Written Information Security Program (WISP)

1. Purpose

The University of Massachusetts Lowell ("UML") maintains a Written Information Security Program ("WISP") to:

- Protect the confidentiality, integrity, and availability of UML information and systems,
- Document the administrative, technical, and physical safeguards established, considering UML's size, complexity, and scope of activities, to manage information security risks, and
- Comply with:
  - Massachusetts General Laws Chapter 93H and 201 CMR 17.00,
  - The Gramm-Leach-Bliley Act (GLBA) Safeguards Rule,
  - Payment Card Industry Data Security Standard (PCI DSS), and
  - Other applicable federal and state laws and regulations.

This WISP supersedes prior standalone GLBA and WISP documents and consolidates them into this unified program document for the UML campus. This document describes the activities UML undertakes to protect Covered Information in order to comply with the provisions of the Federal Trade Commission's safeguard rules implementing applicable provisions of the GrammLeach-Bliley Act (GLBA).

2. Definitions

Customer - means any individual who receives financial services from the University. Customers may include students, parents, spouses, faculty, staff, and third parties.

Non-public personal information - means any personally identifiable financial or other personal information, not otherwise publicly available, that the University has obtained from a customer in the process of offering a financial product or service; such information provided to the university by another financial institution; such information otherwise obtained by the University in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

Financial product or service - includes student loans, employee loans, activities related to extending credit, financial and investment advisory activities, management consulting and counseling activities, community development activities, and other miscellaneous financial services as defined in 12 CFR § 225.28.

Gramm Leach Bliley (GLBA) The Gramm-Leach-Bliley Act, (GLBA) effective May 23, 2003, addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA contains no exception for colleges or universities. As a result, educational entities that engage significantly in financial activities, such as processing student loans, are required to comply. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices both electronic and physical (employee, student, customer, alumni, donor, etc.). Therefore, the University has adopted an Information Security Program for financial information. This security program applies to customer financial information ("Covered Information") the University receives during business as required by GLBA as well as other confidential financial information the University has voluntarily chosen as a matter of policy to include within its scope. The GLBA requires that the University develop, implement, and maintain a comprehensive information security program containing the administrative, technical, and physical safeguards that are appropriate based upon the University's size, complexity, and the nature of its activities

Covered Information - for the purposes of this WISP includes non-public personal information of customers required to be protected under GLBA. In addition to this required coverage, the university chooses as a matter of policy to also define covered information to include any bank and credit card account numbers, income and credit information, tax returns, asset statements, and social security numbers received during business by the University, whether such financial information is covered by GLBA. Covered information includes both paper and electronic records.

Massachusetts General Laws Chapter 93H and 201 CMR 17.00 are Massachusetts data security laws and regulations that require organizations that own or license personal information about Massachusetts residents to develop, implement, and maintain a written information security program (WISP) containing administrative, technical, and physical safeguards to protect that information.

Payment Card Industry Data Security Standards (PCI DSS) are global security standards that requires organizations that store, process, or transmit credit card data to implement technical and operational controls to protect that data from theft and misuse. It is maintained and managed by the PCI Security Standards Council (PCI SSC), an independent body founded in 2006 by the major payment card brands.

3. Scope

UML's WISP addresses:

- UML-owned or managed information systems;
- Personal information of Massachusetts residents processed or held by UML;
- Covered Information under GLBA and PCI-DSS processed or held by UML;
- UML workforce who process Covered Information, manage or implement information security safeguards and controls, or maintain systems that process Covered Information.
- Information security administrative, technical and physical safeguards and controls designed to protect UML Covered Information and systems.
- Note: while UML's WISP is designed to comply with Massachusetts General Laws Chapter 93H and 201 CMR 17.00, federal regulations such as the GLBA Safeguards Rule, and PCI-

DSS requirements, in the event of a security incident, UML will also comply with applicable state breach notification laws based on the residency of affected individuals.

4. Information Security Roles and Responsibilities

4.1. Overview

The Information Security Program has the following components:

- Designating an employee or office responsible for coordinating the program;
- Conducting risk assessments to identify reasonably foreseeable security and privacy risks;
- Designing and implementing safeguards to control the risks identified;
- Testing and monitoring the effectiveness of safeguards;
- Reviewing the security programs and safeguards of service providers; and
- Maintaining and adjusting this Information Security Program based upon the results of testing and monitoring, as well as changes in operations.

4.2 Information Security Program Leadership

The UML Chief Information Security Officer (CISO) is responsible for the Information Security Program.

Unless otherwise designated by UML's Chief Information Officer (CIO), the UML Chief Information Security Officer (CISO) serves as the:

- Designated coordinator responsible for the Information Security Program requirements under GLBA;
- Information Security Program Coordinator under 201 CMR 17.00;
- Campus-level official for PCI-DSS Requirement 12 information security governance obligations. (Top-level oversight for PCI-DSS compliance resides with the University of Massachusetts' system-level Treasury department.)

The CISO:

- Works closely with the University Registrar, Human Resources, the Office of Legal Affairs, the Office of the Bursar, the Office of Student Financial Aid, the Internal Audit Department, the UMass Lowell Office of Information Security, the Controller's office and such other offices and units as may have interface with or control over GLBA Covered Information;

- Consults with responsible offices and Data Custodians to identify units and areas of the University with access to Covered Information;

- Utilizes reasonable measures to include all areas with Covered Information within the scope of the Information Security Program;

- Conducts risk assessments and monitors that appropriate controls are in place for identified risks to Covered Information;

- Designates information security resources to monitor and manage the information security program and safeguards;

- Works with responsible parties to ensure security awareness education is developed and delivered for employees with access to Covered Information;

- Investigates problems and alleged violations of information technology policies and refers violations to appropriate university offices for resolution or disciplinary action;

- Reviews periodically, in consultation with other University offices, the existing policies, procedures, standards and guidelines that provide for the security of Covered Information and makes recommendations for revisions, or the development of new policy, as appropriate; and

- Updates and maintains the Information Security Program and written information security program, including this and related documents annually; makes them available upon request as needed to the university community; and formally reports to the Chief Information Officer and university leadership at least annually on the Information Security Program, addressing program status, material issues and decisions, and recommended program updates. In accordance with the GLBA Safeguards Rule, the required annual reporting to the University of Massachusetts Board of Trustees or appropriate committee thereof is fulfilled through established UMass system-level governance and audit processes.

4.3 Other Roles and Responsibilities

4.3.1 Deans, Directors, Department Heads, and other Managers

The dean, department head, director, or other managers responsible for managing employees with access to Covered Information will designate Data Custodians and other resources as required to work with the Coordinator to assist in implementing the program. Responsibilities for assigned resources include risk assessment for the unit and monitoring based upon the results of assessment. The designated resources will report when requested on the status of the protection of Covered Information accessible in that unit to the Coordinator.

4.3.2 Data Custodians

Data Custodian(s) are designated departmental leaders under UMass system-wide policy with responsibility for Covered Information or other confidential data. System-wide policy defines Data Custodian(s) as the individual(s) responsible for making decisions about the sensitivity and criticality of specific University systems and data stored in these systems. Data Custodians:

- Approve access to systems with Covered Information for users with appropriate job-related responsibilities and at appropriate access levels;

- Make decisions about the sensitivity and criticality of specific university systems in their scope of responsibility and the data stored in these systems on behalf of the university;
- Establish the classification level(s) of data under their control; and
- Maintain any required documentation for the information and system(s) in their scope of responsibility, including the current inventory of systems and data sets containing covered information within their area of responsibility.
- Access to Covered Information is limited to those who reasonably require it to perform their job duties. Access is removed following UML policies and procedures after termination of employment or change in job duties.

4.3.3 Employees with Access to Covered Information

Employees with access to Covered Information must abide by university policies and procedures governing Covered Information as well as any additional practices or procedures established by their leadership.

5. Information Security Program Components

5.1 Risk Assessments

The Information Security Program includes risk assessments to identify reasonably foreseeable external and internal risks to the confidentiality, availability, and integrity of Covered Information and to assess the sufficiency of safeguards in place to control these risks.

Risk assessments are conducted periodically through system-level audits and external assessments and are supplemented by ongoing institutional risk evaluation activities, including vendor risk assessment, vulnerability management, security monitoring, incident response analysis, control testing, and assessment of material changes to systems or operations.

Risk assessments are conducted using defined criteria to evaluate the likelihood and potential impact of identified risks to the confidentiality, integrity, and availability of Covered Information. Identified risks are documented and assigned appropriate treatment strategies, including mitigation, transfer, avoidance, or acceptance based on institutional risk tolerance. Risk assessments are reviewed and updated periodically and upon material changes to university operations, information systems, business arrangements, or the threat environment.

The Coordinator will work with stakeholders to carry out and document institutional risk assessments addressing safeguards for systems, service providers and Covered Information.

5.2 Information Safeguards and Monitoring

The Information Security Program will implement administrative, technical and physical safeguards to control the risks identified in risk assessments. Safeguards and monitoring will include the following:

5.2.1 Employee Management and Training

Safeguards include HR background checks at hire, formal personnel evaluation processes, annual security awareness training for all workforce members, and additional role-based PCI-DSS training for designated individuals. In addition, UML maintains a regular program of information security awareness reminders through the electronic boards on campus and conducts monthly simulated phishing exercises to increase workforce resiliency to phishing threats.

5.2.1 Policies, Procedures, Standards, and Guidelines

UML has established policies, procedures, standards, and guidelines for acceptable use of systems and for protecting Covered Information. The Information Security Program incorporates by reference the university's policies and procedures and augments institutional policies and procedures that may be required pursuant to other federal and state laws and regulations. Information about UML's information security policies and other compliance areas at UML can be found on the university's policies portal. (See Section 11. *References and Resources*, below, for link.) Violations of UML's policies are subject to UML's Human Resources progressive disciplinary procedures.

5.2.2 Information Systems Administrative and Technical Safeguards

Information systems include network and software design, as well as information processing, storage, transmission, and retrieval. Network and software systems at the university are designed to limit the risk of unauthorized access to Covered Information.

UML implements information system administrative and technical safeguards appropriate to risk, including:

- Multi-factor authentication,
- Encryption of personal information in transit and at rest, including encryption of university-managed laptops and portable devices, encrypted transmission methods across wireless and public networks.
- Network segmentation and firewalls protecting internal systems from the Internet as well as separating campus, student, PCI, building services, and other internal networks from each other,
- Logging, detection and response tools to detect malicious software, system compromises and intrusions,
- Active 7x24x365 monitoring,
- Secure Email gateway software,
- Continuous vulnerability scanning of UML networks, specialized quarterly PCI compliance scanning, and annual penetration testing,
- Patch management,
- Endpoint protection,
- Secure configuration standards,
- Formal change management processes,
- Least privilege and role-based access controls, and
- Periodic access review (recertification) for key HR, student and financial systems.

5.2.3 Managing System Failures and Incidents

UML maintains systems and written incident detection and response procedures to prevent, detect, and respond to attacks, intrusions, and other system failures. As a sub-process of the Information Technology Major Incident procedures, *Information Security Incident Reporting, Investigation and Response Procedures* have been documented addressing the goals of security incident response, defined response team roles and responsibilities, procedures for identification, containment, eradication and recovery from an incident, and documentation and post-incident review.

5.2.4 Monitoring and Testing

Systems are implemented to regularly test and monitor the effectiveness of information security safeguards, including technical testing such as vulnerability scanning and penetration testing, key system access recertification, auditing by UMass system and external auditors, and active log and threat monitoring for misuse of systems or personal information by the university's Managed Detection and Response vendor.

5.2.5 Physical Safeguards

UML manages admittance to secure areas with ID card access systems and uses hardened data center facilities with appropriate physical and environmental security controls. Paper records containing Covered Information are stored securely.

UML has secure destruction and device sanitization procedures to address disposal of records and electronic devices.

5.3 Service Provider Review and Oversight

In the course of doing business, the University may appropriately share Covered Information with third parties, such as in support of collection activities, transmission of documents, transfer of funds, destruction of documents or equipment, or other similar services.

5.3.1 Vendor Risk Assessment

The university's procurement process includes a risk management component to identify service providers that will be allowed access to Covered Information or other sensitive data or resources in the course of providing services.

The CISO (or designee) works with the Procurement Office, the General Counsel, and other stakeholders as appropriate, to review the security controls of prospective vendors identified through this process. Where warranted, service providers must complete a Higher Education Community Vendor Assessment Tool (HECVAT) questionnaire to measure vendor risk or provide comparable alternative documentation in the form of a SOC2 audit report or similar.

Results are reviewed, documented, and shared with stakeholders to support selection of service providers that are skilled and trained in information security and can maintain appropriate safeguards for Covered Information. When needed, contract terms in addition to standard template language requiring service providers to implement and maintain specific safeguards are raised with Procurement.

5.3.2 Credit card processing vendors

All UMass system merchants that accept credit or debit cards are required to comply with the PCI-DSS in their entirety and contract language includes this responsibility. PCI vendors are vetted and undergo risk assessment by UMass Treasury, which maintains an annual system-wide PCI compliance and training process. The process includes designated eCommerce representatives at each campus, including members of the UML IT security department for IT and technical controls support for UMass Treasury, PCI audit processes, and UML merchant departments. The process addresses validation and documentation of the PCI scope, review of policies and procedures, validation of merchant department and vendor compliance with PCI 4.0, and validation of PCI network segmentation.

6. Information Security Program Maintenance

The WISP is a departmental procedure of the UML Information Technology department. The CISO, working with responsible units and offices, will annually evaluate and adjust the Written Information Security Program (WISP) as needed considering stakeholder requirements, the results of testing and monitoring, changes in the threat landscape, material changes to operations or business arrangements, legal and regulatory updates and any other circumstances which may reasonably have an impact on the Information Security Program. Updates will be approved by the CISO and formally accepted as an IT procedure by the CIO.

7. References and Resources

- Policies : Policy Portal : Web Services : University of Massachusetts Lowell
- Cybersecurity Framework | NIST *(National Institutes of Science and Technology)*
- CIS Critical Security Controls *(Center for Internet Security)*
- Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements | FSA Knowledge Center *(US Department of Education)*
- University of Massachusetts Policy Statement on Data Security, Electronic Mail, and Computer Policy Development (*DocT97-101, UMass President's Office*)
- eCommerce Compliance Resources | UMass Office of the President

8. Revision History

Effective date	Change History

5/1/2016	*Written Information Security Plan (WISP),* v 1.0
1/30/2020	*Written Information Security Plan (WISP),* v 1.1
5/1/2020	*Information Security Program and GLBA Compliance*
6/26/2025	*Information Security Program and GLBA Compliance*
3/4/2026	*Written Information Security Program (WISP), v 2.0* This UML WISP supersedes prior standalone GLBA and WISP documents and consolidates them into a unified program document that also supports PCI-DSS requirements for information security governance.