The University of Vermont

Policy V.9.1.2

Responsible Official: Chief Privacy Officer

Effective Date: July 23, 2016

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.

Policy Elaboration

See Procedures.

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 Services, 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.

Protected Personal Data (PPD): includes, without limitation, personally identifiable information (PII), protected health information (PHI), and protected student information (PSI) as described below. PPD includes data maintained in any electronic or hard copy medium.

- *Personally Identifiable Information (PII)* – under 9 V.S.A. §2430(5)(A) 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)* – 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 (PSI)* – 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)*.

Security Breach:

1. The unauthorized acquisition of **electronic** data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of PII maintained by the University of Vermont as defined by the State of Vermont's

Security Breach Notice Act (9 V.S.A. §2430(8))(or any other applicable similar state law)**;**

2. 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
3. An unauthorized acquisition or reasonable belief of an unauthorized acquisition of PII or PSI 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 be a Security Breach.

User: Any user of PPD, 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 Protected Personal Data affected

    As directed by the ISO, the reporter shall follow instructions regarding securing data and preserving evidence.

Security Incident Protocol

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

2. The evaluation process shall include:
    a. Securing the Data,
    b. Preserving evidence,
    c. Contacting Law Enforcement, if appropriate, and
    d. Establishing the scope of the Incident.

3. Once the ISO has completed the initial evaluation, the ISO 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 PPD 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. The CPO will advise the University Department where the breach occurred regarding the required form of notice 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 associates agreement.
    c. 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.
    d. 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.
    e. 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 PPD 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 was breached, affected individuals must be provided notice in accordance with legal requirements.

- If 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 of PPD 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

Forms

None

Contacts

Questions related to the daily operational interpretation of this policy should be directed to the:

Chief Information Officer, Chief Privacy Officer and Dean of University Libraries
(802) 656-2003

The Chief Privacy Officer is the official responsible for the interpretation and administration of this policy.

Related Documents/Policies

Computer, Communication and Network Technology Acceptable Use Policy
http://www.uvm.edu/policies/cit/compuse.pdf
Disposal of Surplus Property and Movable Equipment Policy
http://www.uvm.edu/policies/facil/surplusdisposal.pdf
Enterprise Technology Services – Information Security Information
https://www.uvm.edu/it/security/
Guidance for Data Breach Determination and Notice
http://www.uvm.edu/policies/general_html/databreach_guide.pdf
Information Security Policy
http://www.uvm.edu/policies/cit/infosecurity.pdf
Privacy Policy
http://www.uvm.edu/policies/general_html/privacy.pdf

Effective Date

Approved by the President July 23, 2016