



**Information Technology Services
Information Security Office**

100 Morrissey Boulevard, Boston, MA 02125

UMass Boston Information Security Policies

January 19, 2022



V.1.8



Table of Contents

Section	Page Number
Section One: Information Technology Acceptable Use Policy (AUP)	3
Section Two: Incident Response Policy	12
Section Three: Firewall Change Management Policy (FCMP)	16
Section Four: Change Management Policy (CMP)	25
Section Five: Information Security Training and Awareness Policy	32
Section Six: Information Security Risk Management Policy (ISRMP)	38
Section Seven: Vulnerability Scanning, Vulnerability Management, and Pen-Testing Policy (VMPP)	57

Section One: Information Technology Acceptable Use Policy (AUP)

I. POLICY STATEMENT

It is the University of Massachusetts Boston (The University) policy to encourage widespread access and distribution of public data and information. To that end, The University provides access for its community to local, national, and international sources of information and provides an atmosphere that encourages the free exchange of ideas and sharing of information. Access to the University's information technology resources is a privilege that imposes certain responsibilities and obligations on users. The University expects all members of the community to use computing, data, and information technology resources responsibly. Access and use of these resources is subject to the University's policies and procedures, and local, state, and federal laws

It is the responsibility of every user of information resources to understand the Information Security Policies and the acceptable use of information and technology resources and conduct their activities accordingly.

Failure to comply with the appropriate use of these resources threatens the atmosphere for sharing information, the free exchange of ideas, and the secure environment for information technology resources. Individuals in violation of this policy may be subject to disciplinary proceedings and/or legal action.

II. PURPOSE

This policy outlines the acceptable use of information technology resources at the University and promotes the efficient, ethical, and lawful use of the University's information technology resources. This policy serves to put individuals on notice of their obligations to comply with all existing state and federal laws and institutional policies in their use of the University's information technology resources. Individuals using the University's information technology resources may include; but is not limited to employees, agents, contractors, consultants, temporary staff, and other staff such as visiting scholars, at The University, including all staff and affiliated personnel via third-party contractors.

The purpose of this policy is to protect employees, students, partners, and The University against internal and/or external exposure of confidential information, exposure to malicious activity, including the compromise of systems and services, legal issues, financial loss, and damage to reputation by individuals, either knowingly or unknowingly. Accordingly, The University has an obligation to protect the integrity of information technology resources, all users' rights, and The University's property at its sole discretion. **The University thus reserves the right to examine material stored on or transmitted through its resources (i.e., networks, storage media) for any business purpose, including, without limitation, where there is a cause to believe that the standards for acceptable and ethical use are violated by a member of its community or an unauthorized user of its systems or networks.** The University reserves the right at any time, with or without prior notice or permission from the user or users of a computer or other University-owned computing device, to monitor, to seize such device and/or copy or have copied and/or wipe or have wiped, any and all information from the data storage mechanisms of such device as may be



required at the sole discretion of the University. In addition to the preceding, privately owned devices connected to the University network or used for University business are also subject to inspection and/or monitoring by authorized University personnel. All users should bear in mind that public records laws and regulations may result in information and communications on University devices (and University information stored on personal devices) being considered public records, including but not limited to personal communications made on University devices (and personal devices used for business purposes). Consequently, personal devices should not be used for official University business unless a department head provides prior written approval to the Information Security Office and the equipment meets specific University security requirements.

Information Disclaimer: Individuals using online or on-premise computer systems and applications owned and managed by The University are subject to applicable state and federal laws and The University’s policies. The University disclaims any responsibility and/or warranties for information and materials residing on non-University systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of the Commonwealth of Massachusetts, The University, its faculty, employees, staff, or students.

I have read and herein agree to abide by the entire content of this Acceptable Use Policy and all related policies/guidelines/standards referenced. I recognize my overall responsibility to exercise the degree of care required to maintain control of University computing systems and resources (e.g., data, software, hardware, network components, and other digital assets) and agree to abide by established University policies/guidelines/standards and procedures. I acknowledge that failure to comply with the University Acceptable Use Policy as well as other related policies, guidelines, standards, or procedures may result in the loss or restriction of my computer access; reprimand, suspension, dismissal, other disciplinary, or legal action.	
Print Name:	
Signature:	Date:

III. SCOPE

This policy applies to all information technology resources, including personally-owned devices used for work-related purposes, and to each user of these resources. The user community consists of those persons and organizations which use, directly or indirectly, any of these resources.

University information technology resources include but are not limited to the following:

1. Endpoints (Approved use of personal computers, laptops, tablets, and other mobile devices).
2. Infrastructure (Networks, core systems, storage media, and servers).



3. Applications (Electronic mail, database applications, and software).
4. Physical (Computer labs, data centers, and kiosks).
5. Data (Internet, Intranet, Cloud, Off and On-premises Data).

Information technology resources must be used for University business and education-related purposes and activities, and must not be used for illegal or inappropriate activities, including, but not limited to, the following:

1. Unwarranted use of network bandwidth and resources.
2. Fraudulent or personal advantage.
3. Commercial gain.
4. To violate academic integrity, such as selling papers or other coursework.
5. To disclose confidential information concerning another employee or student at the University without that individual's prior written consent.
6. Any use that damages, harasses, intimidates, or harms a person.
7. Any use that intentionally interferes with the University's business operations or any other organization.
8. Distribution or storage of illegal adult content.
9. To violate copyright laws, including the distribution, sharing, or retention of copyright-protected music, movies, games, ebooks, and software acquired illegally.
10. Any use that would violate University policy, including but not limited to hacking, cracking, or intentionally accessing computer resources without authorization.

IV. GENERAL USE

Acceptable and Ethical Use:

1. Complete all privacy and security training required for your position in a timely manner: [Information Security Training and Awareness Policy](#).
2. Safeguard user accounts and passwords and use them only as authorized. Use file sharing and account delegation tools rather than sharing a password.
3. Conduct all communications responsibly. This includes safeguarding the integrity and confidentiality of The University's electronic communication (e.g., email, social media, online meetings, etc.).
4. You are responsible for all activities (including physical access) originating from your user ID or your assigned computing device. Access only your own information or publicly available information or to which you have been granted access.
5. It is expected that employees will exercise good judgment regarding the reasonableness of personal use, and any question regarding appropriate use will be decided by management.
6. Use only those computing, data, and information technology resources for which you have authorization and only for their intended purpose.
7. Protect the access to and integrity of computing, data, and information technology resources.



8. As instructed by the University, activate the University Multi-Factor Authentication (MFA) therefore engaging in one additional step beyond the standard login process to access the University's resources and networks by registering a second approved device. The MFA system will send a message to the device, which the individual must use to authenticate. Upon successful completion of the 2-step authentication process, the individual will be able to access the services.
9. Ensure that sensitive data is created, collected, maintained, used, disseminated, and destroyed in a manner that prevents unauthorized use, corruption, disclosure, loss, or theft according to The University's policy, legal, and contractual requirements.
10. Properly create, collect, maintain, access, disseminate and dispose of The University's data, per the data classification policy, to prevent unauthorized use, corruption, disclosure, loss, or theft accordingly to The University's policies, legal and contractual requirements.
11. Abide by applicable laws and The University's policies and respect the contracts and the copyright and intellectual property rights of others, including the legal use of copyrighted software.
12. Respect the privacy and personal rights of others. For example, do not rebroadcast or forward information obtained from another individual that the individual reasonably expects to be confidential, except as required by your job responsibilities, the University's Policies, and applicable laws.
13. Internet use must comply with the Terms of Service stipulated by the Internet service providers and all University policies.
14. Never use The University's resources to engage in any illegal activity.
15. Immediately report compromises and other security incidents to the Information Technology Service Desk, including, but not limited to, the loss or theft of portable/mobile devices.
16. Encrypt data at rest and in transit to comply with The University's policies and applicable state and federal regulations.
17. Use of personally-owned computer equipment to access University resources may be allowed at the discretion of the University. When allowed, such personally owned computer equipment must be set up to meet University standards, including login password, firewall, encryption, and anti-malware.

The following activities are by no means exhaustive but attempt to provide a framework for activities that are **strictly prohibited**:

1. Use of another person's account (unless permitted explicitly via delegation), identity, security devices/tokens, or presentment of false or misleading information or credentials, or unauthorized use of information systems/services.
2. Accessing unauthorized systems or data resources or utilizing functions that are not necessary to perform one's duties.
3. Sharing personal account credentials with anyone. Employees, students, and contractors who receive usernames and passwords must keep their usernames and passwords confidential and not share that information with others.



4. Accessing and/or disclosing confidential, sensitive data, sensitive system or network information except as authorized as part of your duties and according to established standards.
5. Accessing or using data or information unless you are authorized to do so.
6. Disclosure of Personally Identifiable Information (PII) (i.e., social security numbers, bank or credit card numbers, driver's license or ID numbers, etc.) and any other information classified as "confidential," "personal," or "sensitive" to an unauthorized individual within The University without a business need.
7. Accessing, editing, deleting, copying, or forwarding files or communications of another user in any media (e.g., paper, electronic, video, etc.), unless assigned as a job requirement or with prior consent from the file owner.
8. Removing or deleting data (e.g., email), erasing/wiping computers or storage media, or otherwise deleting university documents and information, including from a remote location, unless required for job responsibilities and in a manner consistent with record retention requirements.
9. Using computer programs to decode passwords, access control information, send chain emails, spam, or phishing emails, generating excessive printing and other inappropriate behavior.
10. Using systems to harass, threaten, libel, or defame any person.
11. Attempting to circumvent or subvert system and network security measures.
12. Operating any University system or any system on The University's networks without the use of anti-malware software configured to auto-update.
13. Engaging in any activity that may be purposely harmful to The University's data, systems, or networks.
14. Using The University's systems or networks for commercial or political purposes (unless otherwise specified in the Intellectual Property agreement).
15. Using the University's systems or networks to conduct activities that pose security risks. Sites that offer gambling, adult content, or cryptocurrency often contain malicious content and should be avoided.
16. Illegal using, including duplication or distribution of copyrighted or University proprietary material, including electronic, hardcopy, audio, and video in any medium.
17. Using the University's systems or networks for personal gain, profit, or convenience (unless otherwise specified in the Intellectual Property (IP) agreement).
18. Connecting unauthorized equipment (for example, a personal wireless access point) to the University's network, directly or via remote connection.
19. Procure or use any Software as a Service (SaaS) providers or implement any information technology component, product, or service without the approval and involvement of Information Technology Services.
20. Removing software from systems (i.e., Alertus, Anti-Malware, KACE, Tenable client, etc.) without prior consent from Information Technology is obtained.
21. Abuse highly authorized or administrative privileges to access data or systems unnecessarily or inappropriately.



22. Circumvent any of the information security measures of any host, network, or account without CISO's approval for emergency business purposes.
23. Disclosure of PII to any individual outside of the University unless there is a legal or regulatory requirement.
24. Unencrypted transmission of PII (and confidential, personal and sensitive information), trade secrets, proprietary financial information, and financial account numbers such as in the body of or an attachment to an electronic message, via FTP, via instant messenger, or via fax.
25. Storing confidential information including PII (confidential, personal, and sensitive information), trade secrets, proprietary financial information, or financial account numbers on laptop computers, mobile computing devices, and removable media (i.e., Thumb drive, external hard drive, etc.) unless no alternative exists and then it **must** be encrypted.
26. Under no circumstances may an employee, student, contractor, or consultant disable anti-virus software or alter anti-virus software settings.
27. Under no circumstances may an employee, student, contractor, or consultant disable firewall software or alter firewall software settings.
28. Employees, students, contractors, and consultants should not open any electronic messaging attachments that are not expected or are from unknown addresses, or appear in any way suspicious.
29. Employees, students, contractors, and consultants must not use University accounts to post publicly accessible messages or posts unless authorized.
30. Employees, students, contractors, and consultants may not perform vulnerability scans, monitor network traffic, attempt to elevate rights or privileges or gain access to information not expressly intended for them.
31. Employees, students, contractors, and consultants must be extremely cautious about the use of instant message applications, as these applications are insecure. Employees must not share sensitive information through this medium.

To ensure compliance with this policy, The University may perform periodic monitoring of systems, networks, and associated equipment at any time. Personnel using any University information or technology resources consent to disclosing the contents of any files or information stored or passed through the University's equipment or personal devices used for University business. All data contained on or passing through the University's assets is subject to monitoring and remains The University's property at all times.

V. OTHER PROVISIONS

- Explicit management approval must be provided for the use of IT resources by employees or third parties.
- Explicit management approval is required to add a new device to the network.
- Authentication is required to use any technology.
- Accessing unauthorized systems or data resources or utilizing functions that are not necessary to perform the employee's duties is prohibited.



- A list of all devices and personnel with access shall be maintained at all times.
- Devices will be labeled with the owner, contact information, and purpose.
- A list of acceptable uses of technology and network locations shall be maintained.
- A list of University-approved hardware, software, and Cloud applications shall be maintained.

VI. ENFORCEMENT

Personnel using The University’s information resources in opposition to this policy may be subject to limitations on the use of these resources, suspension of privileges (including Internet access), as well as disciplinary and/or legal action, including termination of employment.

Employees, contractors, consultants, temporary employees, including visiting scholars, and all personnel affiliated via third parties shall sign an agreement to comply and be governed by this policy and The University’s Information Security Policies upon hire.

The University reserves the right to withhold certain services, such as network access if the computer does not meet our requirements. In these cases, ITS may remediate the problem or require the computer’s owner to do so if the equipment is not owned by the University.

If, in working on computer equipment, material is discovered which indicates a possible violation of university policy or state or federal law, ITS staff may forward this information to the appropriate University department or law enforcement agency.

ITS staff may install or remove software or data files at their discretion if they believe it is necessary to remediate a problem and put the device into compliance with said policies.

VII. RESPONSIBILITIES

Role	Responsibility
Staff	Use information resources with good judgment and in compliance with information security policies and report any inappropriate use of information resources to the Information Security Office (ISO).
Management	Ensure that personnel understand and agree with the AUP.
Business Owners	Implement measures to protect their resources and monitor them against inappropriate use.
IT Staff	Help implement security solutions in compliance with this policy and assist business owners in implementing measures to protect their resources against inappropriate use.
Chief Information Security Officer	Maintains the information security program and monitor compliance with the Information Security Policies.



VIII. REFERENCES

Frameworks	Name	Reference
	(CIS) Cybersecurity Controls Framework (V7.1)	CIS 01: Inventory and Control of Hardware Assets; CIS 02: Inventory and Control of Software Assets; CIS 04: Controlled Use of Administrative Privileges; CIS 07: Email and Web Browser Protection; CIS 08: Malware Defenses; CIS 13: Data Protection; CIS 14: Controlled Access Based on the Need to Know; CIS 17: Security Awareness and Training Program;
Regulations and Requirements	PCI, FERPA, GDPR, HIPAA, CCPA, Massachusetts regulations 201 CMR 17.00	
Supporting Standards and Procedures		

IX. VERSION CONTROL (Revisions and dates)

Revision Number	Date	Name	Description
R1	08/14/2019	Wil Khouri	UMB-AUP-ISOPOL04-19-R1
R1	05/31/2021	Wil Khouri	UMB-AUP-ISOPOL04-21-R1
R2	12/10/2021	Wil Khouri	UMB-AUP-ISOPOL04-21-R2
	(Next Rev.) 07/2022-R1		



UMass Boston Information Security Policies v.1.8
January 19, 22, 2020

Wil Khouri

walid khouri

Date Signed

DocuSigned by:
Walid Khouri
668B0E1CFA4540D...

12/9/2021

Raymond Lefebvre

Date Signed

DocuSigned by:
Raymond Lefebvre
66E15F772702474...

12/9/2021

Section Two: Incident Response Policy

PURPOSE

The Purpose of this policy is to define the steps to be followed to respond to information security-related incidents at the University of Massachusetts, Boston. The Incident Response Policy and subordinate procedures as outlined by the "Information Security Incident Response Plan" define standard methods for detection and analysis, containment, eradication/mitigation, recovery and post-incident review of network and computer-based IT Security incidents and events.

SCOPE

Users shall report any suspected information security incidents immediately to the Information Security Office (ISO) including:

- Suspected violations of any information security policies
- Loss or theft of mobile devices (laptops, mobile phones and PDAs), security tokens, or other items that may provide access to company resources
- Attempts by unauthorized external personnel to gain access to university systems
- Accidental disclosure, modification, or destruction of information

Information Security incidents may be explicitly reported or detected as a result of system monitoring. IDS/IPS and file integrity monitoring systems will be configured to generate alerts.

An incident response team will be appointed by the Information Security Officer and will be ready for deployment in case of any regulated data (PCI, PII, PHI) compromise.

POLICY

All reported security incidents shall be responded to in a timely manner.

If a compromise is suspected:

1. Alert the Information Security Officer who will perform an initial investigation and notify the Incident Response Team if necessary.
2. Follow the steps recommended by VISA and MasterCard (and other affected payment card brands) if the compromise involves credit card data.
 - http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html
 - http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf
3. Follow the steps recommended by the PII managing authority (HIPAA, GDPR, FERPA) if the compromise involves other regulated data.

An incident report form must be completed and submitted for each incident.



In response to an information security incident, the Information Security Office in conjunction with the Incident Response Team shall address the following:

- Detection - Corroborate and define the incident.
- Assessment - The incident should be classified based on available information to determine whether Network communications require closure or Business Continuity Plans require implementation.
- Forensics - Data related to the incident shall be gathered and analyzed
- Containment - Measures shall be taken to separate impacted systems from the rest of the university environment.
- Recovery - Systems shall be restored to normal operation as soon as possible and follow policy and procedures for applicable Backup and Recovery, and BCP and DR.

In the event a compromise has been confirmed, the University of Massachusetts, Boston legal department will be consulted to determine the legal requirements for reporting the breach.

The ISO will activate the Information Security Incident Response Plan (ISIRP).

A log must be kept of all the actions taken, including triage steps and other regular or routine work performed on the affected systems. This log should be separate from normal system logs since it may be used as evidence.

Any system that has been compromised by a malware will be removed from the network until the system can be verified as malware-free. Accounts where the password has been compromised will be disabled until the password can be reset and communicated to the account owner. Connections between information systems components may be interrupted in response to an incident as part of the containment process.

Designated Information Technology personnel will be available to respond to security incidents 24/7. Training will be provided to those with incident response responsibilities on an annual basis.

An incident post-mortem must be conducted to determine if changes are needed to security policies and/or procedures and/or configuration settings and documentation. Additionally, the Incident Response Plan will be tested annually. Alerts from US-CERT or some other security monitoring organization will be monitored for potential changes to the Incident Response Plan based on industry developments.

RESPONSIBILITIES

Role	Responsibility
Staff	Report suspected incidents to the Information Security Officer promptly.
Management	Assist with evaluation and mitigation of the incident in conjunction with IT and the Information Security Officer.



Role	Responsibility
Chief Information Security Officer	Reports the incidents to upper management and appropriate external entities. Determines if incident follow-up is needed. Ensures that all incidents and resolution activities are fully documented and tracked. Uses these incidents in training awareness as examples of what could happen, how to respond to such incidents, and how to avoid them in the future.
IT Staff	Respond to information security incidents according to policy and procedures.

REFERENCES

	Name	Reference
Frameworks	(CIS) Cybersecurity Controls Framework (V7.1)	CIS 17: Implement a Security Awareness and Training Program; CIS 19: Incident Response and Management; CIS 20: Penetration Testing and Red Team Exercises;
Regulations and Requirements	PCI, FERPA, GDPR, HIPAA, CCPA, Massachusetts regulations 201 CMR 17.00	
Supporting Standards and Procedures		

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Revision Number	Date	Name	Description
R1	1/20/2020	Wil Khouri	IRP-ISOPOL01-2020-R1



Signature Page

APPROVED BY:

Ray Lefebvre

03/06/2020

Raymond Lefebvre
Vice Chancellor and Chief Information Officer

Date

APPROVED BY:

Wil Khouri

02/07/2020

Wil Khouri
Assistant Vice Chancellor and Chief Information Security Officer

Date

Section Three: Firewall Change Management Policy (FCMP)

I. POLICY STATEMENT

This policy defines the roles and responsibilities of the Information Security Office (ISO) staff with respect to controlling software, hardware, and configuration changes to a firewall and firewall-related appliances (i.e. hardware and/or virtual blades) which may be deployed or applied to the production environment of the UMass Boston technology network, security, server, storage, and database or solutions architecture.

II. PURPOSE

UMass Boston operates a series of perimeter and internal firewalls between the Internet and the university network to establish a secure environment for the university's computer and network resources. In conjunction with effective security policies and administration procedures, this policy governs how firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to the University's network and information systems.

Firewall rules and rule sets are constantly being updated to respond to threats and vulnerabilities, and to facilitate access to legitimate use. The goal is to maximize availability while maintaining the security of the university network. Network Operations relies on UMass Boston's ISO to provide direction on changes and relies upon a robust change control process, case tracking, and timely responses to ensure that goals are met.

The purpose of this policy is to:

- Manage changes to the IT infrastructure to enable ITS staff members as well as clients to plan accordingly.
- Minimize the impact of changes on other tasks/projects.
- Ensure that required security measures are in place on all deployed equipment.
- Promote communication and collaboration regarding change items.
- Inform the ITS Service Desk about infrastructure modifications and impact.
- Minimize the risk and the time of outages.
- Maintain compliance to applicable regulations.

III. SCOPE

This policy applies to all firewall technology changes; which may be deployed or applied to the production environment of the UMass Boston Information Technology and telecommunications network, server, storage, and database or solutions architecture.

UMass Boston is conducive to an open network policy; facilitating centralized, as well as decentralized, users and systems, and to that end the ISO favors a multilayer security approach in most endeavors. As a result, the ISO must position much of its



defenses in close proximity to critical services and data to protect these critical services from internal and external threats. This layered approach does rely heavily on the protection from the redundant border firewalls. Within these layers, the internal traffic is monitored and protected from untrusted sources by the use of internal firewalls which protect critical assets and services.

All IT staff members, consultants, or agents of UMass Boston and any parties who are contractually bound through the Information Technology department to build or support its technology infrastructure are required to abide by this policy.

Out of scope items include cabling infrastructure, lab equipment, or devices solely used for testing, monitoring, or management purposes.

IV. DEFINITIONS

Change Management - The process of requesting, developing, approving, and implementing a planned or unplanned change within the IT infrastructure.

Change Item (or Change Request) - A documented request to modify the IT infrastructure to be completed via a Change Management Request Form.

ITS Infrastructure - the network, server, storage, database and solutions technologies managed by Information Technology Services (ITS).

Routine Change - A change of regular priorities where review of the change request is made during the change meeting and the approval is received prior to the changes being made.

Urgent Change - A change of escalated priorities, where review and approval of the change is received from the Assistant Vice Chancellor / CISO prior to the change being made and is subsequently reviewed, communicated, and closed during the next scheduled change meeting.

Emergency Change - A change of immediate priorities where ISO personnel is required to execute a change without any review or approval (i.e. service outage, system crashes, etc.). An emergency change request is to be reviewed, communicated, and closed during the next scheduled meeting.

V. PROCEDURES

The following section outlines the process for submitting, reviewing, approving, deferring, and closing technology change items.

A. **Submittal of a Change Request:**

Change requests are to be submitted via the IT Change Control Request Form (Appendix A) by the owner of the change. The change should not be initiated until approved according to procedures

defined within this policy. All sections of the change request should be thoroughly completed. The documentation must identify the scope of the change, areas affected, back-out process, communication plan, and planned date of deployment. This to be done at a level to ensure the scope can be accomplished as described and to provide assurance that the change will have the desired result. Once a change request is submitted, it will be known as a change item and is assigned a change number.

Any change items affecting a high-security (PCI-DSS, HIPAA) environment should be noted as such with any additional fields/requirements completed appropriately.

B. Review of New Change Items:

New change items are reviewed during the bi-weekly ISO meeting. The owner of the change is to review each pending change item with the group to ensure that the ISO staff understand the change and its dependencies. Any incomplete requests will be held or deferred until the next bi-weekly meeting.

C. Approval & Deferral of Change Items:

Authorization of a change item occurs after the change is reviewed and depends on the priority of the item as described in the table below.

D. Authorization Table:

Type	Authorization*	Change Timing/Discussion
Routine	As defined by the ISO staff owning the change	Change occurs after consensus approval from the management meeting
Urgent	Received from CISO prior to the change being made	Change occurs prior to the change meeting discussion
Emergency	CISO or designated representative is communicated with after (or as) the change is being made	Change occurs prior to the change meeting discussion

*** Changes affecting a high-security environment require the approval of the Assistant Vice Chancellor / Chief Information Security Officer regardless of the type of change indicated.**

Note: Items that are not approved according to the table above should not be implemented until the review and approval process is followed. Unapproved change items should only remain so for a short period of time (1 or 2 change meetings only). Items that cannot be approved and/or will not be deployed in a reasonable timeframe should be moved to deferred status and reactivated when the change is ready for deployment.

With the exception of emergency changes, all firewall changes will become operational Monday through Thursday during normal business hours. Emergency requests may be authorized and executed on Friday only if approved by the Assistant Vice Chancellor / Chief Information Security Officer. All changes require authorization by the Assistant Vice Chancellor / Chief Information Security Officer. Firewall Routine and Emergency changes are pre-authorized to occur as needed. Changes are reviewed by network and security teams regularly to determine the overall impact to IT services and the network.

i. Routine Changes:

Routine changes are operational maintenance modifications required to manage and maintain devices. These routine changes are pre-authorized, and post reviewed by the Assistant Vice Provost / Information Security Officer to be deployed as needed. Routine changes include:

- a. Software Updates
- b. Device and Resource Management
- c. SNMP Password Changes
- d. Periodic firewall rule “clean up” of old rules

ii. Emergency Changes

Emergency changes are necessary to protect University resources from imminent threats or to restore and maintain service levels. All emergency changes are pre-authorized and post reviewed. The Information Security and Network Operations staff regularly identify and react to network-based security threats. These threats are significant and must be dealt with in a timely manner. Threats include but are not limited to:

- a. Malicious denial-of-service or destruction/disclosure of protected data



- b. Unauthorized access to controlled equipment (routers, etc.)
- c. Malicious and/or unauthorized access to systems, data, and/or processes
- d. Theft or malicious manipulation of data and/or services
- e. Theft or physical damage to the network hardware component
- f. Phishing email responses and/or Malware, Virus, or ransomware attacks

E. Closing a Change Request:

Change items that are previously approved and subsequently deployed are reviewed for closure during the ISO bi-weekly meeting. The owner of the change should be available at the change meeting to discuss the implementation. The review should note the status of the change item execution and any service or infrastructure impacts reported to service owners via email. If the change has performed as desired it may be closed. In the event a change does not perform as expected or causes issues to one or more areas of the production environment, the ISO team will determine if the change should be removed and the production environment returned to its prior stable state. Appropriate action should be noted within the change form and successfully acted upon prior to marking the item as closed.

F. Change Meeting Attendance:

To ensure successful review, approval, implementation, and closure of change items, each impacted core service area manager should be informed before and after the execution of the change.

VI. RISK MANAGEMENT

The ISO will evaluate the risk of opening the firewall to accommodate requests. Where the risk is acceptable, granting of requests will be dependent on network infrastructure limitations and the availability of required resources to implement the request. If the risk associated with a given request is deemed objectionable, then an explanation of the associated risks will be provided to the original requestor and alternative solutions will be explored.

VII. RESPONSIBILITY

The ISO is the responsible organization for implementing the provisions of this policy. The Assistant Vice Chancellor / CISO is the designated point of contact.

VIII. POLICY FOR FIREWALLS



The default policy for all campus firewalls for outbound and inbound Internet traffic is as follows:

- a. Outbound: Allow ALL Internet traffic to hosts and services outside of the University.
- b. Inbound: Block all incoming traffic except what is explicitly permitted to support the mission of the university.
- c. Specific to the PCI network segment only, restrict outbound connections from non-authorized devices.

IX. AUDIT TRACKING AND FIREWALL LOGS

The implementation of a rule-tracking mechanism that provides for change logging is required in order to audit all modifications to firewalls. The audit logs are stored securely with limited access only by authorized personnel. With the exception of the PCI network segment, all logs will be recorded and available for review for at least 120 days. Log files for security events on the PCI network shall be retained for one year.

X. GAP ANALYSIS

An informal gap analysis shall be performed annually to ensure firewall policies are reviewed against industry best practices, specifically when there are documented security changes in the network.

XI. ATTACHMENTS

Change Control Record Form: **Appendix A**

XII. RELATED POLICIES PRODEDURES AND ANNOUNCEMENTS

UMB-CMP-ISOPOL03-20-R1: UMass Boston Change Management Policy

XIII. REFERENCES

	Name	Reference
Frameworks	(CIS) Cybersecurity Controls Framework (V7.1)	CIS 09: Limitation and Control of Network Ports, Protocols, and Services; CIS 11: Configuration for Network Devices, such as Firewalls, Routers and Switches; CIS 14: Controlled Access Based on the Need to Know; CIS 18: Application Software Security.
Regulations and Requirements		
Supporting Standards and Procedures		



XIV. VERSION CONTROL


This section contains comments on any revisions that were made to this document and the date they were made.

Revision Number	Date	Name	Description
R1	07/31/2016	Wil Khouri	UMB-FCMP-ISOPOL02-16-R1
R1	07/31/2018	Wil Khouri	UMB-FCMP-ISOPOL02-18-R1
R1	06/08/2020	Wil Khouri	UMB-FCMP-ISOPOL02-20-R1
	(Next Rev.) 07/2021-R1		



Appendix A

Change Control Record Form

	Information Technology Services (ITS) Information Security Office (ISO)				
	Title	Change Control Record (CCR) Form			
Department	<i>ISO</i>				
Subject	<i>PAN-OS 9.1.1 software update</i>				
Implementation Date	<i>2/12/2020 - 2/13/2020</i>				
Requestor(s)	<i>David Bonczar</i>				
Scope					
Priority	<input type="checkbox"/>	Emergency	Category	<input type="checkbox"/>	Major
	<input type="checkbox"/>	Urgent		<input type="checkbox"/>	Significant
	<input checked="" type="checkbox"/>	Routine		<input checked="" type="checkbox"/>	Minor
Technology	<i>Palo Alto minor release</i>				
Description	<i>After the update firewall needs reboot</i>				
Impact Analysis	1. Impact of the change		<i>One is up while the other is rebooted.</i>		
	2. Risk(s)		<i>Minor</i>		
	3. Risk(s) of not making the change		<i>Security issues</i>		
	4. Backout plan		<i>Revert to previous version</i>		
	5. Impact on disaster recovery plans		<i>N/A</i>		
Communications	<i>Notifying network team</i>				
Approval	Name, Title, and Date		Approved	Not Approved	
			X		



Signature Page

APPROVED BY:

Ray Lefebvre *June 8, 2020*
Raymond Lefebvre Date
Vice Chancellor and Chief Information Officer

APPROVED BY:

Wil Khouri *June 08, 2020*
Wil Khouri Date
Assistant Vice Chancellor and Chief Information Security Officer

Section Four: Change Management Policy (CMP)

I. POLICY STATEMENT

This policy defines the roles and responsibilities of the Information Technology Services (ITS) staff with respect to controlling software, hardware, and configuration changes to infrastructure equipment which may be deployed or applied to the production environment of the UMass Boston technology network, security, server, storage, and database or solutions architecture.

II. PURPOSE

The purpose of this policy is to:

- Manage changes to the IT infrastructure to enable ITS staff members as well as clients to plan accordingly.
- Manage the impact of changes on other tasks/projects.
- Ensure that required security measures are in place on all deployed equipment.
- Promote communication and collaboration regarding change items.
- Inform the ITS Service Desk and stakeholders about infrastructure modifications and impact.
- Manage the risk and the time of outages.
- Maintain compliance with applicable regulations.
- Apply and operate a governance model to support change control.

III. SCOPE

This policy applies to all technology changes which may be deployed or applied to the production environment of the UMass Boston information technology and telecommunications network, server, storage, and database or solutions architecture.

All ITS staff members, consultants, or agents of UMass Boston and any parties who are contractually bound through the Information Technology department to build or supports its technology infrastructure are required to abide by this policy.

Out of scope items include cabling infrastructure, lab equipment, or devices solely used for testing, monitoring, or management purposes.

IV. DEFINITIONS

Change Management:

The process of requesting, developing, approving, and implementing a planned or unplanned change within the IT infrastructure.

Change Control Record (CCR):

January 19, 22, 2020

A documented request to modify the IT infrastructure to be completed via a Change Control Record Form.

CIS Infrastructure:

The network, server, storage, database, and solutions technologies managed by ITS.

Routine Change:

A change of regular priority where a review of the change request is made during the weekly management meeting and the approval is received prior to the change being made.

Urgent Change:

A change of escalated priority where review and approval of the change are received from managers prior to the change being made and is subsequently reviewed, communicated, and closed during the next scheduled weekly management change meeting.

Emergency Change:

A change of immediate priority where IT personnel is required to execute a change without any review or approval (i.e., service outage, system crashes, etc.). An emergency change request is to be reviewed, communicated, and closed during the next scheduled meeting.

V. PROCEDURES

The following outlines the process for submitting, reviewing, approving, deferring, and closing technology change items.

A. **Submittal of a Change Request:**

Change* requests are to be submitted via the Change Control Record (CCR) Form (Appendix A) by the owner of the change*. The change should not be initiated until approved according to procedures defined within this policy. All sections of the change request should be thoroughly completed. The documentation must identify the scope of the change, areas affected, back-out process, communication plan, and planned date of deployment. The change is to be done at a level to ensure the scope as described can be accomplished and to provide assurance that the change will have the desired outcome. Once a change request is submitted, it will be known as a change control record and is assigned a CCR number.

The owner of the change (Requestor) must not approve nor sign his/her request. CCRs must be approved and signed by the direct supervisor or the CISO when appropriate.

****Any change item affecting the high security (PCI-DSS) environment should be noted as such with any additional fields/requirements completed appropriately.***

B. **Review of New Change Items:**

New change items are to be reviewed with the staff during the weekly functional departmental meeting. Change Managers will alert the change management group about a pending change item via email communications **to ensure that teams across department boundaries understand the change and its dependencies.** Any incomplete requests will be held or deferred until the next weekly departmental meeting.

C. Approval & Deferral of Change Items:

Authorization of a change item occurs after the change is reviewed and depends on the priority of the item, as described in the table below.

D. Authorization Table:

Type	Authorization*	Change Timing/Discussion
Routine	As defined by the ITS team owning the change (i.e., Team Leader, Project Manager, Manager, etc.)	Change occurs after consensus approval from the management meeting.
Urgent	Received from Manager prior to the change being made	Change occurs prior to the change meeting discussion
Emergency	None, Manager is communicated with after (or as) the change is being made	Change occurs prior to the change meeting discussion

*** Changes affecting a high-security environment, require the approval of the Assistant Vice Chancellor / Chief Information Security Officer regardless of the type of change indicated.**

Note: Items that are not approved according to the table above should not be implemented until the review and approval process is followed. Unapproved change items should only remain so for a short period (1 or 2 change meetings only). Items that cannot be approved and/or will not be deployed in a reasonable timeframe should be moved to deferred status and reactivated when the change is ready for deployment.

E. Closing a Change Request:

Change items that are previously approved and subsequently implemented are reported as closed by the owner of the change to Change Managers via an email with the CCR form attached. The email should note the change item, execution status, and any service or



infrastructure impacts, if any. If the change has performed as desired, it may be closed. In the event a change does not perform as expected or causes issues to one or more areas of the production environment, the change managers team will determine if the change should be removed and the production environment returned to its former stable state (Back-out Plan). Appropriate action should be noted within the change form and successfully acted upon before marking the item closed.

F. Change Control Record Life Cycle:

To ensure successful review, approval, implementation, and closure of change items, core-Infrastructure-service-area managers should thoroughly examine all submitted CCRs. Change managers must ascertain that the change won't interrupt ongoing work nor be potentially disruptive to the development environments they each manage.

VI. RESPONSIBILITY

ITS is the responsible organization for implementing the provisions of this policy.

The Assistant Vice Chancellor / CISO shares the responsibility with the directors in charge of Infrastructure services, which serve as the point of contact for all infrastructure-related changes.

VII. ATTACHMENTS

Change Control Record Form: **Appendix A**

VIII. RELATED POLICIES PROCEDURES AND ANNOUNCEMENTS

UMB-FCMP-ISOPOL02-20-R1: UMass Boston Firewall Change Management Policy

IX: REFERENCES

	Name	Reference
Frameworks	(CIS) Cybersecurity Controls Framework (V7.1)	CIS 09: Limitation and Control of Network Ports, Protocols, and Services; CIS 11: Configuration for Network Devices, such as Firewalls, Routers, and Switches; CIS 14: Controlled Access Based on the Need to Know; CIS 18: Application Software Security.
Regulations and Requirements		



Supporting Standards and Procedures	
--	--


IX. VERSION CONTROL

This section contains comments on any revisions that were made to this document and the date they were made.

Revision Number	Date	Name	Description
R1	07/31/2016	Wil Khouri	UMB-CMP-ISOPOL03-16-R1
R1	07/31/2018	Wil Khouri	UMB-CMP-ISOPOL03-18-R1
R1	06/08/2020	Wil Khouri	UMB-CMP-ISOPOL03-20-R1
	(Next Rev.) 07/2021-R1		

Appendix A

Change Control Record Form

	Information Technology Services (ITS) Information Security Office (ISO)			
	Title	Change Control Record (CCR) Form		
Department	<i>Network Services</i>			
Subject	<i>C5 Firmware Upgrade</i>			
Implementation Date	<i>2/12/2020 - 2/13/2020</i>			
Requestor(s)	<i>Azadeh Aslani</i>			
Scope	<i>Upgrading the Firmware to the Latest Version</i>			
Priority	Emergency	Category		Major Significant
	Urgent		X	
	X Routine			
Technology	<i>Palo Alto minor release</i>			
Description	<i>Upgrading the Switch Firmware from version 06.81.08.0005 to 06.81.10.0001</i>			
Impact Analysis	1. Impact of the change	<i>Switch Stacks</i>		
	2. Risk(s)	<i>Minor</i>		
	3. Risk(s) of not making the change	<i>Loss of Network</i>		
	4. Back-out plan	<i>Roll Back to the previous iteration</i>		
	5. Impact on disaster recovery plans	<i>N/A</i>		
Communications	<i>Notifying network team</i>			
Approval	Name, Title, and Date	Approved	Not Approved	
		X		



Signature Page

APPROVED BY:

Ray Lefebvre

June 24, 2020

Raymond Lefebvre
Vice-Chancellor and Chief Information Officer

Date

APPROVED BY:

Wil Khouri

June 18, 2020

Wil Khouri
Assistant Vice-Chancellor and Chief Information Security Officer

Date

Section Five: Information Security Training and Awareness Policy

I. PURPOSE

The purpose of this policy is to describe the program to be implemented to maintain an effective and active knowledge transfer of the University of Massachusetts, Boston (the University) information security policies, and provide security awareness training to all the University's Community. Faculty, staff, students, vendors, and contractors (the Community) who have access to the University's information systems must understand how to protect the **confidentiality, integrity, and availability** of information systems. The University of Massachusetts Boston understands that people, not technology, are often the most significant threat to sensitive information.

II. SCOPE

It is the responsibility and policy of the University of Massachusetts Boston to conduct an on-going information security awareness and training program for all faculty, staff, students, vendors, and contractors. The University shall develop and maintain an Information Security Training and Awareness Program (**Appendix A**) to communicate and educate the Community about information security policies and procedures and make them aware of their roles and responsibilities in safeguarding information resources. All faculty, staff, students, vendors, and contractors are responsible for participating in the program, for being knowledgeable about information security policies and practices, and for complying with the procedures and instructions provided in the training.

This policy applies to all University information resources, whether individually controlled or shared, stand-alone, or networked. Resources include networked devices, cloud computing, mobile computing, including mobile devices or device components, personal computers, workstations, and any associated peripherals and software, as well as any hardcopy information.

III. POLICY

The security and stability of the information systems are vital to daily operations. An awareness and training program for the Community is critical to achieving and maintaining a robust information security capability. Information security awareness, training, and education will improve individual behavior and accountability, and reduce the risk of unauthorized activities.

All users shall complete security awareness training and training on information security policies upon hire and subsequently at least annually. Human Resources or the employee's manager is responsible for notifying the Chief Information Security Officer (CISO) and IT Communication of a new hire immediately so that the employee can be trained promptly. Employees shall sign an agreement that they understand the University information security policies and that they shall abide by them. After the training has been conducted, the University of Massachusetts Boston will maintain such



records as it deems appropriate that confirms that an individual received proper training.

The primary purpose of an effective and active information security awareness and training program is to establish and sustain an appropriate level of protection for data and information resources by increasing users' awareness of their information security responsibilities. Specific objectives include:

- Improving awareness of the need to protect information resources.
- Ensuring that users clearly understand their responsibilities for protecting information resources.
- Ensuring that users are knowledgeable about the University's information security policies and practices and develop skills and knowledge so they can perform their jobs securely.
- Ensuring that users understand the laws governing data privacy and regulated data such as FERPA, HIPAA, GDPR, etc.

Training may be delivered by various means (**Appendix A**) in person or online.

The University CISO is responsible for managing the IT security training and awareness program and will inform users and supervisors of their requirements, monitor compliance with the training requirement and update supervisors regarding the compliance of their employees.

Functional department managers responsible for managing information resources must have adequate training on the proper implementation of security controls for the systems and data under their control.

Information technology personnel responsible for administering security controls must have adequate training on procedures related to security administration.



IV. RESPONSIBILITIES

Role	Responsibility
Chief Information Security Officer	Develops and operates the Information Security Training and Awareness program, ensuring the Community receives the appropriate security training associated with their jobs and maintaining records of training received.
Management	Ensures that all employees are appropriately trained and understands their roles in implementing the University's Information Security Policies.
Staff	Complete annual security training. Review, understand, and agree to comply with all University "Information Security Policies and Guidelines."

V. REFERENCES

	Name	Reference
Frameworks	(CIS) Cybersecurity Controls Framework (V7.1)	CIS 17: Implement a Security Awareness and Training Program; CIS 19: Incident Response and Management; CIS 20: Penetration Testing and Red Team Exercises;
Regulations and Requirements		
Supporting Standards and Procedures		

VI. REVISION HISTORY

This section contains comments on any revisions to this document and the date they were made.

Revision Number	Date	Name	Description
20-R1	6/30/2020	UMB-ISTAP-ISOPOL05-20-R1	Initial Version
(Next Rev.) 21-R1	06/30/2021		

APPENDIX A

INFORMATION SECURITY AWARENESS PROGRAM

Information Security Awareness Program is delivered via multiple means which may include, but are not limited to:

- **ISO maintains an Information Security website.**
The University Information Security Office (ISO) maintains a website <https://www.umb.edu/it/security> featuring recent Information Security announcements, blogs, concepts, best practices, advisories, and relevant security newsletters and articles.
- **ISO must provide a mandatory Cybersecurity Orientation for all new hires.**
- **Personal Strategies for Cyber Safety**
Personal Strategies classes are offered to teach mindful personal security adjustments to personal devices with instantaneous and significant outcomes on personal cybersecurity and response to phishing and other online threats.
- **A comprehensive National Cybersecurity Awareness Month (NCSAM).**
Daily activities are guided by yearly themes from The National Initiative for Cybersecurity Careers and Studies (NICCS) for the entire month of October.
- **Security Smart Newsletter.**
ISO in conjunction with the IT Communication publishes a monthly newsletter sent via email and is posted on UMass Boston's website: https://www.umb.edu/editor_uploads/images/it/Security_Smart_Fall2019_umb.pdf
- **IT Communication provides a periodical hour-long information security class for interested staff, faculty, and students.**
- **IT Communication publishes weekly IT news and alerts, providing relevant Cybersecurity messages, directions, announcements, and news from the ISO via mass email to the Community.**
- **ISO runs simulated phishing campaigns that follow with mandatory online training for those who fall for the Phish.**
- **Regulated data compliance awareness training.**
Training must be provided for the Family Educational Rights and Privacy Act (FERPA) for all faculty and staff.



- **Payment Card Industry (PCI) Compliance Awareness for individuals handling PCI related data.**



Signature Page

APPROVED BY:

Ray Lefebvre

07/02/2020

Raymond Lefebvre
Vice-Chancellor and Chief Information Officer

Date

APPROVED BY:

Wil Khouri

07/02/2020

Wil Khouri
Assistant Vice-Chancellor and Chief Information Security Officer

Date

Section Six: Information Security Risk Management Awareness Policy (ISRMP)

XV. PREAMBLE

The Information Security Risk Management Policy (ISRMP) guides the Information Security Office (ISO) and serves as the foundation of the University of Massachusetts Boston (The University) Information Security Program, and such, it is required that a risk-based focus be pervasive throughout the Information Security Program.

XVI. POLICY STATEMENT

This Policy defines the commitment of the ISO and The University with respect to managing technology and data in a manner that ensures operations are conducted within an acceptable level of risk. The ISRMP addresses all the University's risks associated with the use of information technology.

XVII. PURPOSE

The Information Security Risk Management Policy has been established to outline the measures required to identify, assess, and treat risks to the confidentiality, integrity, and availability (CIA Triad) of the University's data and systems, as well as identify threats to campus assets. This Policy includes the process to determine appropriate management actions, establish priorities for managing and implementing adequate controls, and define the fundamental goals of an Information Security Risk Management Program.

XVIII. PROGRAM GOALS

The purpose of this Policy and Program is to shift the focus away from broadly applying industry standards across the board, and instead help identify and address the risk exposures that are most likely to impact the University and focus the mitigation efforts on risks. The ISO specifies the fundamental goals of the Program as follows:

- Improve the security posture of the organization.
- Empower departments to identify and remediate risks.
- Guide the University to prioritize remediation tasks.
- Identify real threats and weaknesses.
- Increase visibility and grow the capability of tracking and documenting risks.
- Standardize risk assessment approaches and procedures across all units.

- Meet audit, regulatory, and University community expectations.

XIX. SCOPE

The ISRMP encompasses the University's data and systems, internal or external, that store, process, or transmit data. The Policy applies to all users, including faculty, staff, students, employees, service providers, vendors, and any other individuals with access to the University's data and systems. Risk evaluations are performed annually or in real-time as dictated by significant changes to systems or infrastructure and enforced through a continual risk-centric and holistic management process.

XX. RESPONSIBILITIES

The ISO will ensure that:

- The Policy is implemented as described.
- Risk assessments are conducted annually based on threats and vulnerabilities or following significant changes to critical environments.
- Risks are communicated to the Data or Systems Owner.
- Risk assessments will be reviewed annually.
- The Standard is revised and updated when necessary.
- Any exception to the Standard is to be reviewed and approved by the ISO.

All University Managers, systems owners, data owners, and Information Technology custodians will work with the ISO to implement the ISRM Program, including remediation of identified risks in a timely manner.

XXI. PROCEDURES AND PROCESSES

The following section outlines the process for analyzing, selecting, remediating, and monitoring risk items.

G. Risk Analysis:

A documented risk analysis process is used as the basis for the identification, definition, and prioritization of risks (see Appendices B and C). The risk analysis process includes the following:

- *Identification and prioritization of the threats to information systems.*
- *Identification and prioritization of the vulnerabilities of information systems.*
- *Identification of a threat that can exploit vulnerabilities.*
- *Qualitative identification of the impact on the CIA triad of information resources if a threat exploits a specific vulnerability.*

- *Identification and definition of measures and/or controls used to protect the CIA Triad of the information resources.*

The risk analysis process is updated when environmental, operational, or technical changes arise with the potential to impact the confidentiality, integrity, or availability of information systems. Such changes include:

- *New threats or risks concerning the information systems.*
- *An information security incident.*
- *Changes to information security requirements or responsibilities. (Examples: New federal or state laws or regulations, a new role defined in the institution, new or modified security controls implemented.)*
- *Changes to the University's organizational or technical infrastructure that impacts information systems. (Examples: The addition of a new network, implementation of a recent hardware or software standard, implementation of a new method of creating, receiving, maintaining, or transmitting data.)*

When security measures for information systems do not meet a security standard, risks are identified and communicated. Three factors are considered when categorizing the risk (see Appendix A):

- *The type of possible threat and its likelihood.*
- *The effectiveness of current security controls or their vulnerability.*
- *The likely level of impact.*

Risks are categorized as **High**, **Medium**, or **Low** to be defined as follows:

Type	Defining Authority	Definition
High	<ul style="list-style-type: none"> • Defined by the ISO staff • Reviewed by unit managers, or data and systems custodians owning the defined risk* • Approved by the Vice-Chancellor/CIO 	<p><i>Risks represent a significant risk to the University. Management must address these risks within three (3) months of the issue date of its report</i></p>

<p>Moderate</p>	<ul style="list-style-type: none"> • Defined by the ISO staff • Reviewed by unit managers, or data and systems custodians owning the defined risk* • Approved by the Vice-Chancellor/CIO 	<p><i>Risks require remediation within six (6) months of the issue date of its report</i></p>
<p>Low</p>	<ul style="list-style-type: none"> • Defined by the ISO staff • Reviewed by unit managers, or data and systems custodians owning the defined risk* • Approved by the Vice-Chancellor/CIO 	<p><i>Risks represent opportunities for improvement</i></p>

* A risk owner is the department or business unit manager who is impacted by the risk and has the authority and responsibility to address the risk.

H. Security Control Selection:

The appropriate security controls used to mitigate identified risks are selected based on the nature, feasibility, and cost-effectiveness of the controls. The University ISO selected various elements to use as part of its ISRM Program from the following frameworks:

- Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53) framework.
- ISO 27002, Security Techniques – Code of Practice for Information Security Management.
- CIS Top 20 Critical Controls.
- ITIL- Industry Standard Framework for IT Service Management Guidelines and Best Practices.

All systems must meet the baseline requirements as defined in the Acceptable Use Policy and Data Classification Policy. Additional controls are evaluated based on the framework previously identified.

I. Risk Remediations:

The strategies for risk remediation are proportionate to the risks to the information systems. The selected and implemented risk management measures reasonably protect the confidentiality, integrity, and availability of information resources.

The remedial information security actions necessary to mitigate risk to operations, assets, individuals, and other organizations are



documented in a corrective action plan. Also, the risk is managed on a continuous basis. Corrective action plans must be created by the system owner and accepted by the ISO.

The remediation of risks will be tracked and documented based on the accepted corrective action plan.

A low risk can be accepted by an executive manager (Executive Vice Chancellor level or equivalent) with appropriate documentation and periodic reviews. If a previously accepted risk is realized in a real incident, the risk analysis and management are repeated with the new information; and the risk is re-addressed with greater sensitivity and urgency, based on the nature and extent of the incident.

J. Risk Monitoring:

The results of a risk assessment are documented and reviewed by executive managers, the ISO, system owners, data owners, and IT custodians.

The frequency of risk monitoring is based on:

- Legal / Regulatory compliance requirements.
- The importance or sensitivity of the information system.
- The requirements of the Information Security policies.
- The degree to which systems are interconnected to one another and the risk posed by such connections.

XXII. RESPONSIBILITY

The ISO is the responsible organization for implementing the provisions of this Policy. The Assistant Vice Chancellor / CISO is the designated point of contact.

XXIII. ATTACHMENTS

Appendix A: Risk Definitions

Appendix B: Risk Assessment Work Plan

Appendix C: Action Items

XXIV. RELATED UMASS BOSTON POLICIES, PROCEDURES, AND ANNOUNCEMENTS

UMB-WISP-ISOPRO01-19-R1: Written Information Security Program (WISP)

UMB-IRP-ISOPOL01-20-R1: Incident Response Policy

UMB-ISIRP-ISOPLA01-20-R1: Information Security Incident Response Plan

UMB-AUP-ISOPOL04-20-R1: Acceptable Use Policy (AUP)

UMB-ICP-ISOPOL11-20-R1: Information Classification Policy

XXV. REFERENCES



Frameworks	Name	Reference
	(CIS) Cybersecurity Controls Framework (V7.1)	CIS 01: Inventory and Control of Hardware Assets I would not use punctuation at the end of these headings CIS 02: Inventory and Control of Software Assets CIS 10: Data Recovery Capabilities CIS 13: Data Protection CIS 19: Incident Response and Management
Regulations and Requirements	Copyright Act of 1976 Digital Millennium Copyright Law of 1998 (DMCA) Family Educational Rights and Privacy Act of 1974 (FERPA) Health Insurance Portability and Accountability Act (HIPAA)	
Supporting Standards and Procedures	CIS RAM (Risk Assessment Method)	

XXVI. VERSION CONTROL

This section contains comments on any revisions that were made to this document and the date they were made.

Revision Number	Date	Name	Description
R1	09/15/2020	Wil Khouri	UMB-ISRMP-ISOPOL20-20-R1
	(Next Rev.) 07/2022-R1		

Appendix A: Risk Definitions

The following table defines the likelihood ratings for risks:

Likelihood Definition	
Very Likely	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. <i>Any event with a 90% chance of happening.</i>
Likely	The threat source is motivated and capable, but controls are in place that may impede the successful exercise of the vulnerability. <i>Any event with probabilities of 40% to 90% chance of occurring.</i>
Unlikely	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. <i>The event will have less than a 40% chance occurring.</i>

The following table defines the impact ratings for risks:

Impact Definition	
Catastrophic	Exercise of the vulnerability (1) may result in human death or serious injury; (2) may result in a highly costly loss of significant tangible assets or resources. Financial loss will exceed 5% of the University's total Revenue. (3) may significantly violate, harm, or impede an organization's mission, reputation, or interest.
Severe	Exercise of the vulnerability (1) may result in human injury; (2) may result in a costly loss of tangible assets or resources; Financial loss may exceed 3%, but less than 5% of the school's total Revenue (3) may violate, harm or impede an organization's mission, reputation or interest.
Minor	Exercise of the vulnerability (1) may result in loss of some assets or resources; Financial loss of less than 3% of total Revenue (2) may noticeably affect an organization's mission, reputation, or interest.

Appendix A: Risk Definitions (Continued)

The following table shows the intersection of impact and likelihood, resulting in an overall risk rating:

Risk Rating		Likelihood		
		Very Likely	Likely	Unlikely
Impact	Catastrophic	High Risk	High Risk	Medium Risk
	Severe	High Risk	Medium Risk	Low Risk
	Minor	Medium Risk	Low Risk	Low Risk

The following table describes the risks and necessary action associated with them:

Risk Description and Necessary Actions	
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible. <i>Immediate Senior Management action is required. It must be mitigated within 90 days.</i>
Medium	If an observation is rated as a medium risk, corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable time. <i>Risk has material impact levels and requires Management attention. It must be mitigated between 91 to 180 days.</i>
Low	If an observation is described as a low risk, the system's owner must determine whether or not corrective actions are required or decide to accept the risk. <i>It could be managed by routine procedures and checklist.</i>



Appendix B: Risk Assessment Work Plan

UMASS BOSTON: INFORMATION SECURITY OFFICE

Risk Assessment

Objective: The objective of this assessment is to identify and prioritize Information Security Risks for those critical programs and business functions where Regulated Data such as Personally Identifiable Information (PII) and/or Protected Health Information (PHI), is created, stored, disseminated, or managed.

Scope: Data can refer to electronic or hardcopy information associated with the in-scope business processes.

All facets of each business process are in-scope for the assessment. This includes the development of application code; the receipt, movement, dissemination, retention, and destruction of data; all access to the data; all applications, servers, storage devices, networking devices, and computing devices (desktops, laptops, mobile devices) that support the development, dissemination, and storage of the data; all business processes and procedures that support the data lifecycle; and security and privacy policies that support the in-scope business process.

Security Risk Profile Sample

Resource Name: *OneDrive shared resource*

Resource Owner: *Victoria Principal*

Information Security Team Contact: *Alison Murray*

A. General Information

1. Please select which groups of individuals have access to the asset:

- **Employees (Staff, Faculty)**
- **Clients (Students, Alumni)**
- **Partners (DCO, UMass Sister Campus Staff)**
- **Service Providers (Vendors, Outsourcers)**
- **Other:** *Boston University Faculty*

2. Has a penetration test been performed on the application? Yes No

- a. Please enter the date of the most recent penetration test: *April 13*
- b. Who performed the most recent penetration test? *Compass IT Compliance*
- c. Please briefly describe any outstanding security issues:

Severity	Security Issue
1	<i>MFA not enabled on the app suite</i>
2	<i>Hard Drive of Endpoint unencrypted</i>
2	<i>Tenable reported a driver vulnerability</i>
3	<i>Operating System on Endpoint unpatched</i>



Appendix B (Continued)

B. Information Sensitivity

1. Please specify the client data used or collected (select all that apply):

- Financial institution account information
- Credit card information
- Identifying number (i.e., Social Security)
- Home address
- Phone number
- Medical information
- Birthdate
- Personal Identifiable Information
- Cultural information (i.e., Ethnicity, religion, sexual preference, criminal record)
- Dependents, or beneficiaries
- Performance reviews/evaluations
- Salary/compensation information

2. Please select the *regulatory requirements* that are applicable (select all that apply):

- The Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (EU GDPR)
- The California Consumer Privacy Act (CCPA)
- Other, please specify *Massachusetts Privacy Law*

3. Are there any other *requirements* (for example, contractual) that mandate information security controls for confidentiality, integrity, availability, or accountability?

Yes No

C. Business Requirements

1. Please rate the overall confidentiality needs (the consequence of unauthorized disclosure or compromise of data stored, processed, or transmitted by the resource) of the information resource:

- High
- Moderate
- Low

Appendix B (Continued)

2. Please rate the overall integrity needs (basically the consequences of corruption or unauthorized modification/destruction of data stored, processed, or transmitted by the resource) of the information resource:

- High
- Moderate
- Low

3. Please rate the overall availability needs (basically the consequences of loss or disruption of access to data the resource stores, processes, or transmits) of the information resource to non-Company users:

- High
- Moderate
- Low
- N/A

4. Please rate the overall availability needs (basically the consequences of loss or disruption of access to data the resource stores, processes, or transmits) of the information resource to Company users (excluding access to support the application or system itself):

- High
- Moderate
- Low
- N/A

5. Please rate the overall accountability needs (basically the consequences of the inability or compromised ability to hold users accountable for their actions in the resource) of the information resource to its general users:

- High
- Moderate
- Low

6. Please rate the overall accountability needs (basically the consequences of the inability or compromised ability to hold users accountable for their actions in the resource) of the information resource to its support or administrative users:

- High
- Moderate
- Low



Appendix B (Continued)

7. Please rate the overall reputational damage to the organization if it was known to the user community or industry that the information resource had been breached or defaced in some manner:

- High
- Moderate
- Low

Appendix C: Action Items

Action Items: Areas/Initiatives/Business Workflows

1. Obtain a general understanding of the area/function under review.	
<ul style="list-style-type: none"> <input type="checkbox"/> Interview department personnel and prepare or update flowcharts of their operations. 	
<ul style="list-style-type: none"> <input type="checkbox"/> Obtain an organizational chart for the area under review. 	
<ul style="list-style-type: none"> <input type="checkbox"/> Review the department's Web site to gain an understanding of the area. Review the Web site for documentation, policies, and procedures. 	
<ul style="list-style-type: none"> <input type="checkbox"/> Review the department's Web site for existing University policy and procedures. 	
Confidential and Regulated Data	
<ul style="list-style-type: none"> <input type="checkbox"/> Determine if the area under review contains PII, PHI, or other information. 	
Cash\Check\Credit Card Payments	
<p>If the area under review receives any payments on behalf of the University, consult with Finance to ensure that the area is following the business practices established by Finance. For example, ask the following questions:</p> <ul style="list-style-type: none"> <input type="checkbox"/> How are payments collected? Cash, check, credit card <input type="checkbox"/> Does the department forward all payments to the Cashier? 	

2. Objective: Understand how the function supports the University's business objectives.			
Testing Procedure	Risk Impact	Likelihood	Recommendations
Perform a walkthrough of the function, including the flow of information.	<input type="checkbox"/> Catastrophic	<input type="checkbox"/> Very Likely	
	<input type="checkbox"/> Severe	<input type="checkbox"/> Likely	
	<input checked="" type="checkbox"/> Minor	<input checked="" type="checkbox"/> Unlikely	Risk: Low

3. Objective: Ensure that a general level of controls to support the function environment exists, including dedicated staff, a network diagram, and customer service processes. Determine that sufficient technical and end-user training is provided, and documentation exists to ensure that the system is used effectively and efficiently.			
Testing Procedure	Risk Impact	Likelihood	Recommendations
Review the organizational chart to ensure that appropriate resources are assigned to support it.	<input type="checkbox"/> Catastrophic	<input type="checkbox"/> Very Likely	
	<input type="checkbox"/> Severe	<input type="checkbox"/> Likely	
	<input checked="" type="checkbox"/> Minor	<input checked="" type="checkbox"/> Unlikely	Risk: Low

4. Objective: Ensure that a general level of controls to support the function environment exists, including dedicated staff, a network diagram, and customer service processes. Determine that sufficient technical and end-user training is provided, and documentation exists to ensure that the system is used effectively and efficiently.			
Testing Procedure	Risk Impact	Likelihood	Recommendations
Obtain and review function training materials available to new users and for ongoing needs.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Unlikely	
			Risk:
Obtain the network diagram and verify that the infrastructure and network controls exist.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor:	<input type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Unlikely	
			Risk:
Review backup and recovery controls and procedures to ensure that backed up data are defined and recovery from loss is as expected and obtain evidence backup procedures exist. Ensure backups are encrypted in transit and at rest.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Unlikely	
			Risk:
A data retention schedule must be followed to ensure the destruction of sensitive information in an appropriate timeframe.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Unlikely	
			Risk:

5. Objective: Review the relationship between the function and the University. Verify whether business associates agreements exist. If core application/systems are outsourced, verify the relationship between the University and the vendor.					
Testing Procedure	Risk Impact	Likelihood	Recommendations		
Determine if contractual requirements exist and, if yes, what level of security the department has agreed to, and is it compliant?	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Unlikely	<table border="1"> <tr> <td style="background-color: #cccccc;">Risk:</td> <td style="background-color: #ffffcc;">Moderate</td> </tr> </table>	Risk:	Moderate
Risk:	Moderate				
If the function is hosted by a third party (i.e., Cloud), complete an Audit Form for the SAAS environment.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input checked="" type="checkbox"/> Likely <input type="checkbox"/> Unlikely	<table border="1"> <tr> <td style="background-color: #cccccc;">Risk:</td> <td style="background-color: #ffcc99;">High</td> </tr> </table>	Risk:	High
Risk:	High				
Obtain the Service Level Agreement and verify the function is adequately supported by the service provider. Verify the agreement is at a level that corresponds with the University's standards.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Unlikely	<table border="1"> <tr> <td style="background-color: #cccccc;">Risk:</td> <td style="background-color: #ffffcc;">Moderate</td> </tr> </table>	Risk:	Moderate
Risk:	Moderate				

6. Objective: Ensure the integrity and confidentiality of data from source systems, or departments, to the University.					
Testing Procedure	Risk Impact	Likelihood	Recommendations		
Verify interface controls exist that ensure the integrity of data from the source system to and from other systems.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Unlikely	<table border="1"> <tr> <td style="background-color: #cccccc;">Risk:</td> <td style="background-color: #ffffcc;">Moderate</td> </tr> </table>	Risk:	Moderate
Risk:	Moderate				

7. Objective: Verify that activities for granting, modifying, and removing user access to function are appropriate.			
Testing Procedure	Risk Impact	Likelihood	Recommendations
Verify that activities for granting, modifying, and removing user access to function are correct and timely.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input checked="" type="checkbox"/> Likely <input type="checkbox"/> Unlikely	
			Risk:
Verify access is appropriate based on job function.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input checked="" type="checkbox"/> Likely <input type="checkbox"/> Unlikely	
			Risk:
Obtain evidence to verify annual recertification of access is performed.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Unlikely	
			Risk:
New Users: Obtain a system-generated report with 'date created' next to accounts. Obtain access request form verifying management approval, business data owner approval, and that granted access matches access requested.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Unlikely	
			Risk:
Terminated Users: Obtain a system-generated access report and the termination report from HR to verify no terminated users have access to function. Verify the management of function obtains a termination report. Verify that activities for granting, modifying, and removing user access to function are appropriate.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input checked="" type="checkbox"/> Likely <input type="checkbox"/> Unlikely	
			Risk:
Modified Users Verify that activities for granting, modifying, and	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe	<input type="checkbox"/> Very Likely <input type="checkbox"/> Likely	

removing user access to XXX are appropriate.	<input type="checkbox"/> Minor	<input checked="" type="checkbox"/> Unlikely	Risk: Moderate
--	--------------------------------	--	-----------------------

8. Objective: Ensure that data is secure while in transit.

Testing Procedure	Risk Impact	Likelihood	Recommendations		
Verify controls ensure that data being disseminated is secure.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input checked="" type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input type="checkbox"/> Unlikely	<table border="1"> <tr> <td>Risk:</td> <td>High</td> </tr> </table>	Risk:	High
Risk:	High				

9. Objective: Ensure that the password parameters for the function are appropriate.

Testing Procedure	Risk Impact	Likelihood	Recommendations		
Review password parameters, change frequency and complexity, to ascertain that it meets minimum security requirements.	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input checked="" type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input type="checkbox"/> Unlikely	<table border="1"> <tr> <td>Risk:</td> <td>High</td> </tr> </table>	Risk:	High
Risk:	High				
Ensure personal computers are configured to automatically "lock" (Screen Saver Timeouts).	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input type="checkbox"/> Very Likely <input checked="" type="checkbox"/> Likely <input type="checkbox"/> Unlikely	<table border="1"> <tr> <td>Risk:</td> <td>High</td> </tr> </table>	Risk:	High
Risk:	High				

10. Objective: Ensure that network and system controls are in place for in-scope platforms.

Testing Procedure	Risk Impact	Likelihood	Recommendations		
Evaluate system and network security for all in-scope platforms. Determine the following for all in-scope computing platforms: <ul style="list-style-type: none"> • Malware Protection • Whole Disk Encryption • Email Encryption • Administrative Access 	<input checked="" type="checkbox"/> Catastrophic <input type="checkbox"/> Severe <input type="checkbox"/> Minor	<input checked="" type="checkbox"/> Very Likely <input type="checkbox"/> Likely <input type="checkbox"/> Unlikely	<table border="1"> <tr> <td>Risk:</td> <td>High</td> </tr> </table>	Risk:	High
Risk:	High				

11. Objective: Ensure PHI (personal health information), PII (personally identifiable information), and other sensitive data components are adequately protected, and access is based on job responsibility; and verify compliance with in-scope regulations.			
Testing Procedure	Risk Impact	Likelihood	Recommendations
Obtain an understanding of the University's procedures for complying with in-scope regulations.	<input checked="" type="checkbox"/> Catastrophic	<input checked="" type="checkbox"/> Very Likely	
	<input type="checkbox"/> Severe	<input type="checkbox"/> Likely	
	<input type="checkbox"/> Minor	<input type="checkbox"/> Unlikely	Risk: High

12. Ensure that processes and controls for authorizing, constructing, testing, and implementing changes in the function production environment exist.			
Testing Procedure	Risk Impact	Likelihood	Recommendations
Obtain an understanding of the change control process. Select a sample of X out of X (X %) changes to verify controls for authorizing, constructing, testing, and implementing changes in the production environment.	<input checked="" type="checkbox"/> Catastrophic	<input type="checkbox"/> Very Likely	
	<input type="checkbox"/> Severe	<input type="checkbox"/> Likely	
	<input type="checkbox"/> Minor	<input checked="" type="checkbox"/> Unlikely	Risk: Moderate
Verify segregation of duties control to ensure that the roles and responsibilities throughout the program change process are appropriately restricted and segregated.	<input checked="" type="checkbox"/> Catastrophic	<input type="checkbox"/> Very Likely	
	<input type="checkbox"/> Severe	<input type="checkbox"/> Likely	
	<input type="checkbox"/> Minor	<input checked="" type="checkbox"/> Unlikely	Risk: Moderate



Signature Page

APPROVED BY:

Ray Lefebvre *September 23, 2020*
Raymond Lefebvre Date
Vice-Chancellor and Chief Information Officer

APPROVED BY:

Wil Khouri *September 23, 2020*
Wil Khouri Date
Assistant Vice-Chancellor and Chief Information Security Officer

SECTION SEVEN: VULNERABILITY SCANNING, VULNERABILITY MANAGEMENT, AND PEN-TESTING POLICY (VMPP)

I. POLICY STATEMENT

This policy defines the guidelines for conducting vulnerability scanning, vulnerability management, and penetration testing of systems within the University of Massachusetts, Boston (The University).

II. PURPOSE

The purpose of this policy is to establish the minimum requirements for vulnerability scanning, vulnerability management, and penetration testing of The University-owned systems.

III. SCOPE

This policy applies to all information technology assets and systems owned or leased by The University.

IV. DEFINITIONS

Vulnerability Management:

It is the process of identifying, analyzing, approving, and mitigating vulnerabilities [Common Vulnerabilities and Exposures (CVEs)] on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend the compromise to the network.

Vulnerability Scanning:

A technique used to identify hosts/host attributes and associated vulnerabilities.

Penetration Testing:

It is the mimicking of real-world attacks to verify the security features or identify methods to circumvent the security features of an application, system, or network, often involving the execution of attacks on production systems and data, utilizing tools and techniques employed by malicious actors to identify and close gaps in an environment.

V. ROLES AND RESPONSIBILITIES

The following roles are responsible for the discovery, assessment, remediation, and validation of vulnerabilities as follows:

- The University Chief Information Security Officer (CISO), or their designee, is responsible for working with the asset owner to perform a vulnerability assessment of The University-owned assets.
- IT asset owners are responsible for ensuring that the associated assets are available for vulnerability scanning.

- Asset owners, system Administrators, and Desktop Services Staff are responsible for implementing remediation actions for detected vulnerabilities on university-owned or leased IT assets.

VI. POLICY AND PROCEDURES

Vulnerability management, vulnerability scanning, and penetration testing are required for all restricted systems (Endpoints and servers and related peripheral components, including, but not limited to, storage components, systems and applications software, interconnected communications networks or customer communication systems, and electronic funds transfer systems; by which data are electronically collected, transmitted, processed, stored, or retrieved).

1. Vulnerability Scanning:

- a. ISO staff must identify IT assets in-scope and their respective scan windows.
- b. Desktop Services and system and network administrators must configure and deploy scanning software components to the IT assets within the scope as well as endpoints and network infrastructure within scope to allow access for vulnerability scans.
- c. The ISO staff must conduct regularly scheduled vulnerability testing on all public-facing and restricted systems.
- d. Upon significant configuration change to a system, a scan must be performed. In addition, the Change Control Record (CCR) must state the need for a vulnerability scan before the change.
- e. Failed vulnerability scans must be addressed and followed by remediation and rescans, repeating these steps until the vulnerability testing completes successfully.
- f. Upon identifying new vulnerability issues, firewall configuration shall be updated accordingly.

2. Vulnerability Management:

- a. Discovered vulnerabilities must be identified across the entire attack surface, scored, and assessed by risk levels.
- b. A remediation plan must be created by prioritizing patching according to asset categorization or classification, i.e., starting with the most critical vulnerabilities on the most vital assets and then proceeding to the less critical ones.
- c. Critical vulnerabilities should be remediated as soon as possible and must be remediated within 3 days.
- d. High Vulnerabilities must be remediated within 14 days.
- e. Medium Vulnerabilities must be remediated within 30 days.
- f. Low Vulnerabilities should be addressed within 90 days during regular maintenance cycles.
- g. Validate that the vulnerabilities are remediated by rescanning.



3. Penetration testing:

- a. External and internal penetration testing shall be performed on an annual basis.
- b. After any significant infrastructure or application changes, external and internal penetration testing shall be performed.
- c. Penetration testing shall minimally consist of network-layer and application-layer penetration tests.
- d. Exploitable vulnerabilities discovered during penetration testing shall be corrected and followed by a scan to demonstrate that identified exploits are addressed.
- e. Specific third-party penetration testing requirements such as PCI-DSS must be adhered to as applicable.

VII. RELATED POLICIES, PROCEDURES, AND ANNOUNCEMENTS

UMB-PMP-ISOPOL08-21-R1: UMass Boston Patch Management Policy

VIII. REFERENCES

Frameworks	Name	Reference
	(CIS) Cybersecurity Controls Framework (V7.1)	CIS 03: Continuous Vulnerability Assessment and Remediation CIS 06: Maintenance, Monitoring, and Analysis of Audit Logs CIS 7: Email and Web Browser Protections CIS 16: Account Monitoring and Control CIS 20: Penetration Tests and Red Team Exercises
Regulations and Requirements	PCI, FERPA, GDPR, HIPAA, CCPA, Massachusetts regulations 201 CMR 17.00	
Supporting Standards and Procedures		

IX. VERSION CONTROL (Revisions and dates)

Revision Number	Date	Name	Description
R1	02/04/2022	Wil Khouri	UMB-VMPP-ISOPOL19-22-R1
	(Next Rev.) 07/2023-R1		



Signature Page

APPROVED BY:

DocuSigned by:

Raymond Lefebvre

4/27/2022

Raymond Lefebvre
Vice-Chancellor and Chief Information Officer

Date

APPROVED BY:

DocuSigned by:

Wil Khouri

4/27/2022

Wil Khouri
Assistant Vice-Chancellor and Chief Information Security Officer

Date