The University of Vermont

Policy V. 2.20.2

Responsible Official: Dean of University Libraries and Chief Information Officer

Effective Date: January 7, 2013

Information Security

Policy Statement

All members of the University community are required to manage University information in accordance with this Policy and the University Information Security Procedures (the Procedures) made pursuant to it.

The Procedures are incorporated by reference into this Policy. This means that anything included in the Procedures document is to be treated as though it is a part of this Policy and has the same force and effect as this Policy.

Reason for the Policy

This Policy is being adopted in order for the University to maintain the security of its institutional information and information systems, and comply with applicable federal and state laws and regulations.

Applicability of the Policy

This Policy applies to all members of the University community who have access to University Information, including, without limitation, individuals who are faculty, staff, students, contractors, consultants, temporary employees, and affiliates of the University. University community members may have differing rights and responsibilities with respect to University Information. These rights and responsibilities are detailed in the Procedures.

Policy Elaboration

All members of the University community shall comply with the following general principles. The specific way in which these principles are to be applied for any particular community member will depend upon the category or categories in which they are included; however, the general principles will remain constant. These general principles are:

1. **Accountability**
   Those University community members that access University Information are responsible and accountable for ensuring that they are acting in accordance with this Policy and the Procedures. Noncompliance with the provisions of this Policy and the Procedures may result in disciplinary action, up to and including dismissal, expulsion, or severance of contract. In certain circumstance, criminal penalties may apply.

2. **General Responsibilities for all University Community Members**
   The University will structure procedures and system safeguards to protect University information, but members of the University community must be diligent in their own use of it.

   This means that, in accordance with the provisions articulated in this Policy and the Procedures, community members are responsible for their use or misuse of University Information and must protect the foregoing from unauthorized distribution, interception or access. Therefore, all members of the University community must comply with provisions in the Procedures that:

   (a) Establish criteria for the secure transport and storage of University Information, including, for example, University encryption requirements or 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) Require them to 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; and
   (e) Require them to report their knowledge of: (i) activities that may compromise the security of Personally Identifiable Information or (ii) evidence of Personally Identifiable Information having been compromised.

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, Protected University Information 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 responsibilities, in addition to those of other University Employees, because of the Protected University Information contained 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 will 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) Understand the security and other requirements contained within this Policy and the Procedures, as well as contained in any applicable laws, regulation or University Policies, that they must comply with in order to maintain the confidentiality, integrity, and availability of their specific Data Collection;
(b) Convey, in writing, these specific requirements to the departments that have access to their Data Collections;
(c) Work with Deans, Directors and Department Chairs to determine the Users authorized to access the Data Collections and in what manner that access can take place;
(d) 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. Requirements related to how Technology Managers must perform their function are detailed in the Procedures. These requirements include, for example, how to maintain security on their systems and networks, perform routine system backups, and manage client workstation security, as applicable.

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 departments. 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 departmental procedures, consistent with this Policy and the Procedures, that support the University's objectives for security, integrity, and availability of information. Amongst other things, these procedures must ensure that, in compliance with the University Procedures: specific issues related to transportation, storage, destruction and access within their department are detailed, staff have the appropriate access to University Information and University Information Systems necessary for the performance of their jobs and this access is removed upon their separation from employment, and written confidentiality agreements are entered into as required. In order to assist Deans, Directors and Department Chairs in creating these procedures, templates of standardized language that will require some customization have been included within the Procedures.

Finally, 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 a number of federal and state laws and regulations governing the security of information. The requirements generally vary according to the type of information being protected. Compliance with these laws and regulations is required by this Policy and the Procedures and University members are responsible for this compliance.

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.

Definitions

Protected University Information includes both Protected Personal Data and Sensitive University Information as defined below:

- ***Protected Personal Data (PPD)*** includes, without limitation, personally identifiable information, protected health information, and protected student information as described below. Protected University Data includes data maintained in any electronic or hard copy medium. *Note*: Potential breaches of Protected Personal Data (PPD) must be reported in accordance with the Data Breach Notification Protocol (http://www.uvm.edu/policies/general_html/databreach.pdf).
    - *Personally Identifiable Information (PII)* – under 9 V.S.A. §2430(5) is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized person:
        - Social Security number;
        - Motor vehicle operator's license number or non-driver identification card number;
        - Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
        - Account passwords or personal identification numbers or other access codes for a financial account.
    - *Protected Health Information (PHI)* – includes identifiable health information as defined at 45 CFR §160.103 that is transmitted or maintained by the University's covered HIPAA components; PHI also includes identifiable health information that is obtained by a University member pursuant to an agreement with another organization or governmental entity and which is protected under the HIPAA/HITECH Act.

    - *Protected Student Information* – Student education records maintained by the University, whether by academic or administrative units, and protected under the

Family Educational Rights and Privacy Act (FERPA) and as described more fully in the UVM FERPA Rights Disclosure policy (http://www.uvm.edu/policies/student/ferpa.pdf).

- ***Sensitive University Information*** about the University, or University property or information regarding individuals not identified as PPD, that includes, without limitation, information involving certain legal matters, or business and financial transactions, grant applications, pending patent applications, institutional electronic security architecture, and information about security breaches or other events.

Authorized Users: Individuals – faculty, students, staff, or affiliates – who have been issued a UVM NetID and are authorized to access specific information resources in order to perform business functions for the University or in order to 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.

Data Stewards: Members of the University community who have the operational responsibility for particular collections of information such as student, employee, or alumni records (collection(s)).

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

Password: A carefully constructed confidential character string used to validate individuals for access to University Information Systems, specifically, network accounts.

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.

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 development on 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

The Information Security University Operating Procedures, and any specific Data Steward, Technology Manager or departmental procedures, provide additional detail and describe the procedures to be followed to implement this Policy.

Forms

None

Contacts/Responsible Official

Questions related to the daily operational interpretation of this policy should be directed to the individuals listed below.

For questions related to Information Security:

Chief Information Officer
234 Waterman Building
85 S. Prospect Street
University of Vermont
Burlington, Vermont 05405
(802) 656-4900
email: cio@uvm.edu

The Dean of University Libraries and Chief Information Officer is the UVM official responsible for interpretation and administration of this policy.

Related Documents/Policies

Information Security Procedures
http://www.uvm.edu/policies/cit/infosecurityprocedures.pdf
Code of Conduct and Ethical Standards
http://www.uvm.edu/~uvmppg/ppg/general_html/businessconduct.pdf
Computer, Communication, and Network Technology Acceptable Use
http://www.uvm.edu/policies/cit/compuse.pdf
Data Breach Notification Policy
http://www.uvm.edu/policies/general_html/databreach.pdf
Disposal of Surplus Property and Movable Equipment
http://www.uvm.edu/policies/facil/surplusdisposal.pdf

FERPA Rights Disclosure Policy
http://www.uvm.edu/~uvmppg/ppg/student/ferpa.pdf
Intellectual Property
http://www.uvm.edu/~uvmppg/ppg/general_html/intellectualproperty.pdf
Privacy
http://www.uvm.edu/policies/general_html/privacy.pdf
Records and Document Requests
http://www.uvm.edu/~uvmppg/ppg/general_html/record_request.pdf
Records Retention
http://www.uvm.edu/~uvmppg/ppg/general_html/recordretention.pdf
Subpoenas, Complaints, Warrants and other Legal Documents
http://www.uvm.edu/policies/general_html/subpoenas.pdf
University Sponsored Social Media
http://www.uvm.edu/policies/cit/socialmedia.pdf

Effective Date

Approved by the President on January 10, 2013.