UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-4004	**Policy Title:**	Data Security
Effective:	08/05/2024	**Responsible Office:**	Information Services
Date Approved:	08/05/2024	**Approval:**	Vice President for Information Services and Chief Information Officer
Replaces Policy Dated:	09/11/2015	**Responsible University Official:**	Vice President for Information Services and Chief Information Officer

PURPOSE:

This document describes the data security policy for all data created or utilized at or by the University of Richmond. It defines this data, classifies it and details the requirements for its collection, storage, access, use, confidentiality, disclosure and transmission in addition to specifying the requirements of University personnel in its security, the levels of privacy of stored e/voice-mail and files and the steps to be taken in case of a data exposure.

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-4004.1.......Definitions

IRM-4004.2.......Classification

IRM-4004.3.......Access to and Use of Administrative Data and Education Records by University Faculty, Staff, and Students

IRM-4004.4.......Storage, Transmission and Disposal of Administrative Data and Education Records

IRM-4004.5.......Access to and Use of Administrative Data or Education Records by Vendors and Other Third-Parties

IRM-4004.6……Use of Generative Artificial Intelligence (GenAI) with University Data

IRM-4004.7.......Data Exposure Plan

POLICY STATEMENT:

IRM-4004.1 – Definitions

Administrative Data
Data that is gathered, produced, stored, and/or disseminated concerning any aspect of the University's operations. Such data includes, but is not limited to, general ledger/accounting, human capital management, student, alumni/development, space management, student housing data, and also includes any data derived from the use of such data. Administrative data specifically does not include faculty generated classroom data nor faculty- or student-generated research data

Data Steward Domain
A University administrative or operational area, function or process and the authoritative data elements created, collected, and managed by that area throughout the lifecycle of that data, regardless of the Transactional System(s) in which they reside (e.g., Finance data).

Data Steward
Typically, a senior operational manager in a functional area responsible for a Data Stewardship Domain.

Education Records
Any record (in handwriting, print, electronic form, tapes, film, or other medium) maintained by the University of Richmond or an agent of the University that is directly related to a student. The following records are not considered Education Records subject to this policy.

- Records kept in the sole possession of the maker that are not accessible or revealed to any other person except a temporary substitute for the maker of the record.
- An employment record of an individual, maintained in the ordinary course of business and used solely in connection with such employment, provided the individual's employment is not contingent on the fact that he or she is a student. If the individual's employment is contingent upon his or her status as a student, then the records are Education Records.
- Records created and maintained by the University of Richmond Police Department ("URPD") for law enforcement purposes. Records created by URPD that are maintained by another component of the University and records created and maintained by the URPD exclusively for a non-law enforcement purpose, such as a disciplinary action or proceeding conducted by the educational institution, are considered Education Records subject to this policy.
- Clinical records relating to a student who is 18 years of age or older that are made by a physician, psychiatrist, psychologist or other recognized health care professional or paraprofessional, provided those records are made, maintained or used only in connection with treatment of the student and are disclosed only to individuals providing treatment.
- Post-attendance records created or received by the University after an individual is no longer a student in attendance and that ware not directly related to his or her attendance as a student.
- Grades on peer-graded papers before they are collected and recorded by a professor or instructor.

Principle of Least Privilege:
The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Vendor
A vendor is the party with whom the University contracts to provide the goods and/or services identified in a contract.

IRM-4004.2 – Classification

The University classifies Administrative Data into the following categories:

A. **Confidential Information:** Confidential Information is sensitive information that must be safeguarded to protect the privacy of individuals and the security and integrity of systems and to guard against fraud. Confidential Information must be afforded the highest level of privacy and security controls. Confidential information includes, but is not limited to:

- Social Security Numbers (SSN)
- Credit and debit card numbers
- Bank account and other financial account numbers
- Medical or counseling records or information
- Passwords, passphrases, PINs, security codes, and access codes
- Tax returns
- Credit histories or reports
- Background check report

B. **Restricted Information:** 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 Records
- Employment records
- Financial Aid records
- University ID Number
- Date and place of birth
- Public relations strategies
- Information security protocols or systems
- Financial records (other than audited financial statements published on the University website)
- Contracts and other business arrangements and/or strategies with a third-party non-disclosure agreement
- Gramm-Leach-Bliley Act (GLBA) data
- Library circulation records

C. **Official Use Only Information**: Information about individuals that can be shared within the University Community for official purposes but will not be made available to the public except by the Office of Communications or other authorized offices of the University and such disclosure shall be made in a manner consistent with applicable law and the University's Privacy of Education Records (FERPA) Policy. Examples of Official Use Information includes a name in conjunction with the following:

- Addresses: permanent, campus, local (off-campus), e-mail and campus computer network (IP) address, net id
- Associated telephone numbers
- School or college
- Major and/or minor fields of study
- Degree sought
- Expected date of completion of degree requirements and graduation
- Degrees conferred
- Awards and Honors (e.g., Dean's list)
- Full or part time enrollment status
- Dates of attendance
- Previous institutions attended
- Participation in officially recognized activities and sports
- Weight and height of members of athletic team members
- Photograph
- Gender
- Race

D. **Public Information:** Information that the University has made available or published for the explicit use of the public.

IRM-4004.3 – Access to and Use of Administrative Data and Education Records by University Faculty, Staff, and Students

This section sets forth the requirements governing access to and use of Administrative Data and Education Records by University faculty, staff, and students. See Section 4004.4 for requirements governing the storage and transmission of Administrative Data and Education Records and Section 4004.5 for requirements governing access and use of Administrative Data and Education Records by vendors and other third parties.

A. University faculty, staff, students, vendors, and authorized third-parties who have access to Administrative Data or Education Records are required to maintain and manage such information in accordance with this policy.

B. Data Stewards are responsible for implementing and enforcing this policy within their respective areas of responsibility and for the management of Administrative Data and Education Records in their purviews, including: a general inventory of the kind of information specific to their roles, classification of information into one of the four categories defined in Section 4004.2 of this policy and, providing authorization for access to Administrative Data and Education Records under their purview.

C. Administrative Data are to be used only when conducting University business. Education Records may be used only as permitted by the University's Privacy of Education Records (FERPA) Policy

D. Confidential or Restricted Information must be securely maintained, controlled, and protected to prevent unauthorized access.

E. Authorization to access Confidential or Restricted Information is limited to those faculty, staff, students or vendors who require such access to perform their job on behalf of the University and will be provisioned in accordance with the Principle of Least Privilege as noted in section IRM-4004.1. Access to Education Records is limited as set forth in the University's Privacy of Education Records (FERPA) Policy.

F. University committees, task forces, and working groups may have access to institutional data only as defined in their charge and consistent with other University policies, including the Administrative Data Policy. Requests for any information beyond their specific charge must be made to the Director of Institutional Effectiveness or appropriate Data Steward. Such data shall not be disseminated beyond the authorized committee, task force or working group except with the approval of the relevant Data Steward.

G. Administrative Data shared with students, faculty, and staff for specific business purposes (such as serving on committees or in specific roles like department chair or for a particular purpose like advising) may not be used beyond the specific purpose for which it was authorized, or disseminated to others, without permission from the Data Steward.

H. When accessing or transmitting Confidential or Restricted Information an encrypted connection (e.g., Virtual Private Network (VPN), Secure Shell (SSH), Secure Socket Layer / Transport Layer Security (SSL/TLS)) must be used. Alternative controls for this requirement must be reviewed and approved by the Director of Information Security. Refer to the External Data Transfer Policy for detailed requirements.

I. University faculty, staff, and students with access to Administrative Data or Education Records shall prevent unauthorized access to such information by always locking or logging-off of their workstation when they leave their work area.

J. Administrative Data and Education Records may not be used for personal gain or profit.

K. If a University faculty member, staff member, student or vendor loses a computing device that held or contains Administrative Data or Education Records, or becomes aware of the theft of such a device, they must report that loss immediately to their supervisor and the Director of Information Security.

L. University faculty, staff, students and vendors must follow the University Record Retention Policy regarding appropriate retention of Administrative Data and Education Records.

IRM-4004.4 – Storage, Transmission and Disposal of Administrative Data and Education Records

University faculty, staff, and students who have access to Administrative Data or Education Records are required to comply with this policy regarding the storage, transmission and disposal of Administrative Data and Education Records in electronic and hard copy formats.

A. Storing Electronic Confidential and Restricted Information

1. Except as permitted by this policy, electronic Confidential and Restricted Information shall be stored only in systems maintained by or under the control of the University. Confidential or Restricted Information shall not be stored with a software or service vendor such as Google, Dropbox or Microsoft unless the University has a contract with the service provider that contains appropriate confidentiality and security provisions that meet or exceed University policy requirements. See Section 4004.5 of this policy for more information on vendors.

2. Confidential Information must not be stored on any mobile computing or storage device such as a laptop, PDA, USB drive, flash drive or any mobile device or media, regardless of whether such device is owned by the University or is personally owned. Confidential Information may only be stored on a University centrally managed storage system (e.g., Box).

3. Except as permitted by this policy, Restricted Information may not be stored on a personal computing device such as a laptop, PDA, USB drive, flash drive or any mobile device or media.

    a. Restricted Information stored on a University-owned mobile computing device must be encrypted.

B. Use of Email to Store or Transmit Confidential or Restricted Information

1. When University employees must exchange Confidential or Restricted Information via email to conduct University business, the Confidential or Restricted Information must be sent using the University's email service.

2. If University e-mail is accessed or stored on a University or personally owned computing device,

that device must be password/passcode protected and encrypted (e.g., Microsoft BitLocker or Apple FileVault) at all times.

C. Transmission of Electronic Confidential or Restricted Information To Third Parties. This section covers the transmission of Administrative Data or Education Records (other than Public Information) to external vendors, consortiums, companies or individuals on a one-time basis. Data transfers that occur on an ongoing basis must be developed or reviewed by Information Services. For those cases, contact the Director of Systems & Networks or the Director of Information Security for direction and approval.

1. The appropriate Data Steward must approve, in advance, any transfer of Confidential or Restricted Data to a third party.
2. Any staff or faculty member seeking to transfer Confidential or Restricted Data must comply with this policy. Information Services will assist with identifying and securing required approvals.
3. Confidential or Restricted Information must be encrypted at a file-level during transfer. A minimum of AES 128-bit encryption must be used, although stronger encryption levels may be appropriate. This can be achieved using encrypted archive (e.g., .zip) files. Refer to the External Data Transfer Policy for detailed requirements.
4. The key to encrypted data must be transferred out of band. That is, it cannot be transferred using the same mechanism or channel as the data. For instance, if data are sent via e-mail, the key must be exchanged via phone or letter.
5. The third-party must acknowledge receipt of the data. Acknowledgement must be either in writing (e.g., email or letter), via delivery receipt (e.g., if a shipping service or U.S. Mail is used), or auditable log entry for file sharing / transfer services.
6. Data exchange method must be verified as secure by the Director of Information Security, the Director of Systems & Networks or their designate before the transfer is attempted.
7. Data must be securely archived so that in the event of an issue the exact contents of data transmission can be verified.

D. Hardcopy Confidential and Restricted Information

1. Paper or hardcopy documents, records, and media containing Confidential or Restricted Information must be maintained in secure, locked locations when not in use.

E. Disposal or Destruction of Confidential and Restricted Information

1. Confidential and Restricted Information shall be maintained in accordance with the University's Record Retention Policy. Confidential and Restricted Information must be destroyed or deleted at the end of the applicable retention period in accordance with this policy.
2. At the end of the applicable retention period, electronic Confidential or Restricted Information shall be deleted from the University's centrally managed storage system and from University owned and personally owned computing devises or storage media, including from hard drive files such as the recycle bin.
3. At the end of the applicable retention period, hardcopy Confidential and Restricted Information shall be securely disposed of in a document destruction receptacle/bin provided by a University approved vendor.
4. University owned computing devices or storage media (e.g. computer, laptop, mobile device, CD, DVD, flash drive, etc.) that have stored Administrative Data or Education Records must be turned in to Information Services for secure disposal.

IRM-4004.5 Access to and Use of Administrative Data or Education Records by Vendors and Other Third-Parties

The University may share Administrative Data or Education Records with vendors and other third-parties, including government agencies to the extent required by law. University faculty, staff, and students are required to comply with this policy when providing vendors and other third-parties with access to Administrative Data or Education Records (other than Public Information). If an information request is not covered below the recipient of such request must seek the approval of the data steward before providing the requested information.

A. Vendors

1. University faculty and staff shall not provide vendors access to Administrative Data or Education Records unless a business relationship exists, access to such information is necessary for the vendor to provide services to the University, and that there is a contract with the vendor that contains appropriate confidentiality and security provisions.
2. Prior to initiating a contract with a vendor or providing a vendor or other outside entity with access to Administrative Data or Education Records, the University faculty or staff member responsible for the vendor relationship must obtain the approval of the appropriate Data Steward.
3. All faculty, staff, and students must comply with the University's Contract Management Policy and Delegation of Contract Approval and Signature Authority Policy when initiating, negotiating and finalizing a contract with a vendor that will have access to Administrative Data or Education Records.
4. Access to Confidential or Restricted Information will be furnished to vendors and other outside entities only if essential and the information provided will be limited to the minimum necessary for the vendor or outside entity to provide services to the University.
5. Faculty and staff must comply with this policy and the University's External Data Transfer Policy when transferring Confidential and Restricted Data to a vendor. The University faculty or staff member responsible for the vendor relationship must work with University Information Services staff to develop any data extracts or reports to ensure that they comply with this policy and other University policies. Information Services staff will provide guidance regarding the use of record identifiers.
6. Vendors who host or process Confidential or Restricted Information shall periodically complete an independent audit using an established security framework (e.g., NIST 800-53, ISO 270001, HITECH, etc.) to validate the effectiveness of their information security controls.
7. Faculty and staff shall require vendors to which they provide Administrative Data or Education Records to comply with this policy or substantially similar standards contained in the vendor contract.

B. Education Records

1. Education Records are protected under the Family Educational Rights and Privacy Act of 1974 ("FERPA"), as amended, and its implementing regulations.
2. All faculty and staff must comply with the University's FERPA Policy Statement.
3. All requests from third-parties for Education Records or student information must be referred to the Office of the University Registrar (804) 289-8639.

C. Requests from Law Enforcement Officers, Search Warrants, Subpoenas, Court Orders, and Civil Investigative Demands

1. If a law enforcement officer or agent or a process sever requests access to or copies of Administrative Data or Education Records, presents a search warrant or serves a subpoena or civil investigative demand the individual to whom such request is made should:
    a. Request and review the individual's badge or other official identification; and
    b. Refer the officer or agent to the Office of the University General Counsel (804) 287-6683 or (804) 289-8671.
2. Search Warrants
    a. If the law enforcement official presents a search warrant the agent or officer may begin a search as soon as the warrant is served, after confirmation of the official's badge or other official identification.
    b. The university staff or faculty member to whom the search warrant is presented shall immediately contact one of the following individuals depending on availability to inform them that a court-ordered search has been requested or initiated:
        i. University Vice President and General Counsel (804) 287-6683; or
        ii. University Assistant General Counsel (804) 289-8671.
    c. If computers, email, phone records, or electronic information sources are involved in the search, the Vice President and General Counsel or the Assistant General Counsel shall contact the Vice President for Information Services (804) 289-8771 or the Director of Information Security (804) 289-8655.
3. Subpoenas, Court or Agency Orders, Civil Investigative Demands, or Agency Requests for Records
    a. Upon receipt of a subpoena, a court or agency order, a civil investigative demand or any request for Administrative Data or Education Records from a local, state, or federal agency or court, regardless of whether such subpoena, order, demand, or request was personally served, mailed, or emailed, faculty and staff shall promptly notify the University Vice President and General Counsel (804) 287-6683 or the University Assistant General Counsel (804) 289-8671 and shall provide copies of the subpoena, order, demand or request.
    b. The Office of the General Counsel shall be responsible for coordinating the University's response to such subpoena, order, demand or request.
4. If a law enforcement officer needs to locate a student, or a faculty or staff member immediately, refer them to Campus Police (804) 289-8715.

D. Employment Verifications and Background Checks

1. *Current or Former Students:* All requests for employment information regarding current or former students shall be referred to the University Registrar (804) 289-8639. The University Registrar will verify the request, determine whether the student has consented to sharing information, and refer the requestor as necessary. Faculty and staff shall not respond to these requests for information about students unless the Registrar has referred the requestor to you.
2. *Faculty or Staff:* University community members may occasionally have a need to have employment and/or salary information confirmed as part of a job interview, loan application, real estate transaction, etc. All requests for employment or income verification shall be referred to the

Employment Verification page on the HR website. Refer to the Employment Verification web page for instructions on how to access and use The Work Number.

All other HR-related questions and requests, including background checks, shall be referred to the URHR Inbox at URHR@richmond.edu or the HR Solution Center at (804) 289-8747 (URHR). The HR Solution Center will review the request and refer the requestor to members of the university as necessary. Do not respond to these requests unless they come through Human Resources.

E. Requests for References or Recommendations

1. *Current or Former Students:*

   a. Requests for verification of enrollment or degrees shall be referred to the Office of the University Registrar (804) 289-8639.

   b. Prior to providing a recommendation for a current or former student that contains information from the student's Education Records, including but not limited to courses taken, grades or grade point averages, faculty and staff must obtain a written and signed authorization from the student. The authorization must:

      - Be in writing,
      - Be signed and dated by the student or originate from the student's University of Richmond email account,
      - Specify the records that may be disclosed,
      - State the purpose of the disclosure; and
      - Identify the party or class of parties to whom the disclosure may be made

2. *Faculty and Staff:* Faculty and staff should refer requests for references to Human Resources unless the faculty or staff member has been asked and agreed to serve as a reference for a colleague.

F. Request for Information about University Trustees

The President's Office website publishes basic information about trustees, including name, city, state, and committee assignments. Individuals who seek additional information shall be referred to the Secretary of the Board of Trustees at (804) 289-8732.

IRM-4004.6 Use of Generative Artificial Intelligence with University Data

Generative Artificial Intelligence (GenAI) is a technology capable of generating text, images, video, and other data through the statistical modeling of data sets. Diligence must be exercised to ensure the confidentiality, integrity, and availability of Administrative Data and Education Records that may be accessed by, processed with, or generated through GenAI applications. This section defines data security requirements for the use of GenAI by University faculty, staff, and students. These requirements are in addition to all other requirements defined in this policy.

A. Confidential, Restricted, or Official Use Only Information shall not be entered into any publicly available or commercial GenAI application without an approved agreement that includes appropriate data security requirements in compliance with University policies.

B. Confidential, Restricted, or Official Use Only Information shall not be entered into any private GenAI application without prior approval through University IT Governance. Additionally, if the application is not owned and administered by the University of Richmond, an approved use agreement must be executed with the application provider and must include appropriate data security requirements in compliance with University policies.

C. Each GenAI application must have an Acceptable Use Policy (AUP) defining its terms of use, data collection policies, and user responsibilities. Faculty may include the AUP in course syllabi if GenAI is permitted for use in the course.

D. Any Administrative Data or Education Records used in a Generative AI application must be approved by the Data Steward and reassessed annually.

E. Output from a GenAI application must be reviewed by the Data Steward for confidentiality, integrity, accuracy, fairness, regulatory compliance, and academic attribution before publication or ingestion into another University system.

F. When a GenAI application provides data or a decision, a disclaimer must clearly state that artificial intelligence was used to generate the output. This ensures transparency and informs users about the nature of the information they are receiving.

IRM-4004.7 – Data Exposure Plan

Reports of data compromises and the exposure of sensitive 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. The Cybersecurity Incident Response Policy outlines an action plan for our incident response.

RELATED POLICIES AND REGULATIONS:

FERPA Policy

University Record Retention Policy

Cybersecurity Incident Response Policy

Computer Systems Backup Policy

External Data Transfer Policy

HIPAA Privacy Policy and Procedures

Gramm-Leach-Bliley Act (GLBA)

POLICY BACKGROUND:

Date	Policy Action
08/01/2011	Original version
12/30/2012	Minor revisions and web links added
02/26/2014	Formatting and updated links

02/26/2014	Bullet #6 added to Section 3. Responsibilities related to the Storage, Access, and Use of University Administrative Information
09/11/2015	The Responsibilities Related to the Storage, Access, and Use of University Administrative Information section was updated to include specific guidelines about internal sharing of University Administrative Information.
4/2/2024	Major revision. Restructured document for clarity and more defined groupings of requirements. Replaced “University Administrative Information” with “Administrative Data” and aligned that definition with the definition in the Administrative Data Management Policy. Updated the definition of Data Steward to reference the Administrative Data Management Policy instead of the Records Retention Schedule. Added definition for “Vendor” that aligns with the Contract Management Policy. Updated suggestive language to be directive by replacing “should” with “shall” throughout the policy. Added explicit reference to Gramm-Leach-Bliley Act (GLBA) for Restricted Data. Added requirement #5 for annual vendor audit requirement. Updated requirement #8 to clarify the requirement and remove a hyperlink to outdated encryption procedure. Removed reference to “netfiles” as a central storage system. Updated references to the Associate Vice President of Human Resources to Chief Human Resources Officer. Removed IRM-4004.6 Privacy of E-mail, Voice Mail, and Electronic Files since that section is covered by policy IRM-4008 “Access to Electronic Files Policy”. Added IRM-4004.6 Use of Generative Artificial Intelligence with University Data. Updated link for the Employment Verification website. Replaced Data Exposure Policy link in Data Exposure Plan section to refer to the Cybersecurity Incident response Policy. Made general updates throughout the policy to ensure that requirements for Education Records are explicitly defined.
8/5/2024	Revised policy reviewed by President’s Cabinet and approved by VP for Information Services and Chief Information Officer

Policy Contacts:

Vice President for Information Services and Chief Information Officer