

Information Security Policy

Policy Number	ITS-006
Effective Date	November 1, 2019
Responsible Office / Person	CITS
Related Policies	ITS-001 Acceptable use of information technology resources ITS-002 Email communications ITS-005 UMassD Logon account eligibility ITS-007 Confidentiality of institutional information and research data
Additional History	

I. Introduction

Institutional information, research data, and information technology (IT) resources are critical assets necessary for the University of Massachusetts Dartmouth (“UMass Dartmouth”) to fulfill its missions. To maximize the preservation and protection of these assets, and to manage the risks associated with their maintenance and use, this policy establishes information security governance structure, rules, technical standards, and procedures.

By approval of UMass Dartmouth’s Chancellor, this policy exists in conjunction with all other institutional policy.

II. Policy Statements

Information security is the responsibility of every user of institutional information, research data, and information technology resources. All users who create, access, manage, or manipulate institutional information, research data, or information technology resources must comply with this policy’s administrative, technical, and physical safeguards.

A. Governance

This policy establishes campus information security governance with the creation of roles and responsibilities.

- Information Security Program Management
 - Chancellor and VCAF/CFO
 - Associate Vice Chancellor and Chief Information Officer
 - Chief Information Security Officer
 - Vice Chancellors and Deans
- Information Categorization and Management
 - Data Stewards
 - Steward Delegate
 - Data Administrators
 - Subject Matter Experts

- Data Custodians
- Information Security Program Implementation
 - Vice Chancellors and Deans
 - Department Chairs, Directors, Supervisors, etc.
 - Security Liaisons
 - Director of IT Infrastructure
 - Service Administrator
 - Users

Additional details regarding the specific roles in these categories are in section IV.

B. Information Incident Reporting

All users must report incidents involving unauthorized access to institutional information, research data, and information technology resources to the Chief Information Security Officer. You may also report them to your local information security liaison and to UMass Dartmouth CITS. For more information, see the [Data Security Incidents - Prevention and Response Procedures](#).

C. Institutional Information and Research Data Categorization

Institutional information and research data will be categorized in alignment with federal regulations, contractual obligations, and information risk*. Specific technical controls adhere to each category. Data Stewards are responsible for the Categorization of institutional information and research data under their purview. Data Custodians are responsible for using the appropriate security controls associated with each data category.

For more information regarding the categorization of institutional information and research data, see [Data and System Categorization](#).

For more information regarding the specific technical controls that adhere to each category, see [Information Security Controls](#).

* The standards are adapted from the Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199) available at <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.

III. To Whom This Policy Applies

This policy applies to every user (including, but not limited to, all faculty, students, staff, contractors, visiting researchers, or guests and volunteers) who accesses, manages, or manipulates institutional information, research data, or information technology resources.

IV. Responsible Parties

Every person at UMass Dartmouth has a responsibility to protect institutional information, research data, and information technology resources that they use or are otherwise within their control. These responsibilities vary based on the functional role of the individual.

Depending on those functions, some individuals may have more than one role. This section identifies roles and their corresponding responsibilities.

A. Information Security Program Management

The following roles have responsibility for University of Massachusetts Dartmouth information security framework, oversight, and assistance.

1. Chancellor and VCAF/CFO

The Chancellor and VCAF/CFO have primary responsibility for campus information security and safety. The Chancellor and VCAF/CFO may delegate authority for information security to the Associate Vice Chancellor for Computer & Information Technology / Chief Information Officer.

2. Associate Vice Chancellor for Computer & Information Technology / Chief Information Officer (CIO)

As a delegate of the Chancellor and VCAF/CFO, the Associate Vice Chancellor for Computer & Information Technology / Chief Information Officer, will provide executive oversight to the University of Massachusetts Dartmouth Information Security Program.

3. Chief Information Security Officer (CISO)

The Chief Information Security Officer is the University official with the authority to harmonize campus information security. The CISO is responsible for the development, implementation, and maintenance of a comprehensive information security program.

4. Vice Chancellors and Deans

The Vice Chancellors and Deans are responsible for program management oversight for the security of institutional information, research data, and information technology resources within their areas of purview.

B. Information Categorization and Management

As noted in Section II C, institutional information and research data will be categorized in alignment with federal regulations, contractual obligations, and information risk. Specific technical controls adhere to each category. Data Stewards are responsible for the categorization of institutional information and research data under their purview and the implementation of the specific technical controls that adhere to each category. Data Custodians are responsible for following the rules set by the Data Stewards.

For more information see [Information Management](#).

1. Data Stewards

Stewards have the highest level of responsibility for overseeing the categorization of institutional information and research data, and administering the privacy, security, and regulatory compliance of data sets under their purview (e.g., education records, human

resources, and financial data). In the case of research data, in addition to acting as a Data Custodian, the Principal Investigator acts as the steward in consultation with research staff.

2. Steward Delegate

A steward may designate a delegate who will act on behalf of the steward for a portion or all of the information and data under their purview. The delegate should be identified in writing to the Associate Vice Chancellor for Computer & Information Technology / CIO as well as the Chief Information Security Officer, along with how long the delegation will be in place.

3. Data Administrators

Data Administrators are those individuals who are responsible for a particular line of business or who may have special knowledge of and responsibility for the compliance requirements for certain information or data sets. They have responsibility to inform the appropriate Steward(s) of any requirements or considerations that may influence policy, and set procedures, standards, or guidelines.

4. Subject Matter Experts

Subject Matter Experts are those individuals in roles with expertise such as risk, legal, compliance, privacy, and security who have responsibility to inform the appropriate Steward(s) of any requirements or considerations that may influence policy, and set procedures, standards, or guidelines.

5. Data Custodians

Custodians are any individuals (employees, volunteers, etc.) who access, manage, or manipulate institutional information or research data. Custodians must follow campus policy and stewardship rules for handling of institutional information and research data.

C. Information Security Program Implementation

1. Vice Chancellors and Deans

In addition to the responsibilities of Vice Chancellors and Deans as noted in Section IV A 4 above, Vice Chancellors and Deans also have responsibility oversight for the implementation of the information security program within their areas of purview.

2. Department Chairs, Directors, Supervisors, etc.

Individuals who are responsible for a portion of the campus, such as a program, center, or line of business, shall develop, as needed, more restrictive information security controls for better management of risk to the institutional information or research data for which they are responsible. Supervisors may, at their discretion, create specific forms outlining the duties of their direct reports under this policy for review, signature, or workplace performance.

3. Security Liaisons

The unit security liaison is the person or persons designated by the unit head as the primary contact for the CISO. Their primary role is to share information security training in a manner

that works for their unit, to be available for incidents, and provide effective communication between the UMass Dartmouth CITS and the college or division they represent.

4. Director for IT Infrastructure

For central information technology resources, the Director for IT Infrastructure, in coordination with the CISO, draws up technology architectural outlines, issues standards, and develops uniform templates for use by CITS and the campus community.

5. Service Administrator

A Service Administrator (e.g., application administrator, system administrator, or network administrator) is the individual with principal responsibility for the installation, configuration, and ongoing maintenance of an information technology system.

6. Users

In accordance with this policy, users must be aware of the value of information. They must protect information reasonably. Users must therefore follow the requirements for:

- Information technology resources;
- Institutional information; and
- Research data

V. Standards

The user of every device connected to the campus network or that stores or transmits institutional information and research data is responsible for adherence to security control standards.

IT administrators either in UMass Dartmouth CITS or in specific colleges or units may do the actual installation and configuration work, but it remains the responsibility of the user of that device to have those controls installed, configured and up to date (even if that simply means that when prompted to keep a computer on for its update, the user will comply with the prompt).

Faculty, staff or researchers who do not have or accept IT administration support are still subject to these rules and assume all responsibility for maintaining up to date controls on their devices that store or transmit institutional information and research data. This rule applies to whether it is an institutionally owned device or personal, and whether it is on the campus network while physically on the campus or from a remote location.

A. Technology Standards

All information technology resources, regardless of ownership, that contain institutional information or research data must have the following foundational information security controls in place and functioning.

Additional controls may be required based on the categorization of the information or data, the nature of the information technology resource, the applicable regulatory or contractual requirements, or other risk management calculations.

The five foundational information security controls identified at the time of this policy's publication are referenced below. For additional information, or to see a complete, updated list of foundational information security controls, see [Information Security Controls](#).

a) Patch Management

Security patches must be installed, operational and regularly updated on all information technology resources.

b) Anti-Malware

Anti-malware solutions must be installed, operational and regularly updated for applicable information technology resources.

c) Firewall

Software to block incoming connections, unless explicitly allowed, must be installed and configured on applicable information technology resources.

d) Encryption

All institutional information and research data stored on end-user devices must be encrypted.

e) Secure Disposal

All information technology resources that contain institutional information or research data must be disposed of in an authorized manner.

B. User Account Standards

The campus owns all accounts, including UMassD Logon. It creates and provisions these accounts to users for the purposes of accessing university resources. All users have a responsibility to protect the university accounts under their care. Protection of these accounts may vary according to the risk that they present. Accounts with enhanced privileges may have additional requirements. For additional information including account standards, and password complexity rules, see [UMassD Logon Standards](#) and the [UMassD Logon Eligibility Policy](#).

At a minimum, all accounts must adhere to the following:

1. Credential Sharing

Credentials for individual accounts must not be shared.

2. Password Complexity

UMass Dartmouth CITS sets password complexity requirements for your UMassD Logon. It is against policy for a user to subvert those requirements. Other password protected accounts must establish passwords with equivalent or greater complexity as the UMassD Logon requirements.

VI. Terms and Definitions

Assets: Information technology resources, such as hardware and software and also including institutional information, research data, and intellectual property.

Availability: Ensuring timely and reliable access to and use of information. A loss of *availability* is the disruption of access to or use of information or an information system.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of *confidentiality* is the unauthorized disclosure of information.

Custodians: See “Institutional Information and Data Custodians” below.

Data Categorization: See “Institutional Information and Research Data Categorization”.

Data Custodians: Any individuals (employees, volunteers, etc.) who access, manage, or manipulate institutional information or research data. Custodians must follow campus policy and stewardship rules for handling of institutional information and research data.

End-User: Anyone who consumes an information service. For more information see “User”.

End-User Devices: Information Technology system operated by users; e.g. Desktop and Laptop computers, Mobile phones, tablets, etc.

Information security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Service: A collection of information technology systems through which a user can access, manipulate, or create campus assets.

Information Technology (IT) Resources: Anything that generates, stores, processes or transmits electronic information. This includes end-user devices and information technology systems.

Information Technology System: A subset of information technology resources that collectively provide an information service to end-user devices.

Institutional Information: Any information, regardless of medium, in the furtherance of the campus mission, excluding research data.

Institutional Information and Research Data Categorization: The exercise of mapping data to the appropriate security categories as identified in FIPS-199.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of *integrity* is the unauthorized modification or destruction of information.

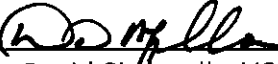
Network: A group of *information technology resources* and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

Research Data: All recorded information, regardless of medium, and all actual samples or examples, that were created or gathered and that could serve to influence or support a research finding or conclusion. Data does not include such items as research papers cited by the researcher, preliminary notes or manuscripts, reviews, or related communications, or items that are already the property of others. This definition is intended to characterize current research norms, not to modify them.


Service Security Plan: Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

User: A person who accesses, manages, or manipulates institutional information, research data, or information technology resources. This definition includes, but is not limited to, all faculty, students, staff, contractors, visiting researchers, or guests and volunteers.

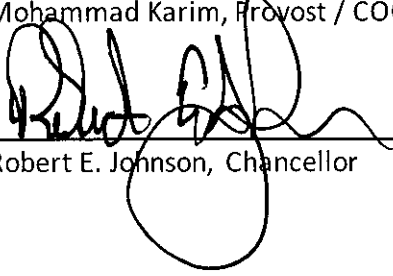
VII. Approval

Approved:  _____ Date: 11/7/19

David Gingerella, VCAF

Approved:  _____ Date: 11-14-2019

Dr. Mohammad Karim, Provost / COO

Approved:  _____ Date: 11/8/19

Dr. Robert E. Johnson, Chancellor