VSC INFORMATION TECHNOLOGY SERVICES

Data Security Incident Response Policy

PURPOSE

This policy is designed to improve the response time 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.

POLICY

This policy establishes guidelines and procedures to provide the basis for appropriate responses to incidents that threaten the security, confidentiality, integrity, and/or availability of information assets, information systems, and/or the networks that deliver the information. The Data Security Incident Response Policy will be reviewed and tested at least annually, then updated to incorporate lessons learned as necessary.

Each college and the system will maintain a trained Critical Incident Response Team to manage security incidents that occur in the VSC.

GUIDELINES AND DEFINITIONS

This policy applies to VSC Information Technology Services and all systems and services for which it is responsible.

An *incident* is any event that threatens the security, 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

Other violations of the VSC Computing and Telecommunications Conditions of Use Policy

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

Incidents such as those listed above vary in their impact on the VSC and in the degree of risk and vulnerability they pose.

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

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 personal information by an employee for a legitimate business purpose.

For the purpose of this policy, and in accordance with state law, *personal information* means 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 persons:

- Social Security number;
- Motor vehicle operator's license number or non-driver identification card;
- 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.

Personal information does not include information that is made available to the general public as a result of state or federal law.

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 Critical Incident Response Team.

Non-critical incidents are defined as medium, low or no risk; these may include good faith but unauthorized acquisition or access of personal information by an employee for a legitimate business purpose, breaches involving encrypted data, unauthorized scans or probes, or other non-critical 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. Non-critical incidents involving security breaches require notification to the Vermont Attorney General's Office even though the misuse of personal information is determined to be not reasonably possible.

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.

ROLES AND RESPONSIBILITIES

Critical Incident Response Teams will be established at each college and for the system; the membership of each of these teams is documented in the "VSC Crisis Management Teams" document. Overall membership will include:

- Executive leadership
- Legal counsel (for the Chancellor's Office team and overall consultation)
- IT leadership
- Communications personnel
- Facilities personnel
- Safety personnel

Participation by individual members may vary by incident as appropriate. Members of critical 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. Critical 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 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.

PROCEDURES

1. 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 or through 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 802-224-3025 on a 24/7 basis.
2. Within four business hours of receipt of notification or suspicion of an incident, the CIO or CTO (or her/ his designee in the case of absence) will consult with the Chancellor/ designee and College President/ designee; remove the risk, if possible; and begin an investigation of the incident, including notification to the critical incident response team. The CIO or CTO will keep a log of all activity related to the investigation.

3. Within three business days of receipt of notification, the critical incident response team, in consultation with the Chancellor/designee and College President/designee, will determine whether the incident is critical or non-critical, and whether the incident is suspected to be or is a security breach.
4. If the critical response team suspects or determines that a security breach has occurred, with the reasonable possibility of the misuse of personal information, 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
     or
     Burlington FBI office during normal business hours
     802-863-6316
     or
     Albany FBI office after normal business hours
     518-465-7551

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

   - Notify the payment card brands as follows:
     Visa Fraud Investigations and Incident Management group at (650) 432-2978

     MasterCard Compromised Account Team
     http://www.mastercard.us/merchants/security/data-security-rules.html

     American Express: Third Party Processor Relationship Manager
     or call (800) 528-5200 immediately

     Discover: notify Discover Network Security at 1-800-347-3083

5. *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/ designee and CIO, or College President/ designee and CTO in consultation with the Chancellor/ designee. The response may include a change in policy or practice, required training, targeted communications or further inquiry. Upon request, 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.

If the incident involves a security breach it can be deemed non-critical if the Critical Response Team, in consultation with the Chancellor/ designee or College President/ designee, determines that the misuse of personal information is not reasonably possible. In this case, the Chief Information Office or Chief Technology Officer, 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 10609-1001

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

6. *If the incident is determined to be critical*, the Critical 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, as conditions require;
   - Conducting a thorough investigation of the incident, including establishing controls for the proper collection and handling of evidence, and 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, and particularly any lessons learned from the security breach.

7. Within four business days of receipt of notification, unless authorized for extended review by the Chancellor, College President or designee, or unless a delay in notification is requested by law enforcement, the critical 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.

8. In accordance with Vermont law, where there has been a security breach, the critical 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 in general terms;
   - the type of personal information that was subject to the unauthorized access or acquisition;
   - the general 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; or
   - 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, and
   - 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.

9. The Critical 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
   - any suggested changes to existing policies or procedures
   - any recommendations to protect against future incidents

10. 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.

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

Approved by/on:	**Council of Presidents 05/15/07**
Amended:	**4/28/09, 11/13/13**
Reviewed:	**2/23/10 by IT Council**