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

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY (AUP)

I. POLICY STATEMENT

The University of Massachusetts Boston (the University) encourages widespread access and distribution of public data and information. To that end, the University provides its community with access to local, national, and international sources of information and an atmosphere that encourages the free exchange of ideas and information sharing. Access to the University's information technology resources is a privilege that imposes specific responsibilities and obligations on users. The University expects all community members to responsibly use computing, data, and information technology resources. Access and use of these resources are 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 violating this policy may be subject to disciplinary proceedings and 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 informs individuals of their obligations to comply with all existing state and federal laws and institutional policies regarding using the University's information technology resources. Individuals using the University's information technology resources may include, but are not limited to, employees, students, 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 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 is obligated to protect the integrity of information technology resources, all users' rights, and its property at its sole discretion. **The University thus reserves the right to examine material stored on or transmitted through its resources (i.e., networks, Clouds, storage media, etc.) for any 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, seize such device, and copy or has copied and wiped any information from the data storage mechanisms of such device as

UMass Boston **IT Acceptable Use Policy**

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 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 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.

UMass Boston **IT Acceptable Use Policy**

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 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 the required privacy and security training programs promptly, as mandated by the State and per University Policy: Information Security Training and Awareness Policy.
   The privacy and security training courses are designed to educate employees on best practices, policies, and procedures related to safeguarding sensitive information, maintaining data privacy, and ensuring information security within the organization.
   Failure to complete the mandatory training programs within the specified timeframe may result in disciplinary action, up to and including termination of employment, per the University's policies and applicable laws.
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 or publicly available information to which you have been granted access.
5. Employees are expected to exercise sound 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), 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 you 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 to prevent 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 according to the University's policies and legal and contractual requirements.

UMass Boston **IT Acceptable Use Policy**

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. In compliance with Personal Privacy Laws, our Acceptable Use Policy (AUP) mandates the protection of personal data and upholds the confidentiality of sensitive information. Users are required to adhere to all applicable laws and regulations, ensuring that personal rights and privacy are respected at all times (i.e., 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. Email distribution lists should be used only for their intended purposes related to University business, including disseminating information, facilitating discussions, or sharing updates relevant to the list's scope and audience.
14. Email distribution lists should not be used to solicit personal business or broadcast political statements. Unauthorized commercial advertising, solicitations, or other unsolicited bulk communications are strictly prohibited on mass email lists owned by the University.
15. Employees should exercise discretion and professionalism when sending messages to email lists, ensuring the content is appropriate, respectful, and aligned with the list's purpose.
16. Internet use must comply with the Terms of Service stipulated by the Internet service providers and all University policies.
17. Never use the University's resources to engage in any illegal activity.
18. 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.
19. Encrypt data at rest and in transit to comply with the University's policies and applicable state and federal regulations.
20. The use of personally owned computer equipment to access University resources may be allowed at the discretion of the University. If allowed, such equipment must be set up to meet University standards, including login passwords, firewalls, 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, presentment of false or misleading information or credentials, or unauthorized use of information systems/services.
2. Accessing unauthorized systems or data resources or utilizing unnecessary functions to perform one's duties.
3. Sharing personal account credentials with anyone. Employees, students, and contractors who receive usernames and passwords must keep them 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.

UMass Boston **IT Acceptable Use Policy**

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 system on the University's networks without using 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 (i.e., 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, Intune, Jamf, 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 information security measures of any host, network, or account without CISO's approval for emergency business purposes.
23. Disclosure of PII/PHI to any individual outside the University unless there is a legal or regulatory requirement.
24. Unencrypted transmissions of PII (confidential, private, 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, but not limited to, FTP, instant messenger, or fax.
25. Storing confidential information, including PII (confidential, private, and sensitive information), trade secrets, proprietary financial information, or financial account numbers, on laptop computers, mobile computing devices, and removable media (e.g., 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 or alter anti-malware software settings.

UMass Boston | **IT Acceptable Use Policy**

27. Under no circumstances may an employee, student, contractor, or consultant deactivate or alter firewall software settings.
28. Employees, students, contractors, and consultants should not open electronic messaging attachments that are not expected, come from unknown addresses, or appear 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 exercise extreme caution when using social media or instant message applications. Employees must not share sensitive or private information through these mediums.

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

V. OTHER PROVISIONS

- Management's explicit approval is required for any 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.
- It is prohibited to access unauthorized systems or data resources or to utilize functions that are not necessary to perform the employee's duties.
- 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 their use, suspension of privileges (including Internet access), and 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 University does not own the equipment.

If, while working on computer equipment, material that indicates a possible violation of University policy or state or federal law is discovered, 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.

UMass Boston **IT Acceptable Use Policy**

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 (V8)	Control 01: Inventory and Control of Hardware Assets; Control 02: Inventory and Control of Software Assets; Control 03: Data Protection; Control 04: Secure Configuration of Enterprise Assets and Software; Control 06: Access Control Management; Control 09: Email and Web Browser Protections; Control 10: Malware Defenses; Control 14: Security Awareness and Skills Training;
Regulations and Requirements	PCI, FERPA, HIPAA, CCPA, GLBA, Massachusetts regulations 201 CMR 17.00	
Supporting Standards and Procedures		

IX. VERSION CONTROL

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
R1	04/30/2024	Wil Khouri	UMB-AUP-ISOPOL04-24-R1
R1	(Next Rev.) 07/2027-R1		

Signature Page

APPROVED BY:

DocuSigned by:

Raymond Lefebvre

66E15F772702474...

5/6/2024

Raymond Lefebvre   Date

Vice Chancellor and Chief Information Officer

APPROVED BY:

DocuSigned by:

Wil Khouri

668B0E1CFA4540D...

5/1/2024

Wil Khouri   Date

Assistant Vice Chancellor and Chief Information Security Officer