University of Vermont

OFFICE OF COMPLIANCE SERVICES
UVM.EDU/POLICIES

POLICY

FOR PRINTED USE ONLY

Title: Data Breach Notification

Policy Statement

The University of Vermont will investigate and provide notice of information security breaches to affected individuals and/or Federal and State agencies in accordance with applicable Federal and State requirements.

Reason for the Policy

This Policy defines the steps that personnel must use to ensure that information security incidents are identified, contained, investigated, and remedied. It also provides a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. Finally, it establishes responsibility and accountability for all steps in the process of addressing information security incidents.

Applicability of the Policy

This Policy applies to all users of Protected Personal Data (PPD), whether faculty, staff, student, contractor, consultant, or agent thereof. This Policy further applies to any computing or data storing devices owned or leased by the University that experience a Security Incident, as well as any computing or data storing device, regardless of ownership, which is used to store Protected Personal Data, or which, if lost, stolen, or compromised, and based on its privileged access, could lead to the unauthorized disclosure of Protected Personal Data.

Definitions

Notification: the act of informing persons affected by a breach of Protected Personal Data (PPD) that their information was included in the breach and the steps they can take to protect themselves and their privacy. Notification also includes required noticing to federal and state agencies. Notification to affected individuals will be overseen by Chief Privacy Officer, and depending on the data breached, may include the following components:

1. A general description of the unauthorized access or acquisition;
2. The type of personal information affected;
3. A general description of the steps the University will take to protect the information from further unauthorized access or acquisition;

4. Instructions and necessary information for notifying the major credit agencies of suspected or potential identity theft as needed; and

5. A toll free number to obtain more information and resources.

Non-Public Protected Data (NPPD): for the purpose of this Policy will be the same as the definition found in UVM's Privacy Policy.

Protected Personal Data (PPD): includes, without limitation, any NPPD relating to an identified or identifiable natural person.

Security Breach:

1. The unauthorized acquisition of **electronic** data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the confidentiality, integrity and availability of PII as defined by the State of Vermont's Security Breach Notice Act (9 V.S.A. §2430(9))(or any other applicable similar state law) maintained by the University of Vermont**;**

2. The unauthorized acquisition of- or a reasonable belief of an unauthorized acquisition of login credentials issued by the University of Vermont that compromises the security, confidentiality, or integrity of PII maintained by the University of Vermont as defined in (1) above;

3. A breach of unsecured protected health information, regardless of the form and format of the information (i.e., electronic, paper) in accordance with the HIPAA Breach Notification rule, 45 CFR § 164.402 and HITECH Act (P.L. 111-5, § 13407); or

4. An unauthorized acquisition or reasonable belief of an unauthorized acquisition of NPPD or login credentials that University management determines to merit notification to affected persons notwithstanding the lack of regulatory obligation to do so.

Security Incident: An event that a User has reason to believe may have encompassed a Security Breach.

User: Any user of NPPD, including any faculty, staff, consultant, contractor, student, or agent thereof.

Procedures

Identifying and Reporting Security Incidents

1. In the event that a User detects a suspected Security Breach, the User must report the Security Incident to the UVM Information Security and Assistance Line at 802-656-2123, toll-free at 866-236-5752, or by email to ISO@uvm.edu. The User will be asked to provide the following information:

    - User contact information
    - Name(s) of University Department(s) involved
    - A brief description of what happened
    - A general description of the NPPD affected

As directed by the Information Security Officer (ISO) or their designee (herein referred to as the Incident Handler or IH), the reporter shall follow instructions regarding preserving evidence. The Incident Handler shall activate the Computer Security Incident Response Team (CSIRT) to advise on- and assist in addressing technical aspects of securing data.

Security Incident Protocol

1. The IH will notify the Chief Privacy Officer (CPO) of the Security Incident, log the incident, and initiate evaluation.

2. The evaluation process shall include:

    a. Establishing the scope of the Incident,

    b. Securing the Data,

    c. Preserving evidence, and

    d. Contacting Law Enforcement, if appropriate.

3. Once the IH has completed the initial evaluation, the IH shall communicate the results to the CPO.

4. The CPO in coordination with the Office of General Counsel (OGC) will make a determination regarding whether a Security Breach has occurred and the type of NPPD involved. See "Guidance for Data Breach Determination and Notice."

5. If it is determined that a Security Breach *did* occur:

    a. The CPO will notify the University Communications Office, and, as deemed appropriate, brief the Office of Federal, State and Community Relations, and executive management.

    b. If it is determined that the Security Breach included PPD, the CPO will advise the University Department where the breach occurred regarding the required form of notice, if any, to be sent to the affected individuals or business associates, if applicable. The University Department shall inform the CPO of the existence of any business associate agreement.

        i. If notice is required, the University Department that was responsible for maintaining the breached information will be responsible, in consultation with the CPO, for noticing affected individuals or business associates. The affected University Department is responsible for expenses related to the breach.

    c. The CPO, in consultation with the OGC, shall notify any governmental entity, as required, of the breach, or shall ask the University Department to do so.

    d. The ISO will make recommendations to the University Department(s) to correct or improve information security practices that may have led to the incident.

6. If it is determined a security breach *did not* occur, the ISO will, when appropriate, make remedial suggestions to the User and/or University Department(s) to correct or improve information security practices that may have led to the incident.

Notice Requirements

Depending on the determination, UVM will take one of the following next steps:

- If GDPR covered PD was breached and notification is required or merited, affected individuals shall receive a notice of the incident, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement agencies.
- If PII as defined under VT law or if login credentials were breached, affected individuals must be provided notice in accordance with legal requirements.
- If HIPAA covered PHI was breached, affected individuals must be provided notice without unreasonable delay and in no case later than 60 days from discovery of the breach.

The method of noticing a breach may vary dependent on the number of individuals affected, the cost of noticing, and the normal means of communication with affected individuals, but in all instances as guided by the applicable legal requirements.

UVM may outsource some or all of the breach notification requirements depending on the nature and extent of the breach.

Documentation

The University will document all reported information security incidents. Documentation responsibilities include:

ISO

- Log of incidents received
- The evaluation process and outcome of the evaluation
- Recommended corrective action to contain the incident and prevent future incidents

CPO

- Breach determination outcome
- Identification of Responsible Department
- Documentation of notice made to affected individuals, Federal offices, State offices, and business associates, where applicable

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:**
Chief Privacy Officer	privacy@uvm.edu
Information Security Officer	iso@uvm.edu

Forms/Flowcharts/Diagrams

- None

Related Documents/Policies

- Computer, Communication and Network Technology Acceptable Use Policy
- Disposal of Surplus Property and Movable Equipment Policy

- Guidance for Data Breach Determination and Notice
- Information Security Policy
- Privacy Policy

Regulatory References/Citations

- None

Training/Education

Training will be provided on an as-needed basis as determined by the Approval Authority or the Responsible Official.

About this Policy

Responsible Official:	Chief Privacy Officer	**Approval Authority:**	President
Policy Number:	V. 9.1.2	**Effective Date:**	July 1, 2020
Revision History:	• V. 9.1.1/V. 9.0.2.1 effective April 6, 2011 • July 23, 2016 • September 4, 2020		