UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-4005	**Policy Title:**	External Data Transfer Policy
Effective:	10/6/2020	**Responsible Office:**	Information Services
Date Approved:	10/06/2020	**Approval:**	Vice President for Information Services and Chief Information Officer
Replaces Policy Dated:	10/17/2013	**Responsible University Official:**	Vice President for Information Services and Chief Information Officer

PURPOSE:

The University of Richmond knows the importance of protecting the sensitive data that is entrusted to it. In order to fulfill the mission and business operations of the University, this data may be shared with external parties. This policy governs the ad-hoc or one-time transmission to external vendors, consortiums, companies, or individuals of University of Richmond sensitive data as defined in the Data Classification Standard or any other University-maintained data whose disclosure would be seen as causing harm to the University.

SCOPE:

This policy applies to the data transfer of Restricted or Confidential data to an external party performed on a manual, ad-hoc, or one-off basis. Data transfers that occur on an ongoing basis are subject to separate policies and procedures per the Data Security Policy.

INDEX:

POLICY STATEMENT:

IRM-4005.1 – Definitions

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.

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.

User – Any individual, including but not limited to faculty, student, staff, contractors, and visitors who has access and uses University information resources, systems, or data.

IRM-4005.2 – Policy Statement

The University will only transfer Confidential or Restricted data to external parties if the owner of the data explicitly approves its transfer. The data owner is the Data Trustee (or their designee, as defined by the Administrative Data Steward list) who has direct authority over and full responsibility for the data—not the internal users of that data.

1. This data must be encrypted during transfer and at rest using an encryption strength of AES128, at a minimum. The preferred encryption strength is AES 256 bit or better. This can be achieved using encrypted ZIP files. If the data is being transferred via web upload, the in-transit encryption should be TLS 1.2 (weak ciphers disabled) or TLS 1.3.

2. The encryption key to the encrypted data must be transferred out of bounds. That is it cannot be transferred using the same mechanism as the data. For instance, if the data is sent via e-mail, the key must be exchanged via phone or letter.

3. The external party must acknowledge receipt of the data. One best practice approach is to create a CD with the encrypted data on it and then to use an overnight shipping company to send it, requesting a return receipt. E-mail acknowledgements are also acceptable although not preferred.

4. The data must be verified as secure by an authoritative member of Information Services before the transfer occurs. The Director of Information Security or designees can provide this service. The data must be securely archived so that in event of an issue, the University can verify the exact contents of the data shared.

IRM-4005.3 – Applicable Regulations and Accreditation Standards

A. Red Flags Rule of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Public Law 108-159, Section 114
B. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
C. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
D. Payment Card Industry Data Security Standard (PCI DSS)
E. SACSCOC *Principles of Accreditation* 10.6 (Distance and Correspondence Education)

RELATED POLICIES:

Information Security Policy
Acceptable Use Policy
Data Security Policy
Data Security Standard
Data Classification Standard
Administrative Data Management Policy

POLICY BACKGROUND:

Initial policy created July 12, 2007

Updated encryption strength October 17, 2013

Added web upload mechanism and encryption strength for data transfers October 2020.

Reviewed by IT Governance Committee and President's Cabinet prior to approval, on October 6, 2020

POLICY CONTACTS:

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