Title	Policy ID:
VSC Incident Response Policy	**612-1**
	Version: **2.0** / Date: **2018/12/05**

1. Purpose

1.1. This policy is designed to ensure a timely response to data security incidents, to improve incident reporting and related communications, to mitigate any damages caused by incidents, and to improve overall data security systems. It establishes guidelines and procedures for appropriate responses to incidents that threaten the confidentiality, integrity, and/or availability of information assets, information systems, and/or the networks that deliver the information.

1.2. If this incident is part of a larger crisis, please contact the VSC Crisis Management Team at crisismanagment@vsc.edu.

2. Scope

2.1. This policy applies to all technology systems, services, and technologies used by the Vermont State Colleges.

3. Policy

3.1. DEFINITIONS

Incident

An *incident* is any event that threatens the confidentiality, integrity, or availability of VSC information assets (electronic or paper), information systems, and/or the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident.

Incidents may include but are not limited to:

- Unauthorized entry
- Security breach or potential security breach
- Unauthorized scan or probe
- Denial of service
- Malicious code or virus
- Violations of the VSC Computing and Telecommunications Conditions of Use Policy
- Networking system failure (widespread)

- Application or database failure (widespread)
- Others as defined by incident response teams

Incidents may be identified through a variety of means, such as reports from users, alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.

Security Breach

A *security breach* is the unauthorized acquisition or access of computerized data that compromises the security, confidentiality or integrity of personal information. Security breach does not include good faith but unauthorized acquisition or access of protected information by an employee for a legitimate business purpose. All data security breaches require notification to the Vermont Attorney General's Office.

Protected Information

Protected information at the VSC is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." (Definition of PII from NIST 800-122) It is all information protected by FERPA, the Vermont Public Records Act or other legal provisions. Any information not discretely listed as Public information in the VSC Information Sensitivity policy, it should be considered protected information.

For more detailed information, see the VSC Information Sensitivity policy.

Critical Incidents

Critical incidents are defined as high impact and high risk; these include known or suspected security breaches, and the known or suspected compromise of institutional protected information to individuals or entities outside the VSC or to individuals or entities inside the VSC without authorization. Critical incidents require the development and implementation of a formal incident response action plan by the Incident Response Team. For the purpose of this policy any incidents involving information considered protected information according to the VSC Information Sensitivity policy should be treated as critical incidents.

Non-critical Incidents

Non-critical incidents are defined as medium, low or no risk; these may include good faith but unauthorized acquisition or access of protected information by an employee for a legitimate business purpose, breaches involving encrypted data, unauthorized scans or probes, or other noncritical or minor issues. Non-critical incidents do not require a formal incident response action plan but must have an appropriate response, as determined by the Chancellor/ designee and Chief Information Officer (CIO) for system incidents, or the College President/ designee and Chief Technology Officer (CTO) for college incidents.

Incident Declaration

An incident is declared to be critical in one of the following ways:

- The Chancellor or designee, or College President or designee, declares an incident to be critical.

- The CIO of the VSC or the CTO at the College, or designee, in consultation with the Chancellor or College President or designee, declares an incident to be critical.

3.2. ROLES AND RESPONSIBILITIES

Incident Response Teams will be established at each college and for the system. Participation by individual members may vary by incident as appropriate. Members may also appoint a designee in their absence. Members of Incident Response Teams are expected to respond immediately and fully when called upon. Responding to a critical incident, in general, takes precedence over all other work. If a member is unavailable at the time the team is assembled, a substitute member may be named by the chair or executive leadership. Incident Response Team members will receive periodic training to ensure all members are prepared to identify and efficiently respond to a potential incident.

The CIO of the VSC, or designee, is available on a 24/7 basis for incident response coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical intrusion detection system alerts, and/or reports of unauthorized critical system or content file changes.

If this incident is part of a larger crisis, please contact the VSC Crisis Management Team at crisismanagment@vsc.edu.

3.3. PROCEDURES

Upon discovery or suspicion of an incident, VSC employees shall notify IT Services in a prompt and effective manner through a submission to the Help Desk and a phone call directly to the CIO of the VSC or the CTO at the College. The CIO of the VSC or designee can be contacted at 802-224-3016.

If this incident involves credit cards or card holder data, please use the 612-2 VSC Payment Card Incident Response Policy to proceed.

Upon receipt of notification or suspicion of an incident, the risk should be mitigated. As soon as possible contact the Incident Response Team to begin an investigation. The Incident Response Team will keep a log of all activity related to the investigation.

As quickly as possible, the Incident Response Team, in consultation with the Chancellor and College President, will determine whether the incident is critical or non-critical, and whether the incident is suspected to be or is a security breach.

Within three business days, unless an extension is granted by the Chancellor or CIO, the Incident Response Team must complete an investigation of the incident and prepare their findings in accordance with the procedures laid out below.

If the incident is determined to be non-critical, public notice of the incident is not required, but an appropriate response will be determined by the Chancellor and CIO, or College President and CTO in consultation with the Chancellor. The response may include a change in policy or practice, required training, targeted communications, or further inquiry. The VSC CIO or the

College President and CTO will submit to the Chancellor a brief description of the incident and the rationale for determining it to be non-critical.

Incidents involving a security breach can be deemed non-critical if the Critical Response Team, in consultation with the Chancellor or College President, determines that the misuse of relevant data is not reasonably possible. In this case, the CIO or CTO, in consultation with legal counsel, shall provide a detailed explanation of the determination to the Attorney General's Office within 10 business days of the breach. The explanation shall be provided to the following:

> Consumer Protection Unit, Vermont Attorney General's Office
> 109 State Street
> Montpelier, Vermont 05609

A post-incident analysis will also be performed, either by a group from a different area within the VSC (different college or department) or by a third party, to provide feedback to the Incident Response Team regarding their response. This will help ensure proper procedure is followed and improve future responses.

The procedures for a non-critical incident end at this step.

If the incident is determined to be critical, the Incident Response Team will follow all remaining procedures. The team will review the incident, create an overall action plan and formulate an appropriate college or system response. This response may include but is not limited to:

- Assuming control of and containing the incident
- Involving appropriate personnel
- Conducting a thorough investigation of the incident, including:
    - establishing controls for the proper collection and handling of evidence
    - keeping a log of all communications and actions related to the incident
- Determining whether or not to involve outside personnel, such as law enforcement or computer forensic experts
- Drafting statements and materials for public notice as required by state law, including posting an incident report on the VSC portal
- Executing a remediation plan, possibly including repairing/ rebuilding any damaged systems and considering any additional remedies for affected constituents
- Recommending any change in policy or practice, required training, targeted communications or further inquiry
- Monitoring and revising the action plan as needed in the period directly following the incident
- Discussing, reviewing and documenting all actions and results, particularly any lessons learned from the security breach

If the critical response team suspects or determines a critical incident is a security breach, with the reasonable possibility of the misuse of protected information (as outlined in policy 627-1 the VSC Information Sensitivity policy), the CIO or CTO, in consultation with legal counsel, shall:

- Notify law enforcement to determine any next steps:

State Police Bureau of Criminal Investigation: 802-244-8781

Burlington FBI office during normal business hours: 802-863-6316

Albany FBI office after normal business hours: 518-465-7551

- Notify the Vermont Attorney General's Office at (802) 828-3171

Within four business days of receipt of notification, unless authorized for extended review by the Chancellor or College President, or unless a delay in notification is requested by law enforcement, the Incident Response Team will confirm with executive leadership at the College and the Chancellor's Office a preliminary course of action; the Chair of the VSC Board of Trustees will be notified of the incident and action plan.

In accordance with Vermont law, where there has been a security breach, the Incident Response Team will notify affected constituents without unreasonable delay, generally within seven business days of receipt of notification. Notice will include a description of the following:

- The incident
- The type of personal information that was subject to the unauthorized access or acquisition
- The acts of the college/ system to protect the personal information from further unauthorized access or acquisition
- A toll-free number that constituents may call for further information and assistance
- Advice that directs the constituents to remain vigilant by reviewing account statements and monitoring free credit reports

Notice may be provided by one of the following methods:

- Direct notice to the constituent's residence
- Telephonic notice directly with the constituent and not through a prerecorded message
- Electronic notice if address or phone information is not available, electronic notice cannot request personal information and must conspicuously warn constituents not to provide personal information in response to electronic communications regarding security breaches.

Vermont law allows for substitute notice if the number of potentially affected constituents is greater than 5000 or the cost to notify constituents will be greater than $5000 or if the institution does not have sufficient contact information. Substitute notice must include:

- A conspicuous posting of the notice on the VSC portal, and VSC and college websites
- Notification to major statewide and regional media.

Substitute notice must be authorized by VSC legal counsel.

In the event of notification to more than 1000 constituents, Vermont law requires notice to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

The Incident Response Team will conduct a post-incident critique and submit a summary report to the Chancellor including:

- A description of the incident
- A summary of lessons learned
- Suggested changes to existing policies or procedures
- Recommendations to protect against future incidents

A post incident analysis will also be performed, either by a group from a different area within the VSC (different college or department) or by a third party, to provide feedback to the Incident Response Team regarding their response. This will help ensure proper procedure is followed and improve future responses.

Any disciplinary action considered in association with a critical incident shall follow procedures set forth in the relevant employee collective bargaining agreement or, in the case of employees not covered by a collective bargaining agreement, the VSC personnel handbook.

4. References

9 V.S.A. §2430 (Definitions)

9 V.S.A. §2435 (Notification of Breach)

VSC Policy 414: Computing and Telecommunications Conditions of Use

Vermont Attorney General Security Breach Notification Guidance April 2007

For sample policies, procedures and communications templates, see: http://www.educause.edu/DataIncidentNotificationToolkit/9320

VSC Crisis Management Teams

627-1_VSC_Information_Sensitivity_Policy

5. Definitions

5.1. VSC – Vermont State Colleges

6. Revisions

Date	Revision	Approval	Signature
2018/09/11	Revised		G. Malinowski
2018/10/22	Final Revision	Kevin Conroy	
2018/12/05	Approval	Kevin Conroy	Kevin Conroy