UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-4002	**Policy Title:**	Cybersecurity Incident Response Policy
Effective:	06/29/2020	**Responsible Office:**	Information Services
Date Approved:	06/29/2020	**Approval:**	Vice President for Information Services and Chief Information Officer
Replaces Policy Dated:	07/12/2007	**Responsible University Official:**	Vice President for Information Services and Chief Information Officer

PURPOSE:

This policy outlines the steps personnel must follow as the initial response to a security incident involving the unauthorized access to University systems or data. Reports of data compromises and the exposure of personal or restricted information seem to occur with increasing frequency. The University of Richmond takes great care to safeguard data and privacy; however, if the University experiences such an event, we must be prepared to act quickly.

SCOPE:

This policy applies to the University of Richmond and all of its Affiliates. As used in this policy, the term "Affiliates" means organizations or entities in which the University owns a controlling interest or has the right to elect the majority of the entity's governing board. This policy applies to all users of University systems or data classified as Restricted or Confidential, 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, process, or transmit University data; which, if lost, stolen, or compromised could lead to the unauthorized disclosure of University data.

INDEX:

POLICY STATEMENT:

IRM-4002.1 – Definitions

Data Exposure: the unauthorized access of Confidential or Restricted data or a reasonable belief of such access that may compromise the availability, confidentiality, or integrity of the data

Event: an observable occurrence in the operation of an information resource (on premise or SaaS), service, or network. Not all events become incidents.

Incident: an event that disrupts the normal operations of IT resources; violation or imminent threat of violation of information technology policies, Information Security Policy, other University policies, standards, and code of conducts; or threatens the confidentiality, integrity, or availability of University information systems or data.

Confidential Information: sensitive information that must be safeguarded in order to protect the privacy of individuals and the security and integrity of systems and to guard against fraud. Confidential information includes, but is not limited to social security numbers, credit card numbers, passwords, etc.

Restricted Information: includes all data, records, documents or files that contain information that is: (a) required to be maintained confidentially under any applicable law, regulation or University policy; (b) subject to a contractual obligation to maintain confidentially; (c) subject to any applicable legal privilege or protection, such as the attorney-client privilege; and/or (d) deemed by the University to be a trade secret, confidential or proprietary. Examples of Restricted Information include; but are not limited to education, financial aid, and employment records, University identification number, business plans, etc.

IRM-4002.2 – Policy Statement

This policy details the basic steps to be followed by anyone discovering or being informed of the unauthorized access of University data or system. A data exposure occurs when restricted or confidential information is revealed or exposed to an unauthorized party. The policy also outlines the responsibilities of the Office of the Vice President for Information Services. The measures taken and their order will depend on the type and scope of the unauthorized access, but the basic process follows as:

Upon discovering or being informed of a security event or data exposure:

1. Enact countermeasures to prevent further data loss. For Information Services staff: if you are in a position to stop the unauthorized activity and prevent any further data loss, do so. This may involve shutting down systems, terminating access, or taking resources offline.
2. Immediately notify the following people of the issue and any actions taken:
    a. Your immediate supervisor and/or director
    b. The Director of Information Security
3. Gather the facts and record what you know. Immediately begin to keep a log of information and actions taken along with the time and date stamp of those occurrences. For Information Services staff: preserve any and all records/logs of access, names of people involved (if known), the data itself, any information used to generate the data in question, and any other evidence that may be needed for a forensic evaluation of the event/incident.

4. Provide contact information and be available for interaction with the Director of Information Security and University of Richmond-Cybersecurity Incident Response Team (UR-CIRT); law enforcement, if needed.
5. All requests for information by the media or other outside parties should be referred to University Communications.

Incident Response Process:

The Vice President of Information Services will be responsible for managing incident response until it is determined that the incident must be handed off to law enforcement, University Counsel, or other person/entity. The Vice President of Information Services will ensure the following occurs:

1. Quickly work with other staff to determine if the activity is still in progress. If so, stop the unauthorized activity to prevent any further data loss. Begin to ascertain the extent of the incident and determine the source and type of data, amount of data, affected persons and to the degree possible the exact data involved.
2. Appoint an incident response team. The composition and charge of the team will depend upon the type of incident and resulting data exposure. The team will conduct a preliminary assessment and risk assessment and help develop a tailored incident response plan. Once the incident is contained, this team will also evaluate changes in processes, systems and/or policies to prevent a repeat event.
3. Be responsible for interaction between IS, the incident response team, and the University administration. In order to ensure that only accurate, timely information that will not interfere with the ongoing investigation is released, no one else is to provide information to any party outside of the incident response team.
4. Alert the appropriate senior administrators to include the Vice President for Business & Finance, Provost, Chief of University Police, Office of Communications, University Counsel, and others as the situation warrants.
5. Work with the Director of Information Security, the incident response team and other internal or external parties to determine the identities of affected individuals and determine exactly how they are affected.
6. Review and refine the incident response plan as appropriate. Help ensure that appropriate resources are available.
7. Develop a separate data exposure notification plan. Provide accurate and timely notification that meets or exceeds all legal requirements. Working with the appropriate parties alert affected individuals and develop remediation strategies as appropriate to the situation. Work with the senior staff and University Communications on the release of information to the media, members of the campus community, and other key constituents as appropriate. University Communications will designate a spokesperson(s) to work with the media and all media and outside requests should be referred to them.
8. Communicate project status as appropriate, determine next steps, and develop a final report to include lessons learned and actions taken.

IRM-4002.3 – Roles and responsibilities

Vice President of Information Services – ensures an incident management program is in place to respond to cybersecurity events and incidents; escalates and informs executive leaders of incidents impacting the University.

Director of Information Security – evaluates event(s) to determine if and when it should be categorized as an incident, the scope, and risk level. This role will activate the UR - CIRT, inform the VP of Information Services, and escalates incidents to the Cybersecurity Support Team, as needed.

Incident Response Team Lead – leads incident handling efforts, coordinates duties among team members, records activities performed during an incident; drafts post incident report.

System Administrator – coordinates and administers centrally managed information resources during an incident

Network Administrator – coordinates and administers campus network resources during an incident.

Administrative Systems Administrator – coordinates and administers centrally managed application resources during an incident.

Help Desk – records event information and alerts Director of Information Security when an event or incident has occurred; may field calls from end-users regarding incidents

Application Owner – alerts Director of Information Security when an incident or event has occurred within their department managed information resource.

Cybersecurity Support Team – a subgroup of the Crisis and Emergency Management team who will develop the high level response, coordination, and decision-making structure during an incident.

UR-CIRT – a team of Information Services staff trained to respond to and resolve cybersecurity incidents, such as unauthorized access to systems or data

IRM-4002.4 – Applicable Regulations and Accreditation Standards

A. SACSCOC Principles of Accreditation 12.5 (Student Records)
B. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
C. Payment Card Industry Data Security Standard (PCI DSS)
D. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
E. Red Flags Rule of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Public Law 108-159, Section 114
F. Code of Virginia, § 18.2-186.6. Breach of personal information notification.
G. General Data Protection Regulation (GDPR) (EU) 2016/679
H. Gramm- Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, Public Law 106–102, 113 Stat. 1338

RELATED POLICIES:

IRM-4003 – Information Security Policy

IRM-4004 – Data Security Policy

IRM-4006 – General Data Privacy Regulation Privacy Notice

ACD-2004 – Privacy of Education Records (FERPA) Policy

POLICY BACKGROUND:

Initial policy created: July 12, 2007

Minor revisions in April 2020 reviewed by IT Governance Committee and President's Cabinet prior to approval on 06/29/2020. Policy was previously titled, "Data Exposure Policy".

POLICY CONTACTS:

Vice President for Information Services and Chief Information Officer
Director of Information Security