OFFICE OF COMPLIANCE SERVICES
UVM.EDU/POLICIES

POLICY

FOR PRINTED USE ONLY

Policies residing on UVM's Institutional Policy website are the most current versions available. If you are viewing a policy anywhere else including in printed form or embedded on other websites, it may not be the most current.

Title: Information Security

Policy Statement

The Information Security Program at the University of Vermont exists to protect and promote the University's sustainability as a premier institution of higher education by maintaining the confidentiality, integrity, and availability of University information resources. Compliance with this policy prevents material harm to the University's operations or reputation due to a breach of those resources. This policy and the Information Security Procedures, in concert with other applicable University Policies and Procedures, ensure compliance with regulations that govern the collection, access, use, disclosure, and protection of University-owned or -managed information.

Reason for the Policy

Information Technology is critical to the cultivation of a culture of innovation and openness at the University. This policy seeks to enable the principles of Our Common Ground to flourish by ensuring the continuity of business operations, the security of personal information entrusted to the University by students, faculty, staff, and other constituents, and the protection of intellectual property.

Because of its prominence in the public sphere, relationships with government or other entities, and the monetary value of its information assets, the University is a target for those who wish to profit from access to its resources or to harm its reputation or operations. This policy mitigates that institutional risk by safeguarding the information resources entrusted to the University. It supports those goals by providing a framework for consistent, security-informed business practices and by engaging all University constituents in the Information Security Program.

Applicability of the Policy

All members of the University community including, without limitation, individuals who are faculty, staff, students, contractors, consultants, temporary employees, and affiliates of the University.

Definitions

Authorized Users: Any individual who has been issued a UVM NetID (or other access account) and are authorized to access specific information resources to perform business functions for the University or conduct business with the University.

Data Destruction: Any physical, chemical, or electronic process that alters magnetic, electronic, paper, CD, DVD, or other forms of data storage in a manner that renders the data permanently and irretrievably unreadable.

Communications Behavior: the actions, habits, and practices of individuals when using communication channels and technologies to transmit, receive, process, or store information. This includes behaviors such as:

- Email usage: How people send, receive, and manage emails.
- Social media interactions: How users engage with online platforms.
- Messaging apps: How individuals communicate using instant messaging services.
- File sharing: How data is transferred between devices or systems.
- Cloud storage: How information is stored and accessed remotely.

Data Stewards: Members of the University community who have the operational responsibility for discrete collections of non-public protected data (NPPD) as defined in UVM's Privacy Policy.

Multifactor Authentication (MFA): a method of authentication that requires a user to provide two or more credentials to verify their identity, which may include a known credential (such as a password), personal details, a known device (such as a computer or mobile device), or a hardware or software token.

NetID or Network Account: The electronic identity managed by Enterprise Technology Services (ETS) that is provided for each member of the University community to access University Information Systems, including internal electronic information services..

Non-Public Protected Data (NPPD): As defined in UVM's Privacy Policy.

Public information: Information that may be disclosed to any person inside or outside the University. Although such information may be made public, precautions may still be required to protect against unauthorized or malicious modification or destruction. Further elaboration on public information may be found in the Privacy Policy.

Technology Managers: Individuals who develop, implement, or maintain information systems or who have privileged access to information technology systems such as servers, networking equipment, and personal workstations in order to manage or support those systems, whether those systems are housed in UVM facilities or hosted externally.

University Employees: Student employees, staff, faculty, contractors, consultants, temporary employees and affiliates of the University of Vermont.

University Information: Information in any form and recorded on any media that the University or its agents use or create in the course of conducting University business, including research and teaching activities, except those materials specifically excluded from University ownership as set forth in the University's Intellectual Property Policy.

University Information Systems: Electronic or physical University or externally-hosted systems that are used to collect, store or transmit information, including, without limitation, email, University-owned computers, communications equipment and software, University network accounts, file cabinets, storage cupboards, and internal mail or delivery systems.

User: An individual who uses University Information or University Information Systems, even if they do not have responsibility for managing institutional resources.

Procedures

1. Accountability and Compliance

Members of the University community that access University Information are responsible and accountable for ensuring that they are acting in accordance with university policies and procedures that govern university data. The University may, at its discretion, enforce compliance through technical or non-technical means. Confirmed misuse of university data may result in disciplinary action. Procedures for the investigation of suspected violations, imposition of disciplinary action, and the availability of grievance or appeal claims shall be governed by otherwise applicable University policies, handbooks, and collective bargaining agreements. In certain circumstances criminal penalties may apply.

2. General Responsibilities for all University Community Members

The information security landscape is continuously evolving. As such, the University has structured procedures and system safeguards to protect University information that will also evolve over time. Even with these procedures and safeguards, members of the University community must be diligent in using university data only as authorized for the purposes of their job duties and for safeguarding university data, especially NPPD, from unauthorized distribution, interception, or access. Therefore, all members of the University community must:

(a) Ensure that university data only be accessed, transmitted, processed, and stored in accordance with university policies and procedures. Examples include implementing University multifactor authentication, following appropriate communications behavior when exchanging NPPD, using encryption, or ensuring physical storage requirements;
(b) Prohibit certain activities to divulge, copy, release, sell, loan, review, alter, or destroy University Information, except as properly authorized;

(c) Restrict access to physical and electronic University Information Systems that are used to contain or transmit University Information, including, without limitation, network security provisions intended to protect the University's network(s);

(d) Safeguard all physical or electronic keys to University Information Systems or University Information, including, without limitation, requirements related to passwords, ID cards, computer/network account or electronic tokens;
(e) Report any knowledge of: (i) activities that may compromise the security of Non-public Protected Data (NPPD) or (ii) evidence of NPPD having been compromised or (iii) activities that could compromise the confidentiality, integrity, or availability of University Information Systems; and
(f) When notified, require users to complete annual training regarding the secure use of information technologies.

3. General Responsibilities for University Employees

University Employees have special responsibilities because of the access they have to University Information and University Information Systems. Each University Employee is expected to know and understand the security requirements of the types of University Information with which they work and to take measures to protect it in accordance with the Procedures. The Procedures detail the protection requirements for different types of information, such as, for example, locking doors and filing cabinets, protecting account passwords, protecting workstations, and securing Confidential Information that may be transmitted.

The University requires that extra precautions be taken when collecting, using, storing, transporting or destroying non-public, Non-public Protected Data (NPPD) as defined in this policy. These extra

precautions are detailed in the Procedures. Every attempt should be made to limit the further circulation or use of this information except where permissible by University policy. The requirements for how this information may be shared are detailed in the Procedures.

4. General Requirement for Data Stewards

Data Stewards have additional responsibilities given their roles as it relates to NPPD in the data collections for which they are accountable. These responsibilities are detailed in the Procedures. While Data Stewards may delegate the day-to-day performance of one or more of these additional responsibilities, they remain ultimately responsible for compliance with this Policy and the Procedures and the requirements specified for the protection of the University Information contained in their Data Collection(s). In general, Data Stewards must:

(a) When notified, complete annual training regarding the roles and responsibilities detailed in the Data Stewardship UOP;
(b) Understand the university's security and other requirements, as well as those requirements contained in any applicable laws, regulations, with which they must comply to maintain the confidentiality, integrity, and availability of their specific data collection;
(c) Convey, in writing, these requirements to the departments that have access to their data collections;
(d) Work with Deans, Directors, and Department Chairs to determine the Authorized Users and an appropriate method of access for each data collection; and
(e) Ensure that contracts with third parties include provisions for maintaining the security of information to which the third party may have access.

5. General Requirements for Technology Managers

Technology Managers support computing and networking environments where University Information is collected, stored, transmitted, or processed. Security requirements for the functional work of Technology Managers are detailed in the Procedures. These include, for example, requirements for the maintenance of secure computing and network environments, routine system backup and encryption procedures, and the management of client workstation security, as applicable. Technology Managers must ensure high level systems integrity and direct that all access used by themselves and technical staff conform to the principle of least privilege.

6. General Responsibilities of Deans, Directors, and Department Chairs

Deans, Directors, and Department Chairs have additional responsibilities because of the supervisory role they have within their units. Deans, Directors and Department Chairs are not only responsible for understanding the security-related requirements of the University Information used within their departments, but must develop internal procedures that support the University's objectives for security, including confidentiality, integrity, and availability of information. These procedures must ensure that:

(a) specific issues related to transmission, storage, destruction, and access within their department are detailed;
(b) staff have the appropriate access to University Information and University Information Systems necessary for the performance of their jobs;
(c) staff do not have access to University Information and University Information Systems where that access is not necessary for them to satisfy the requirements of their jobs;
(d) this access is removed upon their separation from employment; and
(e) written confidentiality agreements are signed as applicable.

The Procedures include templates with standardized language to assist Deans, Directors, and Department Chairs with these requirements. Deans, Directors and Department Chairs are responsible for ensuring that their departmental procedures are communicated to their employees and are being followed.

7. **Legal Requirements**

The University is subject to federal, state, and international laws and regulations and contractual requirements (including, but not limited to, grants and research agreements) governing the security of information. The requirements generally vary according to the type of information being protected.

Agreements with third party vendors or consultants who will have access to confidential information must ensure that the vendor is subject to obligations of confidentiality that will enable the University to continue to comply with its own obligations under applicable laws and regulations.

Contacts

Questions concerning the daily operational interpretation of this policy should be directed to the following (in accordance with the policy elaboration and procedures):	
Title(s)/Department(s):	**Contact Information:**
Information Security Officer	234 Waterman Building 85 South Prospect Street University of Vermont Burlington, Vermont 05405 (802)656-2006 iso@uvm.edu

Related Documents/Policies

- Information Security Procedures
- Code of Conduct and Ethical Standards
- Computer, Communication, and Network Technology Acceptable Use
- Data Breach Notification Policy
- Disposal of Surplus Property and Movable Equipment
- FERPA Rights Disclosure Policy
- Intellectual Property
- Privacy
- Records and Document Requests
- Records Management and Retention Policy
- Subpoenas, Complaints, Warrants and other Legal Documents

Regulatory References/Citations

- Family Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- Gramm-Leach Bliley Act (GLBA) (15 USC § 6801-6809)
- Health Information Technology for Economic and Clinical Health Act (HITECH) of HIPAA (45 CFR Parts160 and 164)
- Health Insurance Portability and Affordability Act (HIPAA) (45 CFR Parts 160, 162 and 164)
- The European Union's General Data Protection Regulations (GDPR)
- Vermont Disclosure of Information Statute (18 V.S.A. § 7103)

- Vermont Protection of Personal Information (62 V.S.A. § 2430)
- Vermont Security Breach Notice Act (9 V.S.A. § 2435)
- Higher Education Act

Training/Education

Training Topic:	Annual Information Security Training (under development)		
Training Audience:	All students and University Employees	**Delivered By:**	Information Security Office
Method of Delivery:	TBD	**Frequency:**	Annual

Training Topic:	Data Steward Training (under development)		
Training Audience:	Data Stewards	**Delivered By:**	Information Security Office
Method of Delivery:	TBD	**Frequency:**	Annual

About this Policy

Responsible Official:	Chief Information Officer	**Approval Authority:**	President
Policy Number:	V. 1.7.3	**Effective Date:**	February 19, 2025
Revision History:	• V. 4.4.2.1 approved on September 8, 2011. • V.4.4.2.2/V.1.7.2 Approved by the President on January 10, 2013 • V.1.7.3 Approved on February 19, 2025		