Information Technology Services
Information Security Office
100 Morrissey Boulevard, Boston, MA 02125

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

I. EXECUTIVE SUMMARY

This document details the University of Massachusetts, Boston (The University) Written Information Security Program (WISP). The WISP sets forth university procedures for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting university information assets and technology resources. The University's security approach is documented in this WISP and based on *implementing controls in layers* and a Defense in Depth Strategy consisting of four critical elements: Visibility, Layered Security, Zero-*Trust (ZT), and Foundational Guidelines.* The objective is to enable university businesses, students, employees, faculty, partners, and visitors to conduct research or business and exchange information and ideas in a secure environment where risk is managed carefully and asset protection is comprehensive and pervasive.

The *WISP* is based on the Center for Internet Security (CIS) Critical Security Controls framework, v8 (The Framework), a prioritized set of actions that collectively form a defense-in-depth (DiD) set of best practices that mitigate attacks against systems and networks. The newest iteration of the Framework considers the wide adoption of cloud-based computing, virtualization, mobility, and Work-from-Home, as well as changing attacker tactics. The model is data-driven and centers its conclusions on Verizon's Data Breach Investigations Report (DBIR), data from the Multi-State Information Sharing and Analysis Center (MS-ISAC), as well as the MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) Framework. This model projects the value of individual defensive actions against those attacks providing a consistent and explainable way to identify the security value of a given set of defensive actions across the attacker's life cycle and the basis for our strategy. Adopting the WISP ensures that the University implements and maintains adequate information security controls that safeguard valuable university assets (Identity, device, network, workloads, and data).

Increasing complexity and uncertainty are the products of adopting a digital life. With that, institutions around the globe witness a sharp rise in emerging threats in an environment of "Everything is Anywhere," where campuses are no longer confined to the classical firewalled physical perimeter. Securing that complexity while keeping some sense of campus-life normalcy is an art of balancing freedom, resiliency, and security.

Wil Khouri, Assistant Vice Chancellor and Chief Information Security Officer

II. TABLE OF CONTENTS

III. VERSION CONTROL

VERSION	UPDATED	RETIRED
2014-R1	04/30/2014	08/31/2015
2015-R1	08/30/2015	05/31/2017
2017-R1	05/30/ 2017	08/31/2019
2019-R1	08/30/2019	05/31/2023
2023-R1	**05/30/2023**	
(Next Rev.) 2024-R1	July 2024	

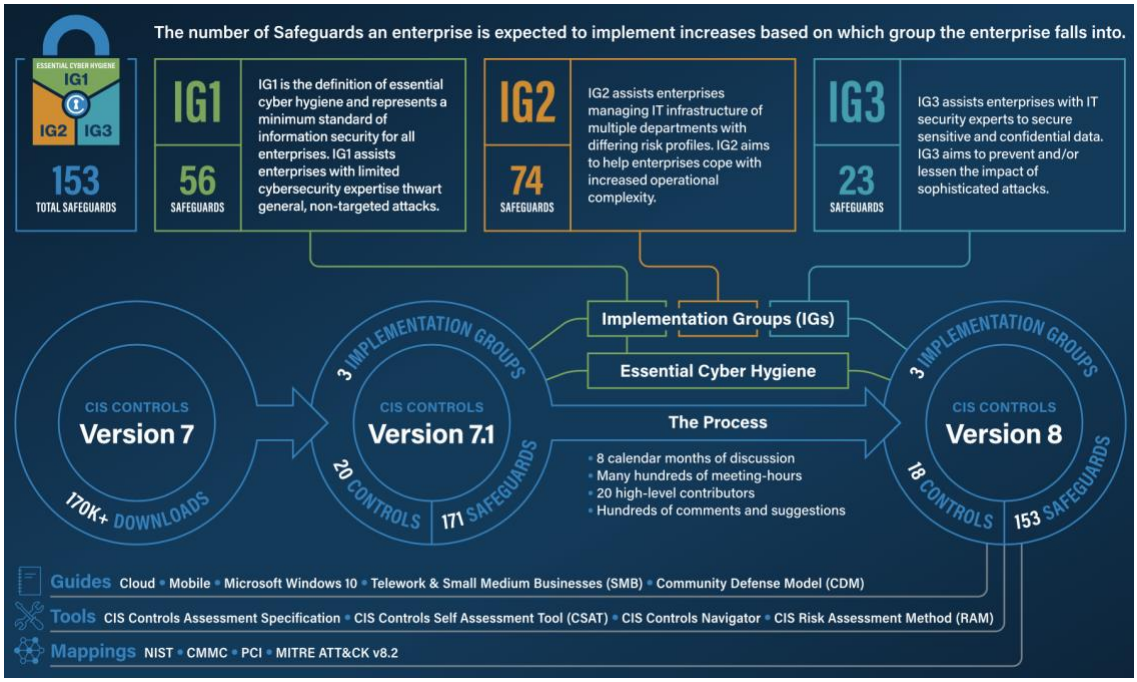
IV. THE CENTER FOR INTERNET SECURITY CONTROLS V8 (THE FRAMEWORK)

1. The Framework's Goals and Objectives

The University uses the Framework as its guide to help it understand, communicate, and manage its cyber risks. The Framework provides the University with a mechanism for gathering and organizing existing global cybersecurity standards and best practices. Additionally, the Framework provides a roadmap based on Framework components to reinforce the connection between the University's business drivers and cybersecurity activities. The Framework includes 18 control areas to evaluate and guide the University's security posture and assists in determining actions to improve its environment.

2. Implementation Groups

The CIS Controls v8 Framework establishes the concept of implementation groups within the controls to scope safeguards based on an organization's size and relative risk. As noted by CIS, these are self-determined categories for organizations. As the University matures, it can prioritize the deployment of safeguards based on the associated implementation group. Definitions of Implementation Groups 1, 2, and 3 are illustrated further in the graphic below.



Based on the size of the University, the nature of its business, and the types of information it processes, it has been assessed as an Implementation Group 3 (IG3) organization. IG3 includes all 153 safeguards of the 18 control areas of the CIS Controls v8 Framework, including those safeguards reserved for highly mature environments.

3. The CIS 18 Controls

The CIS Critical Security Controls framework contains a set of 18 recommended areas of concentration to help ensure the confidentiality, integrity, and availability of systems and data, as illustrated in the table below.

The controls are designed to defend against the most common types of attacks and, when implemented, provide a defense-in-depth strategy to protect the IT environment.

V. Information Security Program, Goals, and Objectives

1. Designated Authority for the Information Security Program

The Assistant Vice Chancellor / Chief Information Security Officer (CISO), under the executive oversight of the Vice Chancellor / Chief Information Officer (CIO), is responsible for developing, implementing, and maintaining a comprehensive standards and risk-based information security program. The WISP is reviewed annually and updated as needed by the CISO.

2. The Information Security Facilities and Staff

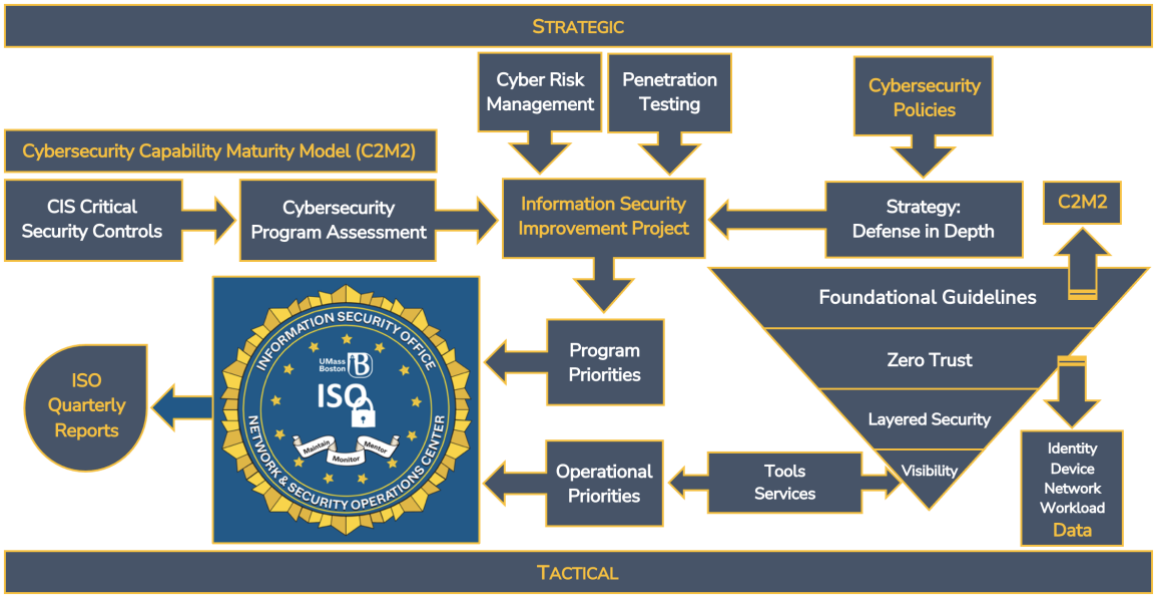
The Information Security Office (ISO) and its staff are responsible for all the activities associated with this Program. In addition, cybersecurity operations are conducted from the Network Security Operations Center (NSOC) to provide rapid response to emerging threats targeting the University.

3. The Information Security Program

The ISO runs various projects and operates tools and services to safeguard personal and institutional data. The ISO manages the NSOC staffed by network and cybersecurity analysts and students in a mentorship format to monitor and proactively mitigate the risks while educating the next generation of network and cybersecurity professionals. The Information Security Program is designed to assist the University's community by:

a. Advising on information security risk management, compliance requirements, and contracts.
b. Providing in-person and online awareness and education.
c. Managing and responding to cybersecurity incidents.
d. Developing and managing University policies related to information security.
e. Monitoring, analyzing, and forecasting threats to information assets.
f. Measuring, analyzing, and reporting Key Performance Indicators (KPIs) to steer decisions.

The ISO Information Security Program, illustrated in the figure below, consists of an amalgam of critical elements: a Defense-in-Depth (DiD) strategy, a Cybersecurity Capability Maturity Model (C2M2), a set of visibility tools and services, controls and frameworks, audits, and assessments, the Information Security Improvement Project (ISIP), and its operational priorities. In addition, the Program is further categorized by an upper strategic layer, which encompasses the top half of the figure, and a lower tactical layer containing the tools, services, and operational priorities.



The components interact under the program umbrella to protect data and systems, establish policies and processes, execute effective measures to stop threat actors, implement purposeful cybersecurity architecture, use cyber intelligence to proactively manage risks and mitigate vulnerabilities, and establish a cybersecurity road map.

C2M2 is a framework of security practices, guidelines, and controls that provide the University with a roadmap for creating an effective and compliant cybersecurity program. C2M2 is a set of tools to benchmark the ISO's current capabilities. It identifies goals and priorities for improvements as prescribed in the Information Security Improvement Project, in which auditors thoroughly assess and rate the outcome. The ISO's Cybersecurity Capability Maturity Model (C2M2) aligns with the Defense-in-Depth (DiD) strategy.

The DiD strategy and associated Framework (CIS Critical Security Controls v8) coupled with the new C2M2 model help organize the Campus cybersecurity mission execution, inform management, and guide decisions. The DiD strategy conforms with the Campus cybersecurity policies.

4. **The Information Security Improvement project (Controls: 01, 02, 05, 06, 08, 11, 18)**

   The ISO staff reviews the University's current security posture yearly. The staff identifies those areas that can most speedily and cost-effectively be improved. The staff then summarizes its findings in a Plan of Action and Milestones (POAM) document dubbed the Information Security Improvement Project (ISIP). The POAM is a corrective action plan for tracking and planning the resolution of information security gaps where it identifies tasks and projects needing to be accomplished, detailing resources required to achieve the elements of the plan, milestones in meeting the tasks, and corresponding scheduled completion dates for the milestones according to "NIST SP 800-37 (Rev.2) Risk Management Framework for Information Systems and Organizations." The ISO pursues a follow-up information security assessment by a third-party entity. Based on the findings, the ISO staff identifies critical and strategic priorities, reviews their impact, and plans for future implementations.

5. **Administrative, Technical, and Physical Controls to protect Personal Information (Controls: 01, 02, 03, 05, 06, 08, 11, 13, 18)**

   The University maintains administrative, technical, and physical controls to protect Personally Identifiable Information (PII) and regulated data:

   a. Administrative controls include but are not limited to, university policies, such as the Acceptable Use of Information Technology Resources Policy (AUP), Confidentiality of Institutional Information and Research Data policy, Security Education Training and Awareness Policy, Data Classification Policy, Data Encryption Policy, and Access Control Policy, internal and external audit, and processes and procedures for granting and revoking access to physical and electronic forms of information.
   b. Technical controls include but are not limited to firewalls, intrusion prevention systems, encryption, anti-malware, patch management, authentication and authorization systems, system logging, file backup, virtual private network, and network monitoring solutions.
   c. Physical controls include but are not limited to the electronic and physical card/key access control systems, locking mechanisms for areas and devices containing sensitive information and information-processing assets, creation of backup media, Cloud storage, intrusion detection systems with central monitoring, closed circuit television monitoring and recording systems, Building Management Systems (BMS), fire detection, reporting and suppression systems, and water leak detection systems.

6. **Identification of printed or electronic records and data, computing systems and endpoints, and storage media that contain PII, and the associated reasonably foreseeable risks (Controls: 01, 02, 03, 04, 05, 06, 09)**

   The University treats all university systems as if they contain PII. Minimum baseline security controls are required for all university systems, including, but not limited to, encryption of data at rest and in transit and protection of such data against unauthorized access to or use of the information in a manner that jeopardizes the confidentiality, integrity, and availability of said data, creating a risk of identity theft or fraud against the University's constituents.

   The University continuously evaluates reasonably foreseeable internal risks to all forms of PII. These evaluations are performed in the normal course of business and cooperation with business and academic units across the University. Recommendations arising from these efforts are

submitted to the applicable department and corresponding data owners for consideration and implementation.

7. Employee Cybersecurity Awareness and Training (Controls: 14)

Per the University's Information Security Training and Awareness Policy, and to further a security culture, the ISO staff conducts an information security awareness program for its community delivered via multiple means:

a. Maintain an Information Security website.
b. Provide a mandatory Cybersecurity Orientation for all new hires.
c. Provide periodic information security training.
d. Publish regular cybersecurity IT news, alerts, and newsletters.
e. Conduct simulated phishing campaigns (Infosec IQ).
f. Run regulated data compliance awareness training.
g. Provide a comprehensive quarterly summary of ISO activities.
h. Conduct a comprehensive National Cybersecurity Awareness Month (NCSAM).

The University offers security awareness and training materials to all students, faculty, and staff, including the proper use of University provided system security software to help minimize risk and safeguard the University's information. The University also sponsors annual information security awareness events including, but not limited to, non-punitive simulated phishing attacks. Specially prepared cyber security awareness and compliance training are made available as needed and as required to meet the unique needs of business, academic, research, and student groups.

8. Policy and Procedures for Monitoring Employee Compliance (Controls: 06, 08, 14)

All individuals applying for electronic access to PII are responsible for familiarizing themselves with all University policies, including handling and protecting sensitive information. Departmental officials and the ISO staff constantly monitor compliance with security procedures. Violations of the policy will follow established disciplinary procedures.

9. Means for detecting and preventing security system failures (Controls: 01, 02, 07, 08, 13, 17)

Security systems are monitored continuously. Failures are reported to appropriate staff via event messages sent to multiple communication channels. Mitigating system failures is accomplished by implementing high-availability fail-over systems, maintaining all security systems with the current operating system and application patches and fixes, and regular maintenance.

10. Blocking of physical and electronic access to records containing Personally Identifiable Information (Controls: 03, 05, 06, 09)

Centrally issued computer accounts are deactivated through notification from Human Resources Management, the Office of the Registrar, special requests through the ISO, or account holder sponsors. Identities of terminated individuals are sent to Information Systems, where automated and manual processes terminate access.

In urgent situations where access must be immediately terminated, a supervisor or other University official may expedite the removal of access through the ISO.

PII records on any device must be encrypted in motion and at rest. Devices and Systems containing PII must be kept in secure facilities.

11. Contracts with third-party providers; Explicit requirement to maintain safeguards consistent with those in "Standards for the protection of personal information of residents of the Commonwealth" (201CMR 17.00) (Controls: 03, 09, 15, 16)

Third-party service providers with whom the University may need to share PII must be evaluated to determine whether they maintain safeguards and practices that protect PII consistent with the Massachusetts data breach regulations. Any University contract with a third-party service provider should require that the service provider protect and maintain PII consistent with Massachusetts data security regulations.

Cloud and SaaS applications service providers and users of said application must complete the "Information Security Risk Assessment Audit for SaaS Applications" form or submit a completed HECVAT (Higher Education Community Vendor Assessment Toolkit) workbook before acquisition.

12. **Procedure for documenting any actions taken in connection with any breach of security and post-incident review of events and actions taken to improve security (Controls: 17)**

    The University maintains an Information Security Incident Management policy, procedures, and plan. As these procedures are executed, contributors document actions taken and post-incident review to improve security where technically, operationally, and financially feasible.
    It is the mission of the Incident Response Team (IRT) to coordinate the response and investigation of attacks on the University's information assets and provide guidance on detecting, containing, and recovering from computer security incidents.

13. **Authentication and Authorization Protocols (Controls: 03, 04, 05, 06, 09, 12)**

    Authentication credentials are created only for individuals identified through established processes as having a right to one or more University technology resources. These accounts are only provisioned for the technology resources to which they are entitled and for which appropriate review has been performed. In addition, all accounts must be provisioned with Multi-factor Authentication (MFA) to provide an additional layer of protection to the sign-in process.

14. **Methods of assigning/selecting passwords; Reasonably secure method of assigning/selecting passwords (Controls: 05, 06)**

    New account holders may either receive a temporary password via email to an account for which identity had previously been established or in person by presenting a valid picture ID. Upon receipt of the temporary password or establishment of identity, the account holder must choose a new password compliant with University password complexity standards.

15. **Control of data security passwords (Controls: 05, 06)**

    Passwords are kept in a location or a format on appropriate technology systems that do not compromise the security of the data they protect. Passwords are generated and maintained on systems in secured areas.

16. **Restricting access to PII to active users and active user accounts (Controls: 03, 05, 06, 09)**

    Access to PII is permitted on a need-to-know and scope-of-employment basis. The duration of time an account is active is limited to the course of a person's role as reported by official University systems of record. Access is revoked as part of the process of termination of employment or engagement. Access can also be revoked on an emergency basis through the ISO.

17. **The University publishes and maintains a records retention and disposition schedule (Controls: 03, 09)**

    Management of the disposition of records is a component of each functional department as described in the University's Records Management Program (RMP). The purpose of the RMP is to establish, in the context of the records lifecycle, the University-wide principles and processes for records retention and disposition and to outline the roles and responsibilities associated with the Program. At the core of the RMP is the concept that records pass through a lifecycle in three stages:

a. Creation (or receipt): Classify (email, records, regulated, etc.) and assign a lifecycle.
b. Use: Active storage area, locked or encrypted.
c. Disposition: Destroy or archive

Judgments about the eventual disposition of records are best made at the beginning of the lifecycle by the data owners. The success of any disposition program depends on an early awareness of which records are to be managed and the need to manage them through all three lifecycle stages. Data Loss Prevention (DLP) tools assist throughout the data's lifecycle.

18. **Blocking access after multiple unsuccessful attempts to gain access (Controls: 03, 06, 08, 13)**

    Access to electronic resources is blocked after a history of unsuccessful attempts to gain access.

19. **Unique identifications and passwords (Controls: 03, 04, 05, 06, 09)**

    Unique user IDs and passwords are assigned to each account holder. Password construction rules allow account holders flexibility in creating passwords while maintaining needed complexity.

20. **Encryption of PII across public and wireless networks (Controls: 03, 09, 12)**

    University practice is that all PII sent across public/Cloud and unencrypted networks be encrypted. PII should only be accessed via ISO-approved encrypted portable devices or media. Privately owned USB flash drives may not be used for PII.

21. **Encryption of PII on portable/removable devices (Controls: 01, 03, 04, 09)**

    University policy requires that all university-owned devices and those containing PII be encrypted. No PII is to be stored on unencrypted portable/removable devices. Only approved Cloud media can be used to store University data. All data, regardless of their classifications, must be encrypted.

22. **Monitoring to alert on the occurrence of unauthorized access (Controls: 01, 02, 04, 06, 08, 12)**

    Internal and external monitoring for unauthorized access is applied to systems where it is technically, operationally, and financially feasible. Monitoring objectives guide the granularity of each tool and technique used ((e.g., intrusion detection systems, intrusion prevention systems, scanning tools, audit record monitoring software, network monitoring software, etc.), as well as the capability of information systems to support such objectives.

23. **Firewalls and operating system security patches (Controls: 02, 04, 07, 08, 12, 13, 16)**

    The University uses access control lists, firewalls, intrusion prevention, and other undisclosed tools at the network and system levels. Vulnerability scanning tools and patch management software must be installed on all systems, servers, and endpoints. All University-owned and managed devices are automatically patched, or where the unmanaged application of a patch may disrupt operations, patches may be applied manually.

24. **System security agent software (Controls: 01, 02, 04, 09, 10, 16)**

    Hard drives must be encrypted, and anti-malware software, vulnerability management agents, and patch management agents must be installed on all University managed computers and systems as baseline configuration requirements.

25. **Manage the security life cycle of in-house developed and acquired software to prevent, detect, and correct security weaknesses. (Controls: 02, 04, 16, 18)**

    All University acquired application software are scanned to determine continual vendor support, updated to current versions, and relevant patches applied. Web applications are tested for vulnerabilities with web application scanners before deployment, and databases are developed and maintained using standard hardening procedures.

Signature Page

APPROVED BY:

DocuSigned by:
Raymond Lefebvre
66E15F772702474...

5/5/2023

Raymond Lefebvre — Date
Vice Chancellor and Chief Information Officer

APPROVED BY:

DocuSigned by:
Wil Khouri
668B0E1CFA4640D...

5/5/2023

Wil Khouri — Date
Assistant Vice Chancellor and Chief Information Security Officer