APL	Low
Procurement Elements	**Information Classification**	**Protection Factor**
Pre-Award Contract Bids	Compliant	Critical
Awarded Contracts	Unclassified - FOAA - subject to public record requests.	Low
Purchasing Card (P-Card) Numbers	Compliant - P-Card protection requirements differ from payment cards accepted by a University merchant activity. However, all credit card numbers are high target theft items. - See Credit/Debit Card Standards APL	High
Information Security Elements (OIS & IT)	**Information Classification**	**Protection Factor**
Authentication Credentials (User Name and Password)	Compliant - Requires the same protection as the level of information that is protected by those credential	Critical

Access & Authorization Information Vulnerability Scanning Results Risk Assessment Results Intrusion Detection Alerts Security Architecture & Design Security Incident Response	Compliant or Business Sensitive - Requires the same protection as any information that could lead to unauthorized access at the level of information that is protected by a system	Critical or High

Other Data Types	**Information Classification**	**Protection Factor**
Export Control Research	Compliant - ITAR, EAR - Specific elements not listed. Refer to appropriate regulation.	Critical
Human Subject Research	Depends on Research- Common Rule (45 CFR 46, 102(d)) -Refer to Board of Trustees Policy Section 601	Depends on Research