I. General

II. Definitions

III. Identification and Assessment of Risks to Customer Information

IV. Information Security Plan Coordinators

V. Design and Implementation of Safeguards Program
   a. Employee Management and Training
   b. Administrative Safeguards
   c. Physical Security
   d. Information Systems
   e. Management of System Failures

VI. Selection of Appropriate Service Providers

VII. Continuing Evaluation and Adjustment

VIII. Campus Information Security Plans

Appendix A Checklist for Safeguarding Information
I. General

The University of Maine System is responsible for collecting, distributing and storing a large volume of information. Some of this information is legislated as private and must be protected in accordance with laws such as the Gramm-Leach Bliley Act (“GLBA”) for non-public personal financial information, the Family Educational Rights and Privacy Act (“FERPA”) for student educational records and state laws pertaining to personnel records and medical records. All information which is deemed confidential by such laws is considered Covered Data for the purposes of this APL. “Protected Health Information” under the Health Insurance Portability and Accountability Act will be maintained and used in accordance with University HIPAA Policies and is not subject to this APL.

This APL describes the University of Maine System’s Information Security Plan (the “Plan”) which sets forth safeguards to protect Covered Data. This APL applies to all Covered Data in the possession of, used or maintained by the University of Maine System and any of its campuses, departments, offices, faculty and staff, (hereinafter “University’) whether such information pertains to individuals with whom the institution has a relationship, or pertains to people who have a relationship with other institutions that have provided the information to the University. These safeguards are provided to:

- Ensure the security and confidentiality of Covered Data;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of Covered Data that could result in substantial harm or inconvenience to any individual.

This APL also provides for mechanisms to:

- Identify and assess the risks that may threaten Covered Data maintained by the University;
- Develop written policies and procedures to manage and control these risks;
- Implement and review the Plan; and
- Adjust the Plan to reflect changes in technology, the sensitivity of Covered Data and internal or external threats to information security.
II. Definitions

“Covered Data” for the purpose of this Plan includes, but is not limited to, any record containing information which is confidential by law, any record containing Personally Identifiable Financial Information and any list, description or grouping derived using Personally Identifiable Financial Information, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the University or its affiliates. “Covered Data” includes Student Financial Information (defined below) required to be protected under the GLBA. In addition to this coverage which is required under federal law, the University chooses as a matter of policy to also include in the definition of “Covered Data” any credit card information received in the course of business by the University of Maine System. Notwithstanding the above, “Covered Data” does not include any information which is a public record as defined in 1 M.R.S.A. §402(3) or publicly available information as defined in GLBA.

“Personally Identifiable Financial Information” is information provided by a consumer to obtain a financial product or service; information about a consumer resulting from a transaction involving a financial product or service; or information otherwise obtained about a consumer in connection with providing a financial product or service to that consumer.

“Student Financial Information” is that Personally Identifiable Financial Information that the University has obtained from a student in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include, but are not limited to addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers.

III. Identification and Assessment of Risks to Covered Data

The University recognizes that it has both internal and external risks. Each department is responsible for identifying the types of information and the forms of the information with which it deals. The department must then identify and document the potential risks to the security, confidentiality and integrity of the respective department’s Covered Data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. Such potential risks include, but are not limited to:

- Use of Social Security Number as student identification number;
- Lack of or failure to use locks on file cabinets, offices, etc;
ADMINISTRATIVE PRACTICE LETTER

SUBJECT: SECURING CUSTOMER INFORMATION

- Inadequate procedures and mechanisms for responding to requests for Covered Data;
- Failure to appropriately destroy Covered Data when no longer needed;
- Storage and transmission of unencrypted Covered Data;
- Sharing of computer IDs and passwords;
- Inadequate computer backup procedures and failure to adequately protect the hardware;
- Computers left on and unattended; failure to use screen savers.
- Inappropriate procedures or physical space for discussing Covered Data or playing communication devices, such as voice mail;
- Unauthorized access to Covered Data by someone other than the owner or other appropriate University staff member in the performance of their job;

Potential Results Include:

- Compromised system security as a result of system access by an unauthorized person;
- Interception of data during transmission;
- Loss of data integrity;
- Physical loss of data;
- Errors introduced into the system;
- Corruption of data;
- Unauthorized access to Covered Data;
- Responding to inappropriate requests by furnishing Covered Data;
- Unauthorized transfer of Covered Data through third parties;
- Unauthorized use of an ID or password;
- Compromised system security due to infiltration.

The University recognizes that this may not be a complete list of the risks associated with the protection of Covered Data. Since technology growth is not static, new risks are created regularly. Accordingly, the UMS IT Department will actively participate and monitor advisory groups such as the EduCause Security Institute, the Internet2 Security Working Group and SANS for identification of new risks.

The University’s safeguards as set forth in this APL are reasonable and are intended to provide security for and the confidentiality of Covered Data maintained by the University. These safeguards protect against currently anticipated threats or hazards to the integrity of such information. The University recognizes that, to have an effective security plan, risk assessment, monitoring and corrective action efforts must be ongoing. As such, the University will periodically review this Plan and update University procedures and safeguards as risks change.
IV. Information Security Plan Coordinators

Employees on each campus of the University of Maine System have been appointed as the coordinators of this Plan. (See individual campus Information Security Plans.) Together with department heads, they are responsible for assessing the risks associated with unauthorized access to and use of Covered Data and implementing procedures to minimize those risks to the University. Internal Audit personnel will also periodically review areas that have access to Covered Data to assess the internal control structure and to determine if University departments are in compliance with the requirements of this APL.

V. Design and Implementation of Safeguards Program

a. Employee Management and Training

References of new employees working in areas that regularly work with Covered Data will be checked by the search committee or the employee responsible for hiring. During employee orientation, each new employee in these departments will receive training on the importance of confidentiality of student records, student financial information, and other types of Covered Data. Each new employee also will be trained in the proper use of computer information, IDs and passwords. Training also will include controls and procedures to prevent employees from providing Covered Data to an unauthorized individual, including “pretext calling” and how to properly dispose of documents that contain Covered Data. (“Pretext calling” occurs when an individual improperly obtains personal information so as to be able to commit identity theft. It is accomplished by contacting the University, posing as a student, employee or someone authorized to have the information, and through the use of trickery and deceit, convincing an employee of the University to release identifying information.) Each department responsible for maintaining Covered Data will take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures. Further, Information Security Plan Coordinators will communicate on an annual basis with each department responsible for maintaining Covered Data to determine and coordinate additional safeguarding and privacy training appropriate to the department. University Counsel will be consulted as needed. One-on-one training may be necessary in some circumstances. These training efforts should help minimize risk and safeguard Covered Data security.
b. Administrative Safeguards

Where possible, the University will avoid using the Social Security Number as the primary identifier when providing services to students, applicants, employees or others. In addition, departments shall adopt other procedures and practices that reduce the dependency on and use of the Social Security number. For example, departments shall update forms where possible and as appropriate so that employees’ and students’ PeopleSoft IDs are used as the identifier rather than Social Security numbers. If needed in order to verify a person’s identity, date of birth and/or the last four digits of the SSN may be used. When grades are posted for students’ viewing, whether in hallways, on office doors, or on electronic bulletin boards, the Social Security number or any part of it shall not be used as an identifier. When sending Covered Data in an e-mail, such Covered Data shall not be included in the subject line of the e-mail. People shall be identified in the body of an e-mail only by name and last four digits of SSN, if necessary. Discussions of Covered Data shall be conducted in as private a location and manner as possible. (See Appendix A - “Checklist for Safeguarding Information” for more specific administrative safeguards.)

c. Physical Security

The University has addressed the physical security of Covered Data by limiting access to only those employees who have a business reason to know such information. For example, personal customer information, accounts, balances and transactional information shall be available only to University employees with an appropriate business need for such information. Loan files, account information and other paper documents shall be kept in file cabinets, rooms or vaults that are locked each night. Only authorized employees shall know combinations and the location of keys. Paper documents that contain Covered Data must be shredded at time of disposal. (See Appendix A - “Checklist for Safeguarding Information” for more specific physical safeguards.)

d. Information Systems

Access to Covered Data via the University’s computer information system shall be limited to those employees who have a business reason to access such information. Each individual shall be assigned a personal ID and shall maintain their password in accordance with best practices. The password will be kept confidential and kept in a secured location if written down.
When disposing of computers, hard drives, software, diskettes or any other electronic media, all Covered Data must be electronically or physically destroyed. Deleting files or moving them to the recycle bin and emptying the recycle bin are inadequate. Diskettes and CD’s will be shredded or otherwise destroyed.

The University will take reasonable and appropriate steps consistent with current technological developments to ensure that all Covered Data is secure and to safeguard the integrity of records in storage and transmission.

The University’s firewalls will be configured to allow only legitimate University hardware and software to access Covered Data.

All University hardware and software will be maintained in accordance with best practices which will include physical security, fire protection, console intrusion prevention, periodic data and software back-up, restore cycling and the timely maintenance of the operating system including application of patches and updates.

IT Management will maintain an Incident Response Policy which will include a mechanism for sharing information between all members of the University responsible for intrusion prevention and mitigation.

When electronically transmitted, (including e-mails) all Covered Data will be encrypted or similarly protected from unauthorized access.

Covered Data will be stored on devices that are protected from unauthorized access by the University’s Firewall-IDS (Intrusion Detection Systems).

When Covered Data cannot be stored on a device which is protected by the University’s Firewall-IDS system, (i.e. temporarily or permanently off the network) the Covered Data will be encrypted and password protected. Devices used off the University network will be configured with an operating system, antiviral, personal firewall and similar software which will preclude the device from passing any infection acquired off the network to the network when (re)connected.

All firewall software will be kept current.
The University has a number of policies and procedures in place to provide security to the University’s information systems. These policies are maintained at both the campus and SWS levels of the University and are available upon request from the Office of the UMS Chief Information Officer.

e. Management of System Failures

Any and all system failures or other breaches of security will be reported immediately to the supervisor of the area in question. The supervisor shall notify the campus Information Security Plan Coordinator(s) and other appropriate campus and System staff. UNET has developed written plans and procedures to detect any actual or attempted attacks on University systems and has an Incident Response Policy which outlines procedures for responding to an actual or attempted unauthorized access to Covered Data. This policy is available upon request from the Office of the UMS Chief Information Officer. An investigation must be conducted of an alleged violation of the safeguards for Covered Data by an employee and any sanctions must be imposed in accordance with existing University disciplinary procedures and any applicable Collective Bargaining Agreement. The sanction imposed for a violation of these safeguards will depend on the severity of the violation. Human Resources staff will review the incident and determine suitable discipline up to and including termination of employment.

VI. Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that the University determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access Covered Data, the evaluation process shall include the ability of the service provider to safeguard Covered Data. The University will require by written contract that the service provider implement and maintain appropriate administrative, technical and physical safeguards. The University of Maine System Administrative Practice Letter No. VII-A – University of Maine System Purchasing Procedures - includes addenda and attachments to be used in conjunction with current and future contracts that require safeguarding language.
VII. **Continuing Evaluation and Adjustment**

The University will regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems and procedures. This Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within UNET and campus IT departments, where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the UMS Chief Information Officer, designated Information Security Plan Coordinators, UNET, campus IT staff and System Office staff, who will assign specific responsibility for implementation and administration as appropriate. The Coordinators, in consultation with the Office of University Counsel, the UMS Chief Information Officer and the Office of Finance and Treasurer, will review the standards set forth in this APL and campus plans and recommend updates and revisions as necessary. It may be necessary to adjust the APL and campus plans to reflect changes in technology, the sensitivity of Covered Data, internal or external threats to information security and applicable law. A committee of campus coordinators and System Office staff will meet periodically to evaluate the effectiveness of the information security safeguards and any changes in applicable laws and will make recommendations to the administration for any necessary modifications.

VIII. **Campus Information Security Plans**

Each of the University institutions may adopt procedures and policies for carrying out the provisions of this APL within the guidelines set forth by and consistent with this APL. Campus Information Security Plans, including Campus IT Security Plans, together with this APL and other University policies regarding the security of Covered Data, constitute the University of Maine System Information Security Plan.

**APPROVED:**

________________________
Chief Financial Officer and Treasurer
APPENDIX A

Checklist for Safeguarding Information

The University of Maine System collects and stores a large volume of information. Some of this information is federally legislated as private and must be protected in accordance with laws such as the Gramm-Leach-Bliley Act (“GLBA”) for non-public personal financial information and the Family Education Rights and Privacy Act (FERPA) for student records.

General Guidelines

☐ Read this checklist for safeguarding information and adhere to its principles.
☐ Contact your local Desktop Support Technician with any questions you have about protecting electronic information.
☐ If you are in doubt as to whether certain information is considered private, contact the office responsible for that information or contact University Counsel.
☐ If you hire vendors or other outside parties who will be handling UMS information that must be safeguarded, be sure that the necessary addendums or attachments pertinent to safeguarding information are included in the contract. See APL VII-A for further information.
☐ Ensure that you provide to vendors or other employees only information that is absolutely necessary to perform the requested function.
☐ Lock desks and file cabinets where sensitive information is stored, and lock office doors at the end of the workday.

Information Communicated Orally

☐ Do not discuss confidential information outside of the workplace or with anyone who does not have a specific need to know.
☐ Be aware of the potential for others to overhear communications about sensitive information in offices, on telephones, and in public places.

Information Stored on Paper

Documents that include confidential information like social security numbers, student education records, medical benefits, compensation, loan, financial aid, credit card number, driver’s license number, etc. need to be secured during printing, transmission (including by fax and e-mail), storage, and disposal.

☐ Do not leave paper documents containing sensitive information unattended; protect them from the view of passers-by or office visitors.
☐ Store paper documents containing sensitive information in locked files.
☐ Do not leave the keys to file draws containing confidential information in unlocked desk drawers or other areas accessible to unauthorized personnel.
☐ Store paper documents that contain information that is critical to the conduct of University business in fireproof file cabinets. Keep copies in an alternate location.
ADMINISTRATIVE PRACTICE LETTER

SUBJECT: SECURING CUSTOMER INFORMATION

- Shred confidential paper documents that are no longer needed and secure such documents until shredding occurs. Shredders should employ the cross-cut method of shredding. If a shredding service is employed, ensure that the service provider has clearly defined procedures in the contractual agreement that protect discarded information and that the provider is legally accountable for those procedures, with penalties in place for breach of contract.

- Make arrangements to immediately retrieve or secure sensitive documents that are printed on copy machines, fax machines, and printers.

- Double-check fax messages containing confidential information:
  - Recheck the recipient’s number before you transmit
  - Verify the security arrangements for the receipt of the fax prior to sending
  - Verify that you are the intended recipient of faxes you receive

Information Stored Electronically

- Orient your computer screen away from the view of people passing by.
- Screen savers with password protection should be set to activate with a reasonably short period of time.
- Completely shut down your desktop computer at the end of the workday. If you must leave your desktop computer on for UNET back-up service or for remote access, make sure you have followed the proper procedures to “lock-down” your computer with the appropriate password protection.
- Secure your passwords – if you must write them down, do not store them in an unsecure area. They should be kept in a locked drawer or cabinet.
- Passwords should not be shared.
- Use passwords that are easy for you to remember but impossible for someone else to guess:
  - Make sure to change passwords promptly and frequently.
  - Passwords should not consist of a word that can be found in a dictionary
  - Passwords should consist of a combination of numeric characters, mixed upper and lower case alpha characters, and at least one special character.
  - Consider using the first letter of each word in a phrase or sentence that you can easily remember. For example, "pC#1imb" is derived from “Professor Carter is #1 in my book.”
- Do not download and install various free software programs as these may also install Spyware software which allows the original owner or sender of the software to access your hard drive without your knowledge and/or log your keystrokes.
- Do not open unexpected e-mail attachments.
- Do not download documents from unknown parties.
- Take precautions not to send anything by e-mail that you would not want disclosed to unknown parties. Keep in mind that recipients of your email may then distribute the information to unauthorized recipients or store it on an unsecured machine.
- Make sure that all Anti-Virus and operating system updates are promptly installed.
- Physically secure your computer - especially laptops.
- Make sure that computer hard drives declared as surplus or going out of service for other reasons 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.
- Be aware that information stored on laptops, cell phones, and other mobile devices is susceptible to equipment failure, damage, or theft. Proper firewalls, encryption, and antivirus software must be in place to help ensure that data being transmitted remains secure.