VIRGINIA COMMONWEALTH UNIVERSITY

VCU

Information Security Incident Response Standard

Responsible Office: VCU Technology Services, Information Security
Initial Standard Approved: 11/14/2016
Current Revision Approved: 11/14/2016

Standard Statement and Purpose

In order to effectively and consistently identify, classify, and respond to information security incidents, Virginia Commonwealth University will define and maintain a set of information security incident response processes and procedures. This Information Security Incident Response Standard delineates the general requirements for monitoring, handling, and response to information security incidents, and the roles and responsibilities of all parties involved in the process.

This Standard should be used in conjunction with the documents listed in the Related Documents section.

Noncompliance with this standard may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Standard 1
Definitions 2
Contacts 3
Standard Specifics and Procedures 3
Forms 5
Related Documents 5
Revision History 5
FAQs 5

Who Should Know This Standard

All persons responsible for the technical and management support of systems should read and this Standard and familiarizing themselves with its contents and provisions.

Definitions

Data Custodian
The Data Custodians can have both a business and/or technical role, though it is typically considered a business role. The Data custodians are responsible for entering, modifying and maintaining data in the enterprise databases and information systems.

Data Steward
Data stewards are appointed by and report to the data trustees. Data stewards have knowledge of and work in accordance with numerous University rules and policies across the institution, including university policies on information security and privacy. Data stewards are essentially Executive Subject Matter Experts (ESMEs) for the business domains under their authority.

Data Trustee
Data Trustees will carry out plans and policies to implement appropriate data management practices as defined by industry regulations, federal and state statues, and University policies and procedures. Data trustees are high-level employees (e.g., vice presidents, vice provosts, and deans) appointed by and reporting to the President, including but not limited to Provost and Senior Vice President of Academic Affairs, Vice President of Finance, Vice President for Administration, Vice President for Research, or Senior Vice President of Health Sciences.

Federal Information Security Management Act (FISMA)
Federal Information Security Management Act (FISMA) requires the use of the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 as a common security framework for the management of various information belonging to federal government. The framework outlines the expected security controls for information that are rated at the low, moderate, or high level, where each level requires additional controls to be implemented. This regulation can impact the research projects involving federal government data, or projects that are funded by federal government. The moderate and high level controls are a set of minimal baseline set to handle any data with medium to high sensitivity.

Information Security Incident Response
Within the context of this document, information security incident response is an organized approach to addressing and managing the effects of a security breach or attack (also known as an information security incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

Information Security Event
Information Security events are unique and abnormal behaviors exhibited by an information system which may jeopardize the confidentiality, integrity, and availability of the information system or data contained in the information system.

Information Security Incident (Incident)

Information Security incident is an information security event that has jeopardized the confidentiality, integrity, and / or availability of the information system and / or the data contained in the information system. Information Security incidents include but is not limited to

- Unauthorized access to a system or its data
- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

Payment Card Industry Data Security Standard (PCI-DSS)
Payment Card Industry Data Security Standard is a set of comprehensive requirements for enhancing payment card data security. Compliance with the PCI-DSS helps to alleviate vulnerabilities that put cardholder data at risk.

System Administrator
An analyst, engineer, or consultant who implements, manages, and/or operates a system on behalf of the Trustee, Data Steward, and/or Data Custodian.

System Owner
A system owner is an employee with the oversight responsibility for the management of an IT system. The system owner is typically not the administrator managing the system, but rather the departmental business manager and sponsor of the system. The system owner holds the authority to provision, de-provision, or modify the IT system to address specific business needs.

Contacts

VCU Technology Services (Technology Services) officially interprets this Standard. The VCU Information Security Office (Information Security Office) is responsible for obtaining approval through the appropriate governance structures. Questions about this Standard should be directed to the Information Security Office (infosec@vcu.edu).

Standard Specifics and Procedures

A. General Requirements

This sections contains the requirements for all data types and systems.

1. The Information Security Office is responsible for establishment, maintenance and execution of an Information Security Incident Response Plan (IRP). (N16)

- At a minimum, the IRP must include instructions, procedures, and guidance related to:
    1. Preparation
    2. Detection and Investigation
    3. Initial Response
    4. Containment
    5. Eradication and Recovery
    6. Notification

7. Closure and Post-Incident Activity

- IRP is also expected to include the following key points related to incident handling and response:
  1. Procedures for reporting security incidents to authorities
  2. Procedures for handling security incidents in an area
  3. Procedures for handling security incidents involving IT systems.

- The IRP is expected to define personnel roles and responsibilities, including but not limited to information security incident response coordinators, designated information security incident handlers, and information security incident response team composition.

The VCU Information Security Office is responsible for defining incident reporting processes and communicating such processes to data stewards and system owners. Data stewards and system owners are responsible for ensuring the awareness of these processes for their employees, contractors, vendors, and any other personnel who handle VCU systems and / or data (F21)

2. Annual test and review of the information security incident response plan.
The VCU Information Security Office is responsible to coordinate the performance of information security incident response testing on an annual basis, and review and address deficiencies in processes and procedures in plan. (N30)

3. Investigations of incidents or forensic analysis must be directed by the VCU Information Security Office.
All information security related incidents and forensic analyses must be initiated and directed by VCU Information Security Office. Following the discovery of an incident, VCU Information Security Office must be contacted without unreasonable delay. Evidence collection or forensic analyses by individuals outside of VCU Information Security Office is prohibited, unless directed by VCU Information Security Office incident responder. (F25)

B. Category I Information Requirements

In addition to the requirements in the General Requirements Section, Category I data must also adhere to the following requirements:

1. Data breach notification procedures.
If the security incident jeopardizes the confidentiality of Category I information, then the VCU Information Security Office is expected to work with the system owner and data steward to initiate a data breach assessment, and when applicable, response and notification process in accordance with University policies and federal and state regulations. (N17)

2. Notify system administrator of automatic account lockouts.
System administrators must be notified without unreasonable delay of all automatic account lockout events. Acceptable notification methods include email, Short Message Service (SMS), and phone call. If failed logon attempts persist, the system administrator must immediately inform the system owner and Information Security Office. (H23)

C. Special Requirements

The following requirements apply to systems used to handle specific data types; all data types listed in this section are considered Category I data and must also adhere to the requirements listed in the Category I Requirements Section.

1. Designate specific personnel to be available 24 / 7 / 365 to respond to alerts.
Data stewards, data custodians, and system owners must jointly identify data and systems requiring 24 / 7 / 365 monitoring and alerting. The VCU Information Security Office will designate qualified individuals to monitor and respond to alerts. Required for PCI-DSS and FISMA (mod+high). (F23)

Forms

1. VCU Information Security Exception Form

Related Documents

VCU Information Technology Policies are located in the University's Policy Library. The Information Technology Policy Framework contains VCU Information Technology Policies, Standards and Baseline requirements.

1. **Computer Network and Resources Use Policy**
2. **Information Security Policy**
3. **Exposure and Breach of Information Policy**
4. **Data Classification Standard**
5. **Network Management and Security Policy**

Revision History

Approval/Revision Date	*Title*
None – New Standard	

FAQs

There are no FAQs associated with this Standard.