UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-4002	**Policy Title:**	Cybersecurity Incident Response Policy
Effective:	08/14/2024	**Responsible Office:**	Information Services
Date Approved:	08/05/2024	**Approval:**	Vice President for Information Services and Chief Information Officer
Replaces Policy Dated:	06/29/2020	**Responsible University Official:**	Vice President for Information Services and Chief Information Officer

PURPOSE:

The Incident Response Policy provides the structure and processes required to effectively respond to an information security incident with the goal of minimizing the negative impact to the confidentiality, integrity, and availability of University of Richmond (UR) data and information technology assets. The University of Richmond takes great care to safeguard data and privacy; therefore, 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 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 or services (e.g., Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), etc.) owned or leased by the University that experience a cybersecurity incident, as well as any computing or data storing device or service, regardless of ownership, which is used to store, process, or transmit University data; which, if lost, stolen, or compromised could lead to unauthorized disclosure of University data.

INDEX:

POLICY STATEMENT:

IRM-4002.1 – Definitions

Confidential Information: see definition in the University of Richmond Data Security Policy.

Event: is an observable occurrence in the operation of an information resource, service, or network. Not all events become incidents. An event may be electronic, physical, or social in nature.

Incident: an event that disrupts the normal operations of information and technology services; or threatens the confidentiality, integrity, or availability of University information systems or data.

Incident Response Plan (IR Plan): the documentation of a predetermined set of instructions and procedures to detect and respond to cybersecurity incident.

Restricted Information: see definition in the University of Richmond Data Security Policy.

UR-CIRT: University of Richmond Cyber Incident Response Team. The UR-CIRT is a function of the Information Security Office and is responsible for coordinating the response to cybersecurity incidents

IRM-4002.2 – Policy Statement

This policy outlines the roles and responsibilities that govern the response to and reporting of cybersecurity incidents that impact the confidentiality, integrity, or availability of the University of Richmond's information and technology services. This policy is supplemented by an internal Incident Response Plan (IR Plan) developed and maintained in alignment with the National Institute of Standards and Technology (NIST) Special Publication 800-61 "Computer Security Incident Handling Guide." The IR Plan contains detailed procedures and guidelines for incident response handling at the University.

IRM-4002.3 –Record Retention

Incident documentation and evidence will be maintained for five (5) years after the issuance of the final incident report. If the incident pertains to data or systems that fall under a regulatory retention period that exceeds five (5) years, the regulatory retention period will take precedence.

IRM-4002.4. – Reporting a Cybersecurity Incident

All members of the University shall immediately report any suspected cybersecurity incident to the University of Richmond Information Security Department using either the "Report Cybersecurity Incident" form located on SpiderTechNet, email, phone, in-person, or by initiating a help desk support ticket.

Information Security Department – Email: infosec@richmond.edu Phone: 804-289-8655
Information Services Help Desk – Email: helpdesk@richmond.edu Phone: 804-287-6400
SpiderTechNet: https://spidertechnet.richmond.edu

Members of the University must cooperate with incident response investigations and may not interfere, obstruct, prevent, retaliate against, or dissuade others from reporting an incident or cooperating with an investigation.

IRM-4002.5 – 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; appoints members to the UR-CIRT.

Director of Information Security – evaluates events to determine if and when they should be categorized as an incident, the scope, and risk level; activates the UR-CIRT; informs the VP of Information Services, and escalates incidents to the Cybersecurity Support Team, as needed; maintains the University IR Plan and overall security awareness program that trains users on how and when to report incidents; ensures that technical resources are in place or requested to identify if an incident has occurred; ensure corrective actions identified in incident reports are appropriately prioritized and executed.

Incident Response Team Lead – leads incident handling efforts under direction of the Director of Information Security or Vice President of Information Services; coordinates duties among team members; records activities performed during an incident; responsible for ensuring incident preparation activities are completed in accordance with the IR Plan; drafts post incident report; updates the University IR Plan at the direction of the Director of Information Security.

Server Administrator – coordinates and administers centrally managed servers during an incident. Alerts Director of Information Security when a real or suspected incident has occurred within their department managed information resource. Responsible for developing procedures to train their department information resource users to recognize and report incidents.

Network Administrator – coordinates and administers campus network and identity resources during an incident. Alerts Director of Information Security when a real or suspected incident has occurred within their department managed information resource. Responsible for developing procedures to train their department information resource users to recognize and report incidents.

Administrative Application Owner/Data Steward – coordinates and administers in-scope application resources during an incident as well as alerts Director of Information Security and Data Trustee when a real or suspected incident has occurred within their department managed information resource. Responsible for developing procedures to train their department information resource users to recognize and report incidents.

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

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 – Composition of the UR-CIRT is defined in the IR Plan and members are appointed by the Vice President of Information Services. The team will conduct risk assessment and response in accordance with the IR Plan. Once the incident is contained, this team will also conduct a "lessons learned" post-incident review to evaluate changes in processes, systems and/or policies to prevent a repeat incident. Members of the UR-CIRT are required to respond to declared incidents both during and after standard work hours.

UR-CIRT General Responsibilities

1. The UR-CIRT directs the analysis, containment, eradication, and recovery phases for incidents in accordance with the IR Plan and may authorize or expedite emergency changes to systems when required to as part of the response. Emergency changes will be documented in the UR change management system.
2. The UR-CIRT will coordinate external response with 3rd party suppliers who host University data in accordance with existing agreements and the IR Plan.
3. During the conduct of incident response activities, the UR-CIRT is authorized to monitor University information resources in scope to the response and retrieve any communications or other relevant records (e.g., email, instant messages, login session data, metadata, files, documents, etc.) for specific users without notice or further approval. All monitoring and access will be documented in accordance with the IR Plan.
4. Any external disclosure regarding an incident must be reviewed and approved by the Vice President of Information Services in consultation with University General Counsel and University Communications.
5. The UR-CIRT will coordinate with external law enforcement, service providers or government agencies as required and defined in the IR Plan. The UR-CIRT is authorized to share threat and incident information with these organizations under a court order or approval of University Counsel.
6. Upon conclusion of an incident, the UR-CIRT will finalize and distribute the incident report in accordance with the IR Plan.

IRM-4002.6 – 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
I. National Institute of Standards and Technology (NIST) SP 800-61

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".

06/26/24: Major revision to shift focus away from operational processes since those are covered in the Incident Response Plan. Aligned definitions with other policies for uniform terms. Added incident documentation retention. Updated general responsibilities to be more policy-focused. Included NIST 800-61 reference.

Policy Contacts:

Vice President for Information Services and Chief Information Officer

Director of Information Security