OFFICE OF COMPLIANCE SERVICES
UVM.EDU/POLICIES

POLICY

FOR PRINTED USE ONLY

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(8) (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.

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(s) 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. 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

- 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 to9 (orre)1 (c)0.83-0.6 -0.003 Tw 1.198 0r Tw -14.1(e)7 (e)1 ( ) (t)1.7ow (on

- 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		