UMASS

Written Information Security Program (WISP)

EXECUTIVE SUMMARY

This document details the UMASS 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 UMASS security approach is documented in the Written Information Security Program (WISP). The WISP is based on the principal of implementing controls in layers. The objective is to enable university businesses, students, employees, faculty, partners and customers to conduct research or business, exchange information and ideas in a secure environment where risk is carefully managed and protection of assets is both comprehensive and pervasive.

The WISP is based on the National Institute of Science and Technology (NIST) Cybersecurity Framework (The Framework), which was published on February 12, 2014 as a how-to-guide for public and private sector critical infrastructure organizations to enhance their cybersecurity. The goal is consistent delivery across all campuses and the President's Office. Adoption of the WISP ensures that the university implements and maintains effective information security controls that safeguard valuable university assets (information, people and identities, applications and infrastructure).

Larry Wilson
Information Security Officer
UMASS President's Office

August, 2015

TABLE OF CONTENTS

VERSION CONTROL

1. Approvals and Signatures

The Written Information Security Plan (WISP) and University of Massachusetts Information Security Policy (T10-089) is established to protect the assets and interests of the University, to increase overall information security awareness and to ensure a coordinated approach for designing, implementing, managing and maintaining a comprehensive controls environment based on industry best practices. This policy sets the direction for protecting information and IT resources owned and used by the University of Maassachusetts, its employees, subsidiaries, affiliates, service providers and customers.

I have read the University Security Policy (BOT T10-089) included on page 11, and this Written Information Security Plan (WISP) and approve of the contents as documented:

Name	Campus	Date	Signature
Jayshree Krishnamoorthy	UMASS Boston	September 1, 2015	
Brian Sullivan	UMASS Dartmouth	September 1, 2015	
James Packard	UMASS Lowell	September 1, 2015	
Brian Coleman	UMASS Worcester	September 1, 2015	
Lawrence Wilson	UMASS President's Office	September 1, 2015	

2. The UMASS Security Program Goals and Objectives

The overall objective of the University of Massachusetts Written information Security Program (WISP) is to protect university assets against unauthorized access and modification. The UMASS security program has the following key goals:

1. Develop and communicate a comprehensive security framework and strategic programs under the WISP framework:
   - Establish a University of Massachusetts Information Security Policy (approved by the Board of Trustees)
   - Comply with Massachusetts General Law Chapter 93H and its regulations 201 CMR 17.00 for a written information security program
   - Meet business, technical , operational, educational, research and regulatory requirements of the University
   - Protect from threats against information and IT resources, based on the security principle of defense in depth

2. Align the University Security Program with industry leading practices (the NIST Cybersecurity Framework)

3. Manage security throughout its lifecycle.

4. Integrate security and compliance into "normal" operations.

5. Identify and assign / acquire appropriate resources and investments (tools, technology, training, staffing), to implement and maintain the security programs at the campuses and president's office.

6. Develop a WISP implementation roadmap for the University inclusive of all campuses and departments. Review and receive approval from the Information Technology Leadership Council (ITLC) for implementing security programs across all campuses and the president's office based on the WISP roadmap.

7. Develop and implement a comprehensive communication plan designed to increase general awareness and educate/ advise key stakeholders of the security policy, WISP components, key program deliverables, and WISP implementation roadmap.

8. Conduct audits and reviews (both internal and external) to assess the overall security posture of University assets including networks, systems, applications, information, etc.

Disclaimer: Although it is widely acknowledged by industry security experts that the risk of security incidents and/or data breaches cannot be totally eliminated, the likelihood of occurrence, the exposure, and resulting impact can be controlled.

3. The University Security Policy (Doc T10-089)

The UMASS security policy is as follows:

Doc. T10-089
Passed by the BoT
12/8/10

UNIVERSITY OF MASSACHUSETTS INFORMATION SECURITY POLICY

Purpose, Scope, and Applicability:
Information is a critical asset of the University of Massachusetts and protecting information assets and their related processing systems is the primary goal of the University of Massachusetts Information Security Policy Statement. All information created or used in support of the University of Massachusetts business is considered university information. University information will be protected from accidental, malicious or unauthorized disclosure, misuse, modification, destruction, loss and/or damage.

By identifying and monitoring security risks and mitigating the risks through the implementation of information security controls, the security environment at the university is enhanced and trust is established between the university and our customers and regulators.

Policy Statement & Security Controls:
This policy statement is established to protect the assets and interests of the University, to increase overall information security awareness and to ensure a coordinated approach for implementing, managing and maintaining a control environment based on industry best practices. This policy statement sets the direction for protecting information and IT resources owned and used by the University of Massachusetts, its employees, subsidiaries, affiliates, service providers and customers.

This policy stipulates putting forth security controls that are based on an information security standard and framework published by the ISO (International Organization for Standardization)/IEC (International Electro-technical Commission) 27002. This internationally recognized set of security standards addresses various security requirements including risk assessment and treatment, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, incident management, business continuity and compliance.

Information security controls are to be developed and published to ensure university information is adequately protected. These controls are to be reviewed and updated as needed to ensure continued compliance with industry best practices and regulatory requirements. The information security controls apply to all departments, data processing platforms and systems owned, leased or managed by the University of Massachusetts or by third party providers.

UMASS Information Security Governance:
The University of Massachusetts Information Security Policy Statement is approved by the Board of Trustees. The policy statement sets the direction for information security at UMASS.

The President shall develop and issue guidelines for campuses to follow in the implementation of this policy.

Additional details are included in the UMASS Written Information Security Plan (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 WISP is managed by the UMASS Information Security Council (ISC) at the direction of the Information Technology Leadership Council (ITLC)

4. The Massachusetts Privacy Law and Regulations

The Massachusetts General Law Chapter 93H and its regulations 201 CMR 17.00 require that any companies or persons who store or use personal information (PI) about a Massachusetts resident develop a written, regularly audited plan to protect personal information. Both electronic and paper records need to comply with the law. The regulations went into effect on March 1, 2010.

Key deliverables of 201 CMR 17 includes:

- **Purpose** - This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

- **Scope** - The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

- **Definitions: Personal information** - a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

- **Duty to Protect and Standards for Protecting Personal Information** - Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:
    a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;
    b) the amount of resources available to such person;
    c) the amount of stored data;
    d) and, the need for security and confidentiality of both consumer and employee information.

The safeguards contained in the security program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

The Office of Consumer Affairs and Business Regulation compiled a checklist to help businesses comply with 201 CMR 17.00.
The Office of Consumer Affairs and Business Regulation has compiled this checklist to help businesses in their effort to comply with 201 CMR 17.00. This Checklist is not a substitute for compliance with 201 CMR 17.00. Rather, it is designed as a useful tool to aid in the development of a written information security program for a small business or individual that handles "personal information." Each item, presented in question form, highlights a feature of 201 CMR 17.00 that will require proactive attention in order for a plan to be compliant.

5. 201 CMR 17.00 Compliance Checklist

The Comprehensive Written Information Security Program (WISP)

- ☐ Do you have a comprehensive, written information security program ("WISP") applicable to all records containing personal information about a resident of the Commonwealth of Massachusetts ("PI")?
- ☐ Does the WISP include administrative, technical, and physical safeguards for PI protection?
- ☐ Have you designated one or more employees to maintain and supervise WISP implementation and performance?
- ☐ Have you identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices that contain personal information?
- ☐ Have you chosen, as an alternative, to treat all your records as if they all contained PI?
- ☐ Have you identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PI?
- ☐ Have you evaluated the effectiveness of current safeguards?
- ☐ Does the WISP include regular ongoing employee training, and procedures for monitoring employee compliance?
- ☐ Does the WISP include disciplinary measures for violators?
- ☐ Does the WISP include policies and procedures for when and how records containing PI should be kept, accessed or transported off your business premises?
- ☐ Does the WISP provide for immediately blocking terminated employees" physical and electronic access to PI records (including deactivating their passwords and user names)?
- ☐ Have you taken reasonable steps to select and retain a third-party service provider that is capable of maintaining appropriate security measures consistent with 201 CMR 17.00?
- ☐ Have you required such third-party service provider by contract to implement and maintain such appropriate security measures?
- ☐ Is the amount of PI that you have collected limited to the amount reasonably necessary to accomplish your legitimate business purposes, or to comply with state or federal regulations?
- ☐ Is the length of time that you are storing records containing PI limited to the time reasonably necessary to accomplish your legitimate business purpose or to comply with state or federal regulations?
- ☐ Is access to PI records limited to those persons who have a „need to know" in connection with your legitimate business purpose, or in order to comply with state or federal regulations?
- ☐ In your WISP, have you specified the manner in which physical access to PI records is to be restricted?
- ☐ Have you stored your records and data containing PI in locked facilities, storage areas or containers?
- ☐ Have you instituted a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and for upgrading it as necessary?
- ☐ Are your security measures reviewed at least annually, or whenever there is a material change in business practices that may affect the security or integrity of PI records?
- ☐ Do you have in place a procedure for documenting any actions taken in connection with any breach of security; and does that procedure require post-incident review of events and actions taken to improve security?

Additional Requirements for Electronic Records

Do you have in place secure authentication protocols that provide for:

- ☐ Control of user IDs and other identifiers?
- ☐ A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)?
  - Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect?
  - Restricting access to PI to active users and active user accounts?
  - Blocking access after multiple unsuccessful attempts to gain access?
- ☐ Do you have secure access control measures that restrict access, on a need-to-know basis, to PI records and files?
- ☐ Do you assign unique identifications plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls?
- ☐ Do you, to the extent technically feasible, encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted wirelessly?
- ☐ Do you, to the extent technically feasible, encrypt all PI stored on laptops or other portable devices?
- ☐ Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to PI?
- ☐ On any system that is connected to the Internet, do you have reasonably up-to-date firewall protection for files containing PI; and operating system security patches to maintain the integrity of the PI?
- ☐ Do you have reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security patches and virus definitions?
- ☐ Do you have in place training for employees on the proper use of your computer security system, and the importance of PI security?

6. The NIST Cybersecurity Framework

In 2013, US President Obama issued Executive Order (EO) 13636, Improving Critical Infrastructure Security. The EO called for the development of a voluntary risk-based cybersecurity framework (called the Framework) that is "prioritized, flexible, repeatable, performance-based, and cost-effective". The Framework was developed through an international partnership of small and large organizations, including owners and operators of the nation's critical infrastructure, with leadership by the National Institute of Standards and Technology (NIST). The Framework provides a risk-based approach that enables rapid success and steps to increasingly improve cybersecurity maturity.

The University has adopted the NIST Framework for Improving Critical Infrastructure Cybersecurity as the basis of the Written Information Security Program (WISP). The Framework includes a set of guidelines and practices created by the US National Institute of Standards and Technology (NIST), provides government and non-government organizations with a vital *first step* toward managing cyber-security risk. Moving forward, organizations need solutions that not only satisfy the NIST Cybersecurity Framework at the time of deployment but that also enable continued security as threats and business needs change and evolve. The Framework was originally intended to support critical infrastructure providers, but is applicable to any organization that wishes to better manage cybersecurity risk, including higher education institutions.

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.

The *Framework Core* is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example informative References such as existing standards, guidelines, and practices for each Subcategory.

Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

A *Framework Profile* ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

7. How to Use the Framework

The Framework provides a guide to help organizations understand, communicate and manage their cyber risks. In addition, the Framework provides a mechanism for gathering and organizing existing global cyber security standards and best practices. For organizations that do not know where to start, the Framework provides a roadmap. For organizations with more advanced cybersecurity, the Framework offers a way to better communicate with their CEOs and with suppliers about management of cyber risks. Each of the Framework components reinforces the connection between business drivers and cybersecurity activities. The Framework also offers guidance regarding privacy and civil liberties considerations that may result from cybersecurity efforts

The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

8. The University Sub-Committee on Information Security

Directive

The Sub-Committee on Information Security (SCIS) serves as a system-wide advisory group for UMass information security and related compliance programs. The SCIS directly supports the information Technology Leadership Council (ITLC) mission of ensuring that appropriate and cost-effective information protection measures are applied to UMass information and IT assets.

The SCIS, working in close partnership with university and campus stakeholders, performs the following functions:

1) Provides guidance and support to the UMass information security program.
2) Provides regular status reports to the ITLC on the overall status of the university information security program; advises the ITLC of emerging information security, and provides the ITLC with risk management options and recommendations.
3) Ensures that the effectiveness of the university's information security program is continuously monitored and evaluated in terms of: security controls, incident management, security awareness, security risk management
4) Ensures coordination and information sharing among the respective campuses responsible for implementing and managing the university information security program.
5) Engages as a team when a wide-spread information security incident or threat surfaces.
6) Advises on priorities for information security and related compliance projects and initiatives, with program approval provided by the ITLC.
7) Coordinates post-implementation reviews, with an assessment of actual vs. expected outcomes and returns on security investments.

Reporting Channels/Procedures

The SCIS reports to the Information Technology Leadership Council, with a rotational SCIS chair serving as the liaison to the ITLC.

SCIS Leadership

The chairperson of the SCIS shall be appointed by the ITLC and shall serve three consecutive months, then rotate to another SCIS member. A second member will act as the scribe and record notes and actions.

Membership

Membership on the Sub-Committee on Information Security shall be determined by the ITLC. The ITLC shall periodically review the SCIS's membership and make adjustments as necessary. Membership shall include one voting representative from each of the campuses and the President's Office:

- UMass Amherst Information Security Officer
- UMass Dartmouth Information Security Officer
- UMass Medical Information Security Officer
- UMass Boston Information Security Officer
- UMass Lowell Information Security Officer
- UMass President's Office Information Security Officer

Meeting Frequency

The SCIS shall meet monthly by video conference for sessions lasting no more than 90 minutes.

Sub-Committee Minutes

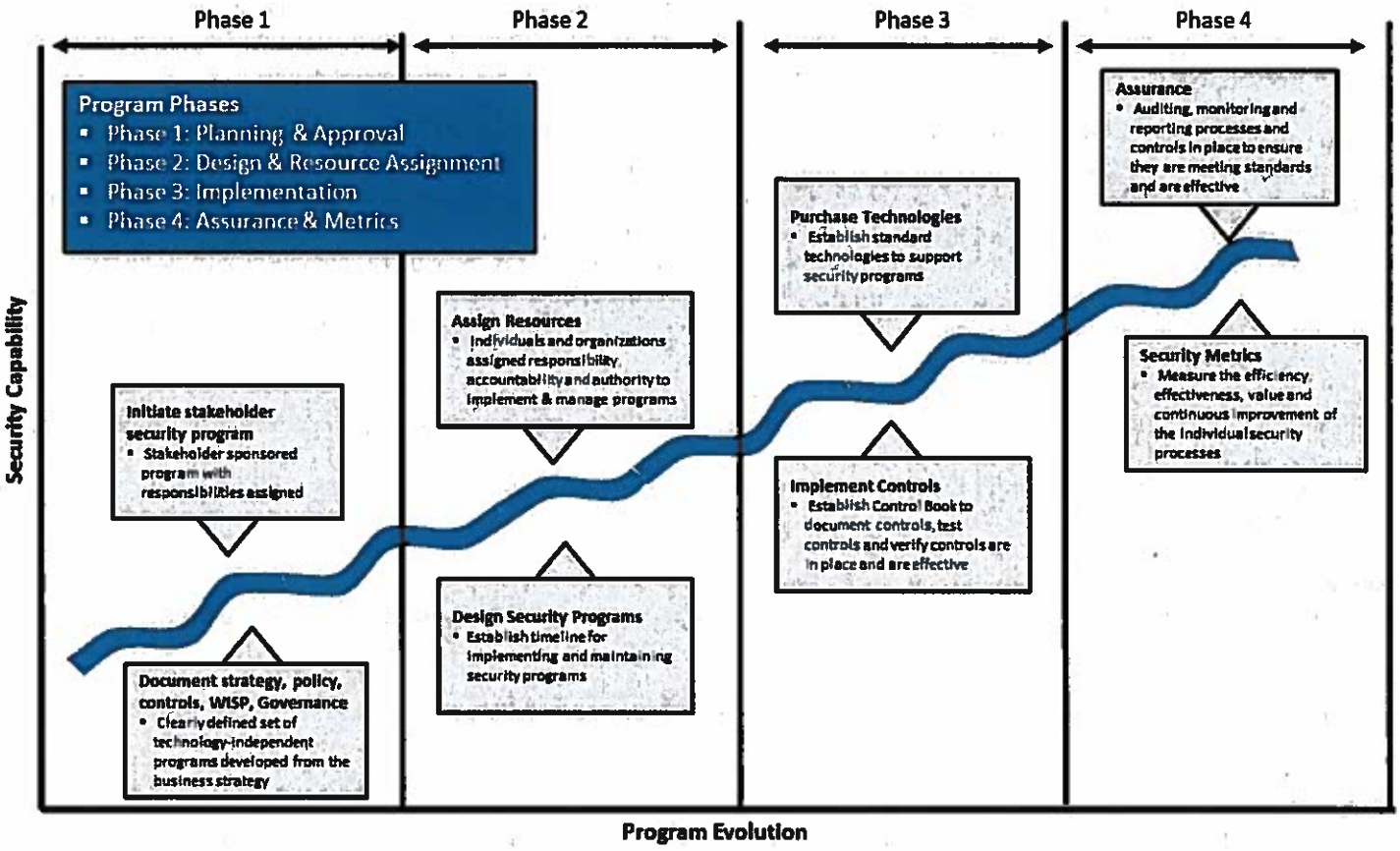
Sub-committee actions will be tracked on Action Tracker and be available to the ITLC.

Sub-Committee Reports

The SCIS Chair will submit a written progress report each month to the ITLC, following the guidelines of the ITLC status report.

9. The University Security Program Roadmap

The following diagram outlines the University information Security Roadmap:



Phase 1: Planning and approval

- Initiate stakeholder program: Identify key stakeholders and establish program deliverables, teams, reporting structure
- Document strategy, policy, controls, WISP, governance: Establish key program-level documentation

Phase 2: Design and resource assignment

- Assign resources: Assign campus resources and document roles / responsibilities
- Design security programs: Develop standards and procedures for each security program based on ISO 27002 controls

Phase 3: Implementation and operations

- Purchase technologies: Select technologies that prevent threats / vulnerabilities or detect and mitigate attacks
- Implement and manage controls: Implement and manage technical, operational and management controls

Phase 4: Assurance and metrics

- Assurance: Develop security scorecard to measure the existence and effectiveness of programs and controls
- Metrics: Develop security metrics to measure effectiveness of technologies that mitigate threats and vulnerabilities

Appendix 1 - The Critical Security Controls

Control	Control Area	Deliverables
CSC 1.0	Inventory of Authorized and Unauthorized Devices	• Maintain an asset inventory of all systems connected to the network • Ensure inventory tools are operational and continuously monitoring • Identify critical information and map information to hardware assets
CSC 2.0	Inventory of Authorized and Unauthorized Software	• Devise a list of authorized software for each type of system • Monitor for unauthorized software installed on each machine
CSC 3.0	Secure Configurations for Laptops, Workstations, Servers	• Create secure image as baseline to build new systems that are deployed • Document security settings that are tested before deployment • Run the last version of software and make sure it is fully patched
CSC 4.0	Continuous Vulnerability Assessment and Remediation	• Run automated vulnerability scanning against all networked systems • Deploy automated patch management for operating system software • Chart unmitigated, critical vulnerabilities for each department/division
CSC 5.0	Malware Defenses	• Employ anti-malware software and signature auto update on a daily basis • Configure systems for automated anti-malware scan of removable media
CSC 6.0	Application Software Security	• Deploy web application firewalls for application attacks • Test in-house & 3rd party software for coding errors & malware insertion • Conduct configuration review of operating system and database software
CSC 7.0	Wireless Device Control	• All wireless devices on the network must match authorized configuration • Wireless intrusion detection systems to identify rogue wireless devices • Ensure wireless networks use authentication protocols such as EAP/TLS
CSC 8.0	Data Recovery Capability	• Ensure each system is automatically backed up on as needed basis • Test backup media on a regular basis by performing data restoration process
CSC 9.0	Security Training	• Develop security awareness training for various personnel job descriptions • Metrics should be created for all policies and measured on a regular basis
CSC 10.0	Secure Configurations for Network Devices (Firewalls, Routers, Switches	• Compare firewall, router, switch configuration against standards • At network connection points, implement ingress and egress filtering • Limit ports and protocols with an explicit and documented business need
CSC 11.0	Control of Network Ports, Protocols, Services	• Host-based firewalls or port filtering should be applied on end systems • Any server visible from the Internet should be verified or removed • Internal network services should be reviewed quarterly for business use
CSC 12.0	Controlled Use of Administrative Privileges	• Use automated tools to inventory all administrative accounts • Change default passwords to a difficult-to-guess value • Configure systems to issue alert when an account is added or removed
CSC 13.0	Boundary Defense	• Deny communications with known malicious IP addresses (black lists) • Deploy network IDS sensors on Internet and extranet DMZ systems • Separate internal systems from DMZ and extranet systems.
CSC 14.0	Maintenance, Monitoring, analysis of Security Audit Logs	• Validate audit log settings for hardware devices and installed software • Run biweekly reports that identify anomalies in logs
CSC 15.0	Controlled Access Based on Need to Know	• Establish a multi-level data identification/classification scheme • Configure file shares to allow access to only authenticated users • Portable USB drives should be limited or data automatically encrypted
CSC 16.0	Account Monitoring and Control	• Report locked-out accounts, disabled accounts, non-expiring passwords • Establish process for disabling accounts immediately upon termination • Monitor dormant accounts that have not been used for 30 days
CSC 17.0	Data Loss Prevention	• Network monitoring tools should analyze outbound traffic for anomalies • Conduct periodic scans of servers to discover and validate sensitive data • Encrypt data on portable devices and removable media such as USB tokens
CSC 18.0	Incident Response Capability	• Assign job titles and duties for handling incidents to specific individuals • Devise university standards for time required l to report anomalous events • Establish University Computer Security Incident Response Team (CSIRT)
CSC 19.0	Secure Network Engineering	• Network architecture should include DMZ, middleware, private network • Segment the enterprise network into multiple, separate trust zones
CSC 20.0	Penetration Testing and Red Team Exercises	• Conduct regular penetration tests to identify vulnerabilities & attack vectors • Perform red team exercises to test readiness to identify and stop attacks

Appendix 2 – The ISO 27002:2013 Controls

ISO Reference	Control Area	Deliverables
ISO 5.1	Information Security Policy & WISP	• Document, publish, communicate Information Security Policy (T10-089), WISP
ISO 6.1	Information Security Governance (Internal)	• Information Security Operations Center (ISOC) • Information Technology Leadership Council (ITLC): Leadership &oversight • Information Security Council (ISC): Security programs, standards, controls
ISO 6.2	Mobile devices and teleworking	• Manage the risks introduced by using mobile devices. • Protect information accessed, processed or stored at teleworking sites.
ISO 7.1	HR Security: Prior to Employment	• Roles and Responsibilities: Human Resources to develop job descriptions • Screening: T10-088 Policy on Employee Background Reviews • Terms and Conditions: Personnel Policy for Non-Unit Staff (T94-023)
ISO 7.2	HR Security: During Employment	• Management Responsibilities: Information Security Policy and WISP • Information Security Awareness, Education and Training • Disciplinary Process: Include in Acceptable Use Standard &Procedure
ISO 7.3	HR Security: Termination of Employment	• Management Responsibilities: include security and legal responsibilities • Return of Equipment: Return all software, documents, and equipment • Removal of Access Rights: Employees, contractors and third party users
ISO 8.1	Responsibility for assets – ownership	• Maintain an asset inventory of all systems connected to the network • Ensure inventory tools are operational and continuously monitoring • Identify critical information and map information to hardware assets • Identify asset owner and map to asset inventory • Devise a list of authorized software for each type of system • Monitor for unauthorized software installed on each machine
ISO 8.2	Information classification	• Classification of assets (identities, infrastructure, applications, information) • Classify information in terms of its value, sensitivity, and criticality • Develop procedures for information labeling and handling
ISO 8.3	Media Handling	• Management of removable media in accordance with classification scheme • Media should be disposed of securely when no longer required • Media should be protected against unauthorized access, misuse or corruption during transportation.
ISO 9.1	Business requirements for access controls	• Document university access control standards and procedures
ISO 9.2	User access management	• Document & implement user registration and de-registration procedure • Control allocation of passwords through a formal management process • Establish procedures to review users' access rights at regular intervals
ISO 9.3	User responsibilities	• Advise users to follow best practices in the selection and use of passwords • Users ensure that unattended equipment has appropriate protection • Establish clear desk policy and clear screen policy
ISO 9.4	System and application access controls	• Access to operating systems are controlled by a secure log-on procedure • Password management systems are interactive & ensure quality passwords • Utility programs that override system controls are restricted and controlled • Restrict access to information and applications by users and support staff • Create dedicated (isolated) computing environment for sensitive systems
ISO 10.1	Cryptography	• A policy on the use of cryptographic controls for protection of information • Key management should be in place to support the cryptographic techniques.
ISO 11.1	Physical security for perimeter, offices and secure areas	• Protect areas that contain IT resources &information • Control access to secure areas, offices, rooms, and facilities
ISO 11.2	Equipment Protection	• Locate equipment to protect against environmental threats and hazards • Protect equipment from power failures and utility failures • Protect cabling carrying data or IT services from interception or damage

Appendix 2 – The ISO 27002:2013 Controls (Continued)

ISO Reference	Control Area	Deliverables
ISO 12.1	Operational procedures and responsibilities	• Ensure operating procedures are documented for those who need them • Segregate duties to reduce unauthorized or unintentional modification • Segregate dev, test, prod to reduce risk of unauthorized access or change
ISO 12.2	Protection against malware	• Employ anti-malware software and signature auto update on a daily basis • Configure systems for automated anti-malware scan of removable media
ISO 12.3	Back-up	• Ensure each system is automatically backed up on as needed basis • Test backup media on a regular basis by performing data restoration process
ISO 12.4	Logging & Monitoring	• Validate audit log settings for hardware devices and installed software • Run biweekly reports that identify anomalies in logs
ISO 12.5	Control of Operational Software	• Procedures to control the installation of software on operational systems.
ISO 12.6	Technical Vulnerability Management	• Run automated vulnerability scanning against all networked systems • Deploy automated patch management for operating system software • Chart unmitigated, critical vulnerabilities for each department/division
ISO 12.7	Information Systems Audit capabilities	• Audit requirements and activities involving verification of operational systems should be planned and agreed to minimize disruptions to business processes.
ISO 13.1	Network security management	• Networks should be managed and controlled to be protected from threats. • Security features, service levels, and management requirements of network services. • Groups of information services, users and information systems should be segregated.
ISO 13.2	Information transfer	• Controls to protect transfer of information through communication facilities. • Agreements for information transfer between the organization and external parties. • Information involved in electronic messaging should be appropriately protected. • Confidentiality or non-disclosure agreements for the protection of information.
ISO 13.3	Third party service delivery management	• Security controls, service definitions in third party service agreements • Monitor and review services, reports & records provided by third party • Manage changes to services, security policies, procedures and control
ISO 14.1	Security requirements of information systems	• Controls reflect business value of the information assets • Security is integrated in the early stages of information system projects • If products are purchased, a testing and acquisition process is followed
ISO 14.2	Security in development and support processes	• Formal change control procedures should be documented and enforced • Control information leakage by scanning media and communications • Outsourced software development include licensing arrangements, etc.
ISO 14.3	Test data	• Test data should be selected carefully, protected and controlled
ISO 15.1	Information Security in Supplier Relationships	• Requirements for mitigating risks of supplier access to organization's assets. • Agreements with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. • Requirements to address the information security risks associated with information and communications technology services and product supply chain
ISO 15.2	Supplier service delivery management	• Organizations should regularly monitor, review and audit supplier service delivery. • Changes to the provision of services by suppliers should be managed .
ISO 16.1	Management of Security Incidents and Improvements	• Assign job titles and duties for handling incidents to specific individuals • Devise university standards for time required l to report anomalous events • Establish University Computer Security Incident Response Team (CSIRT)
ISO 17.1	Information Security Continuity	• A managed process should be developed for business continuity • Plans developed and implemented to maintain or restore operations • Business continuity plans should be tested and updated regularly
ISO 17.1	Redundancies	• Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.
ISO 18.1	Compliance with legal requirements	• All regulatory and contractual requirements are explicitly defined • Appropriate procedures to ensure compliance intellectual property rights • Important records protected from loss, destruction, and falsification
ISO 18.2	Information security reviews	• Audit activities planned to minimize risk of disruption to business processes • Access to audit tools protected to prevent possible misuse or compromise

Appendix 3 –Reference Documents

- 201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH
- NiST Framework for Improving Critical Infrastructure Cybersecurity, February, 2014
- ISACA White Paper: Implementing the NIST Cybersecurity Framework, 2014
- PWC White Paper: Why you should adopt the NiST Cybersecurity Framework, May 2014
- intel White Paper: US Executive Order 13636 and Critical Security Capabilities to Consider, March 2014
- IBM White Paper: Applying IBM Security solutions to the NiST Cybersecurity Framework, August 2014