Written Information Security Plan (WISP)

Effective Date: 5/01/2016
Last Review Date: 01/30/2020

I. Introduction

The Written Information Security Program (WISP) is a set of comprehensive guidelines and policies designed to safeguard personal information maintained at the University of Massachusetts Lowell (UML) and to comply with applicable state and federal laws and regulations on the protection of personal information.

The WISP has been adopted in accordance with Chapter 93H of the Massachusetts General Laws and corresponding regulations setting forth Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR §17)' and other applicable laws, regulations, and contractual obligations.

In the course of carrying out its academic, research and administrative missions, faculty, staff and students at UMass Lowell ("University"), collect many different types of information including financial, academic, medical, human resources and other personal information. Such information is an important resource of the University and any person who uses information collected by the University has a responsibility to maintain and protect this resource. Federal and state laws and regulations, as well as industry standards, also impose obligations on the University to protect the confidentiality, integrity and availability of information relating to faculty, staff, students, research subjects and patients. Additionally, terms of certain contracts and University policy require appropriate safeguarding of information.

This Plan and the information security policies adopted by the University (collectively, the "Information Security Policies") define the principles and terms of the University's Information Security Management Program (the "Information Security Program") and the responsibilities of the members of the University community in carrying out the Information Security Program. The current Information Security Policies are listed in Appendix A.

The information resources (the "Information Resources") included in the scope of the Information Security Policies are:

- All Data (as defined in Section IV below) regardless of the storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, CD, DVD, external drive, copier hard drive, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.);
- The computing hardware and software Systems (as defined in Section IV below) that process, transmit and store Data; and
- The Networks (as defined in Section IV below) that transport Data.

The Information Security Policies are University-wide policies that apply to all individuals who access, use or control Information Resources at the University, including faculty, staff and students; as well as contractors, consultants and other agents of the University and/or individuals authorized to access Information Resources by affiliated institutions and organizations.

The WISP has been adopted in accordance with Chapter 93H of the Massachusetts General Laws and corresponding regulations setting forth Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR §17)' and other applicable laws, regulations, and contractual obligations

II. The Mission

The mission of the Information Security Program is to protect the confidentiality, integrity and availability of Data. Confidentiality means that information is only accessible to authorized users. Integrity means safeguarding the accuracy and completeness of Data and processing methods. Availability means ensuring that authorized users have access to Data and associated Information Resources when required.

This Plan establishes the various functions within the Information Security Program and authorizes the persons described under each function to carry out the terms of the Information Security Policies.

The functions are:

A. Executive Management

Executive Managers are senior University officials, including the Provosts, Deans, Vice Chancellors, Department Chairs, and Department Heads, who are responsible for overseeing information security for their respective areas of responsibility and ensuring compliance with all Information Security Policies. Such responsibilities include, but are not limited to:

- Ensuring that each System Owner and Data Owner in their respective areas of responsibility appropriately identify and classify Data in accordance with the UMass Lowell Data Classification Policy;
- Ensuring that each such System Owner and Data Owner receives training on how to handle Sensitive Data and Confidential Data; and
- Ensuring that each IT Custodian/Administrator in his/her area of responsibility provide

periodic reports with respect to the inventory of Information Resources used in such area to the applicable Information Security Office.

B. Security, Policy and Compliance Governance

The following committees have been established to govern security, policy and compliance issues relating to the Information Security Program at the organizational level:

- Information Security Steering Committee
- UMass Lowell Policy Committee
- Information Security Cabinet (UMass System-wide – advisory capacity)

C. Security Management

The Chief Information Security Officer (CISO) is responsible for the management oversight of the Information Security Program/Office. The Office is responsible for the day to day management of the Information Security Program, including:

- Developing, documenting and disseminating the Information Security Policies;
- Educating and training University personnel in information security matters;
- Communicating information regarding the Information Security Policies;
- Developing and executing the Information Security Risk Management Program;
- Translating the Information Security Policies into technical requirements, standards and procedures;
- Collaborating with Data Owners and System Owners to determine the appropriate means of using Information Resources.; and
- Authorizing any required exceptions to any Information Security Policy or any associated technical standards or procedures and reporting such exceptions to the Office of the General Counsel.

In addition to the responsibilities listed above, the Executive Managers have granted the authority to the Information Security Office to conduct the following activities:

- Monitoring communications and Data that use the University Network or Systems for transmission or storage;
- Monitoring use of the University's Information Resources;
- Conducting vulnerability scanning of any Information Resources connected to the University Network;
- Conducting security assessments of Systems, Server centers and Data centers;

- Disconnecting Information Resources that present a security risk from the University Network;
- Erasing all Data stored on personal Endpoints previously used for University business, as requested or required; and
- Leading and managing the University Incident Response Team in connection with any breach or compromise of Sensitive Data, to the extent provided for in the UMass Lowell Electronic Data Security Breach Reporting and Response Policy

D. Data Ownership

Data owners are University officials, including Directors, Officers of Instruction and Officers of Research, who are responsible for determining Data classifications, working with the applicable Information Security Office in performing risk assessments and developing the appropriate procedures to implement the Information Security Policies in their respective areas of responsibility. Such responsibilities include, but are not limited to:

- Appropriately identifying and classifying Data in their respective areas of responsibilities in accordance with the University of Massachusetts Lowell Data Classification Policy ;
- Establishing and implementing security requirements for such Data in consultation with the applicable Information Security Office;
- Where possible, clearly labeling Sensitive Data and Confidential Data;
- Approving appropriate access to Data; and
- Ensuring that the UMass Lowell Sanitization and Disposal of Computer Resources Policy is followed.

E. System Ownership

System owners are University officials, including Directors, System Administrators and Officers of Research, who are responsible for determining computing needs, and applicable System hardware and software, in their respective areas of responsibility and ensuring the functionality of each such System. Such responsibilities include, but are not limited to:

- Classifying each System in their respective areas of responsibility based on the identification and classification of Data by the applicable Data Owner;
- Ensuring that each such System that contains Sensitive Data or Confidential Data is scheduled for risk assessment in accordance with the University of Massachusetts Lowell Information Security Risk Management Policy
- Establishing and implementing security requirements for each such System in consultation with the Information Security Office;

- Documenting and implementing audit mechanisms, timing of log reviews and log retention periods;
- Maintaining an inventory of such Systems;
- Approving appropriate access to such Systems; and
- Ensuring that the University of Massachusetts Lowell Sanitization and Disposal of Computer Resources Policy is followed.

F. Technical Ownership

IT Custodians/Administrators are University personnel who are responsible for providing a secure infrastructure in support of Data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges as authorized by Data Owners or System Owners and implementing and administering controls over Data in their respective areas of responsibility. Such responsibilities include, but are not limited to:

- Maintaining an inventory of all Endpoints used in their respective areas of responsibility;
- Conducting periodic security checks of Systems and Networks, including password checks, in their respective areas of responsibility;
- Documenting and implementing audit mechanisms, timing of log reviews and log retention periods;
- Performing self-audits and reporting metrics to the Information Security Office and monitoring assessments and appropriate corrective actions; and
- Ensuring that the UMass Lowell Sanitization and Disposal of Information Resources Policy is followed.

G. System or Data Users

Users are persons who use Information Resources. Users are responsible for ensuring that such Resources are used properly in compliance with the University of Massachusetts Lowell Acceptable Use Policy; information is not made available to unauthorized persons and appropriate security controls are in place.

IV. Reporting Actual Breaches of Security

Incidents that raise concerns about the privacy or security of Personal Information must be reported promptly upon discovery to the Information Security Officer. The Incident Response Team (IRT) shall investigate all reported Security Incidents and Breaches. Led by the UML's Information Security Office, the IRT's objective is to:

1. Coordinate and oversee the response to Incidents in accordance with the requirements of state and federal laws and UML policy;
2. Minimize the potential negative impact to the University, Client and 3rd Party as a result of such Incidents;
3. Where appropriate, inform the affected Client and 3rd Party of action that is recommended or required on their behalf; ·
4. Restore services to a normalized and secure state of operation;
5. Provide clear and timely communication to all interested parties.

V. Employee Training

UML privacy and information security program serves to educate UML workforce in maintaining compliance within their particular UML business function or activity, whether it be under research grants or industry contracts' privacy and security requirements, MGL Ch. 93H - Identity Fraud Statute, the Health Insurance Portability and Accountability Act (HIPAA), or other related federal and state laws and regulations regarding data privacy and information security.

University of Massachusetts Lowell (UML) requires that employees are trained in the proper .handling of sensitive data. All UML faculty, staff, contingent workers, contractors and students in its schools, departments, centers and business units are required to complete privacy and information security training if their job entails the handling of sensitive data.

VI. Enforcement

Violations of the Information Security Policies may result in corrective actions which may include: (a) the immediate suspension of computer accounts and network access; (b) mandatory attendance at additional training; (c) a letter to the individual's personnel or student file; (d) administrative leave without pay; termination of employment or non-renewal of faculty appointment or student status; or (f) civil or criminal prosecution.

VII. Applicable Laws, Regulations and Industry Standards

The federal and Massachusetts State laws and regulations and industry standards that are applicable to information security at the University are listed in Appendix B.

VIII. Approvals

James W. Packard, CISO

1/31/20

Date

Revision Date	Revision Description	Revised by
05/01/2016	V1.0	JWP
01/30/2020	V1.1 – updates	JWP

Appendix A

UNIVERSITY OF MASSACHUSETTS LOWELL

Information Security Policies

Acceptable Usage Policy

Business Continuity and Disaster Recovery Policy

Data Classification Policy

Security Awareness Policy

Email Usage Policy

Institutional Review Board Security Policy

Password Policy

Mobile Device and Cellular Services Policy

Cloud Computing Policy

Information Security Incident Response Policy

Sanitization and Disposal of Information Resources Policy

Appendix B

Applicable Federal and State Laws and Regulations

Federal

The Digital Millennium Copyright Act
http://www.copyright.gov/legislation/dmca.pdf

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

The Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999)
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

The Health Insurance Portability and Accountability Act (HIPAA)
The Health Information Technology for Economic and Clinical Health Act (HITECH)
http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

State of Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth
http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

Industry Standards

Payment Card Industry/Data Security Standard
https://www.pcisecuritystandards.org/tech/

Appendix C

Definitions

As used in the Information Security Policies, the following terms are defined as follows:

AES: the Advanced Encryption Standard adopted by the U.S. government.

Approved Email System: as defined in the University of Massachusetts Lowell Email Policy

UMass Lowell or the University: as defined in Section I of this Plan.

Confidential Data: any information that is contractually protected as confidential information and any other information that is considered by the University appropriate for confidential treatment. See the University of Massachusetts Lowell Data Classification Policy for examples of Confidential Data.

Covered Entity: as defined in HIPAA (45 CFR 160.163).

Data: all items of information that are created, used, stored or transmitted by the University community for the purpose of carrying out the institutional mission of teaching, research and clinical care and all data used in the execution of the University's required business functions.

Data Owner: as defined in Section (D) of this Plan.

Email System: a System that transmits, stores and receives emails.

Endpoint: any desktop or laptop computer (i.e., Windows, Mac, Linux/Unix), Mobile Device or other portable device used to connect to the University wireless or wired Network, access UMass Lowell email from any local or remote location or access any institutional (University, departmental or individual) System either owned by the University or by an individual and used for University purposes.

EPHI: Electronic Personal Health Information.

FERPA: Family Educational Rights and Privacy Act

HIPAA: Health Insurance Portability and Accountability Act

HITECH: Health Information Technology for Economic and Clinical Health Act

IDEA: International Data Encryption Algorithm. Information Resources: as defined in

Section I of this Plan. Information Security

Internal Data: as defined in the University of Massachusetts Lowell Data Classification Policy

IP: Internet Protocol.

IT Custodian: as defined in Section III (F) of this Plan.

Key Business System: as defined in the University of Massachusetts Lowell Business Continuity and Disaster Recovery Policy.

MAC: Media Access Control.

Mobile Device: a smart/cell phone (i.e., iPhone, Android, Windows phone), tablet (i.e., iPad, Nexus, Galaxy Tab and other Android based tablet) or USB/removable drive.

Network: electronic Information Resources that are implemented to permit the transport of Data between interconnected endpoints. Network components may include routers, switches, hubs, cabling, telecommunications, VPNs and wireless access points.

OHCA: an Organized Health Care Arrangement, which is an arrangement or relationship, recognized in the HIPAA privacy rules, that allows two or more Covered Entities who participate in joint activities to share PHI about their patients in order to manage and benefit their joint operations.

Payment Card: for purposes of PCI-DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc.

PCI: Payment card industry.

PCI-DSS: the PCI Data Security Standard produced by the PCI–SSC, which mandates compliance requirements for enhancing the security of payment card data.

PCI-SSC: the PCI Security Standards Council, which is an open global forum of payment brands, such as American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc, that are responsible for developing the PCI-DSS.

Peer: a network participant that makes a portion of its resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by Servers or stable hosts. Examples include KaZaa, BitTorrent, Limewire and Bearshare.

Peer-to-Peer File Sharing Program: a program that allows any computer operating the program to share and make available files stored on the computer to any machine with

similar software and protocol.

PHI: as defined in the University of Massachusetts Lowell Data Classification Policy

PII: as defined in the University of Massachusetts Lowell Data Classification Policy

Public Data: as defined in the University of Massachusetts Lowell Data Classification Policy

Removable Media: CDs, DVDs, USB flash drives, external hard drives, Zip disks, diskettes, tapes, smart cards, medical instrumentation devices and copiers.

Risk Analysis: The process of identifying, estimating and prioritizing risks to organizational operations, assets and individuals. "Risk Assessment" is synonymous with "Risk Analysis".

Risk Management Program: The combined processes of Risk Analysis, Risk Remediation and Risk Monitoring.

Risk Monitoring: The process of maintaining ongoing awareness of an organization's information security risks via the risk management program.

Risk Remediation: The process of prioritizing, evaluating and implementing the appropriate risk-reducing security controls and countermeasures recommended from the risk management process. "Risk Mitigation" or "Corrective Action Planning" is synonymous with "Risk Remediation".

RSA: the Rivest-Shamir-Adleman Internet encryption and authentication system.

Sensitive Data: any information protected by federal, state and local laws and regulations and industry standards, such as HIPAA, HITECH, FERPA, M.G.L. c93H, similar state laws and PCI-DSS. See the University of Massachusetts Lowell Data Classification Policy for examples of Sensitive Data.

Server: any computing device that provides computing services, such as Systems and Applications, to Endpoints over a Network.

SMTP: Simple Mail Transfer Protocol, which is an internet transportation protocol designed to ensure the reliable and efficient transfer of emails and is used by Email Systems to deliver messages between email providers.

SSL: the Secure Sockets Layer security protocol that encapsulates other network protocols in an encrypted tunnel.

Student Education Records: as defined in the University of Massachusetts Lowell Data Classification Policy

System: Server based software that resides on a single Server or multiple Servers and is used for University purposes. "Application" or "Information System" is synonymous with "System".

System Owner: as defined in Section III€ of this Plan.

UPS: Uninterruptible Power Supply.

User: as defined in Section III(G) of this Plan.

User ID: a User Identifier.

VPN: Virtual Private Network.