PURPOSE:

Reports of data compromises and the exposure of personal and 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. This policy outlines an action plan for our initial response.

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.

INDEX:

IRM-4002.1......Policy
IRM-4002.2......Roles and responsibilities
IRM-4002.3......Applicable Regulations and Accreditation Standards

POLICY STATEMENT:

IRM-4002.1 – Policy

This policy details the basic steps to be followed by anyone discovering or being informed of a data exposure at the University of Richmond. 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 exact measures taken and their order will depend on the type and scope of the breach, but the basic process follows:

Upon discovering or being informed of a data security breach or suspected exposure:
1. Prevent further data exposure. 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, cutting off access, or disabling applications.

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
   c. The Vice President for Information Services
   d. The Manager of Network Services

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 at issue and any other evidence that may be needed for a forensic evaluation of the issue.

4. Provide contact information and be available for interaction with the Director of Information Security and law enforcement if needed.

5. All requests for information by the media or other outside parties should be referred to University Communications.

IRM-4002.2 – Roles and responsibilities

The Vice President for Information Services will be responsible for incident management until it is determined that this must be handed off to law enforcement, University Counsel, or other person/entity. The Vice President for Information Services will:

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 breach 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 breach 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, the Provost, the Chief of the University Police Department, the 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. University Communications will designate 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 – Applicable Regulations and Accreditation Standards**

*SACSCOC Principles of Accreditation 12.5 (Student Records)*

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
B. Payment Card Industry Data Security Standard (PCI DSS)
C. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
D. Red Flags Rule of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Public Law 108-159, Section 114
F. General Data Protection Regulation (GDPR) (EU) 2016/679

**RELATED POLICIES:**

*IRM-4003 – Information Security Policy*

**POLICY BACKGROUND:**

Initial policy created: July 12, 2007

Revision: July 18, 2018 - Changed IS Security Administrator to Director of Information Security; added regulations

**POLICY CONTACTS:**

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