University of Richmond

Data Security Policy

Scope: 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.

1. Definitions

Data Steward

A University Official with executive responsibility over a University Division, or Department. Examples of Data Stewards include, Deans, Vice Presidents and Department Directors. Data stewards are those individuals listed as the responsible party in the University of Richmond's Records Retention Schedule.

University Administrative Information

University Administrative Information is defined as recorded information, in hard copy or electronic copy, produced or acquired in the course of the University's business. It includes all documents, papers, letters, memoranda, e-mail messages, patient records, images, cards, books, maps, photographs, blueprints, sound or video recordings, microfilm, magnetic tape, electronic media, and other information-recording media, regardless of physical form or characteristic, that is generated and/or received in connection with the University's operations, business, strategy, services, or transactions of any kind.

2. Classification

The University classifies University Administrative Information as follows:

I. **Confidential Information:** Confidential Information is 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 and debit card numbers
- Bank account or other financial account numbers
- Medical or counseling records or information
- Passwords, passphrases, PIN numbers, security codes and access codes
- Tax returns
- Credit histories or reports
- Background check reports

Confidential Information must be afforded the highest level of privacy and security controls.

II. **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 (see the University's definition at: http://registrar.richmond.edu/ferpa/statement/definitions.html)
- Employment records
- Financial aid records
- University ID number
- Date and place of birth
- Business plans

- Public relations strategies
- Information security protocols or systems
- Financial records (other than audited financial statements published on the University website)
- Prospective and existing contracts and other business arrangements and/or business plans, procedures, and other strategies.
- Library circulation records

III. **Official Use Only Information**: Official Use Only Information is information about individuals that can be shared within the University Community for official purposes but will not be routinely made available to the public except by the Office of Communications.

Official Use Only Information includes:

- Name
- 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

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

3. Responsibilities Related to the Storage, Access, and Use of University Administrative Information

This policy applies to all University faculty, staff, students, vendors and contractors.

University faculty, staff, students, vendors and contractors who have access to University Administrative Information are required to maintain and manage such information in accordance with the guidelines set forth in this policy regarding the storage, disclosure, access, and classification of such information. They are required to ensure that any contractors, vendors, and other parties with whom they work also comply with this policy.

Data Stewards are responsible for implementing this policy within their respective areas of responsibility and for the management of University Administrative Information in their purviews, including: a general inventory of the kind of information specific to their roles, classification of information into one of the four data security categories set forth in this policy and, providing authorization for access to University Administrative Information.

1. University Administrative Information is to be used only when conducting University business.

2. University Administrative Information that includes Confidential or Restricted Information will be securely maintained, controlled and protected to prevent unauthorized access.

3. Authorization to access Confidential or Restricted Information is limited to those faculty members, staff members, students or contractors who require such information to perform their job.

4. University committees, task forces and working groups may have access to institutional data only as defined in their charge. Requests for any information beyond their specific charge must be made to the Director of Institutional Effectiveness. It is expected that such data will not be disseminated beyond the authorized committee, task force or working group.

5. University-owned 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 for purposes beyond the specific purpose for which it was accessed, or disseminated to others without permission.

6. Confidential or Restricted Information should never be stored on a computing device or electronic storage media that is personally owned.

   Exception: The University acknowledges that faculty may wish to do their work using personally owned computing devices or electronic storage media therefore education records managed or created by faculty when teaching their classes are exempt from this restriction. However, faculty are advised to delete education records from personally owned computing devices and electronic media as soon as it is practical to do so.

7. University E-mail: If University E-mail will be accessed or stored on a University or personally owned computing device, that device must be password/passcode protected at all times.

8. When University employees must exchange confidential or restricted information via email in order to conduct University business they must send this information in an encrypted email using the University's email service. http://is.richmond.edu/email/manage/encryption-outlook.html

9. Paper or hardcopy documents, records and media containing Confidential or Restricted Information must be maintained in secure, locked locations when not in use. Electronic and hard copies of Confidential and Restricted Information should be stored only in University offices or facilities.

   Exception: The University acknowledges that faculty may need to do their work at an off-campus location therefore education records managed or created by faculty when teaching their classes are exempt from this restriction. However, faculty are advised to carefully secure these documents, records and media when they are not in use.

10. Confidential Information, as defined in Section 2, 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 be safely stored on the University's centrally managed storage system referred to as "netfiles."

11. Restricted Information must not be stored on a mobile computing or storage device such as a laptop, PDA, USB drive, flash drive or any portable device or media unless that data is properly encrypted. Contact the Information Services Security Administrator for guidance on appropriate encryption options.

    Exception: The University acknowledges that faculty may wish to work with education records on mobile computing devices or create learning environments for mobile platforms therefore education records managed or created by faculty when teaching their classes or advising students are exempt from this restriction. However, faculty are encouraged to encrypt this information whenever possible.

12. Confidential or Restricted Information should never be stored with a software or service vendor such as Google Apps, Dropbox or Mozy unless the University has a contractual agreement with the vendor or service.

13. When accessing or transmitting Confidential or Restricted Information from an off-campus computing device (i.e., not connected to the University's network), an encrypted connection (e.g., VPN, SSH, RDP, SSL) must be used.

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

14. The University has business relationships with various outside contractors and vendors. These relationships may require that these outside entities be provided with access to University Administrative Information. Great care must be taken when creating and transmitting files containing Confidential and Restricted information. Specific guidelines for transmitting and providing access to such information to outside entities are contained in the policy for "Providing University Administrative Information to Others" in section C of that policy. The External Data Transfer Policy (section 5) provides the procedures that must be followed when providing Confidential or Restricted Information to an outside entity

15. University Administrative Information may not be used for personal gain or profit.

16. Information Services employs secure data destruction technologies when disposing of equipment. If University employees have control of a University owned computing device or storage media (e.g. computer, laptop, CD, DVD, thumb drive, etc.) that has stored University Administrative Information they should not dispose of it themselves but must turn it in to Information Services for secure disposal.

17. If a University faculty member, staff member, student or contractor loses a computing device that held or contains University Administrative Information or becomes aware of the theft of such a device they must report that loss immediately to their supervisor and the Information Services Security Administrator.

18. University faculty, staff, students and contractors must follow the University Record Retention Policy regarding appropriate retention of University Administrative Information.

4. Providing University Administrative Information to Others

This section discusses providing University Administrative Information (other than Public Information) or access to that information to others and the terms under which University Administrative Information may be provided and who must approve these requests. Unless an information request is covered below the recipient of such request must seek the approval of his or her dean/supervisor before providing the requested information.

A. Education Records

i. Education Records are protected under the Family Educational Rights and Privacy Act of 1974 ("FERPA"), as amended, and its implementing regulations.
ii. All faculty and staff must comply with the University's FERPA Policy Statement http://registrar.richmond.edu/ferpa/index.html .
iii. All requests from outside entities for education records or student information must be referred to the Office of the University Registrar (804)289-8639.

B. Requests from law enforcement officers, subpoenas and search warrants

If a law enforcement officer or agent requests access to or copies of University Administrative Information, the individual to whom such request is made should:

i. Request and review the individual's badge or other official identification; and
ii. Inform the officer or agent that he or she is going to refer them to the appropriate University administrator.

For Inquiries relating to current students:

All requests for information regarding current students should be referred to the University Registrar (804)289-8639. If a law enforcement officer needs to locate a student immediately, refer them to Campus Police (804)289-8715.

For Inquiries relating to faculty, trustees, or staff:

i. If the law enforcement official makes a verbal or written request or presents a subpoena or court order, refer the officer or agent to the Associate Vice-President for Human Resources (804)289-8166 or to the University General Counsel (804)287-6683.

ii. If the law enforcement official presents a search warrant the agent or officer may begin a search as soon as the warrant is served. The university staff or faculty member on whom the order is served should immediately contact one of the following individuals depending on availability to inform them that a court ordered search has been requested or initiated:

University General Counsel (804)287-6683 (o) (804)334-3870 (c)

Associate Vice-President for Human Resources (804)289-8166

iii. University faculty and staff should cooperate with the search when a search warrant is served. If computers, email, phone records, or electronic information sources are involved in the search contact the Vice-President for Information Services (804)289-8771 or the Information Services Security Administrator (804)289-8655.

iv. Unlike search warrants, subpoenas do not require an immediate response. Subpoenas are usually delivered by the Sheriff's Office and allow 10 days for response. If a law enforcement official presents a subpoena contact one of the following individuals depending on availability:

a. University General Counsel (804)287-6683
b. Associate Vice-President for Human Resources (804)289-8166

The University's General Counsel will review the information and coordinate the University's response. Only requested information will be released.

Special considerations regarding the "USA Patriot Act."

The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act," Pub. L. No. 107- 56, 115 Stat. 272-402 (2001)(codified in various titles and sections of U.S.C.) is also known as the "USA Patriot Act". If law enforcement officials present an order under this act or FISA ("Foreign Intelligence Surveillance Act") the University's General Counsel will coordinate the University's compliance with such order, involving appropriate representatives from Information Services, Human Resources and other areas of the University.

If you are served with an order under the USA Patriot Act or under FISA, contact the University General Counsel immediately (287-6683 (o) or (804)334-3870 (c)). If the General Counsel is not available, contact Vice-President for Information Services (804)289-8771.

A search warrant issued under the "USA Patriot Act" may contain the stipulation that the institution does not disclose that the warrant has been served or that information has been provided pursuant to the warrant. You should not inform anyone other than the administrators listed above about this action.

C. Confidential or Restricted Information supplied to or accessed by contractors or vendors, outside agencies and individuals

The University has business relationships with various third party contractors and vendors. These relationships may require that these contractors and vendors be provided with or have access to University Administrative Information.

i. University Administrative Information or access to that information may not be provided to contractors or vendors unless a verified business relationship exists and access to such information is necessary for the contractor or vendor to provide services to the University.

ii. Prior to providing a vendor, contractor, or other outside entity with data files or access to University Administrative Information, the University faculty or staff member responsible for the relationship must ensure that the vendor, contractor or outside entity has signed an appropriate confidentiality agreement or that the terms of the overall agreement with the vendor, contractor or outside entity contains an appropriate confidentiality provision. The University General Counsel and Information Services must review and approve new or amended contracts that involve the transfer, storage or management of Confidential or Restricted Information before those contracts or amendments are finalized.

iii. Confidential or Restricted Information or access to that information will be furnished to contractors, vendors and other outside entities only if essential and the information provided will be limited to the minimum necessary for the contractor, vendor, or outside entity to provide services to the University.

iv. The University faculty or staff member responsible for the relationship must work with University Information Services staff to develop any data extracts or reports to ensure that they comply with specifications and with the Data Transmission portion (section 5) of this policy. Information Services staff will provide guidance regarding the use of record identifiers.

v. All transmission of Confidential or Restricted information must conform to the "Transmission of Confidential or Restricted information" policies listed in section 5.

D. Employment verifications requests and background checks

For inquiries relating to current or former students:

All requests for employment information regarding current or former students should be referred to the University Registrar (804)289-8639. The University Registrar will verify the request and waiver and refer the requestor as necessary. Do not respond to these requests for information about students unless the Registrar has referred the requestor to you.

For inquiries relating to 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 should 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, should be referred to the URHR Inbox at URHR@richmond.edu or the HR Solution Center at 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. Job references

For inquiries relating to current or former students:

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

When asked to write letters of recommendation for students or former students, faculty and staff should not share information from student Education Records, including grades

or grade point averages, with others outside the institution without written permission from the student.

To release information relating to Education Records (non-directory information), faculty and staff must obtain written consent from the student for such disclosure. Consent for the disclosure of a student's Education Records must:

- Be in writing,
- Be signed and dated by the student,
- 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

For inquiries relating to faculty or staff:

Job reference checks should be referred to Human Resources unless you have been asked and agreed to serve as a reference for a colleague.

F. Request for Information about University Trustees

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

5. Transmission of Confidential or Restricted Information

This section covers the transmission of University Administrative Information (other than Public Information) to external vendors, consortiums, companies or individuals.

This section covers cases where data transfer is being performed on a one-time basis. Data transfers that will occur on an ongoing basis must be developed or reviewed by Information Services. For those cases, contact the Director of Systems & Networks or the Information Systems Security Administrator for direction and approval.

i. Confidential or Restricted data will be transferred to external parties only if the Data Steward explicitly approves the transfer and all requirements of Section 4 of this policy are met. Information Services will assist with identifying and securing the appropriate approvals.

ii. Confidential or Restricted Information must be encrypted during transfer. A best practice approach is to use a standard of AES 128 bit encryption, although other levels may be appropriate. This can be achieved using encrypted ZIP files.

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

iv. 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 acceptable although not preferred.

v. The data must be verified as secure by the Information Services Security Administrator, the Director of Systems & Networks or their designate before the transfer is attempted.

vi. The data must be securely archived so that in event of an issue the exact contents of the data transmission can be verified.

6. Privacy of E-mail, Voicemail, and Electronic Files

The University of Richmond intends to provide secure and reliable email and voice mail services for authorized users and uses. Electronic mail and voice mail resources are deployed and maintained by Information Services to support the University's work of teaching, scholarship, research, administration, and public service.

Information Services monitors and collects data related to the University's systems and networks as necessary to manage the campus network traffic and to ensure that resources are available for academic, scholarly, and administrative uses. Designated Information Services personnel, such as email system administrators, have special privileges necessary for the implementation, recovery and maintenance of the University's systems and networks. The number of Information Services staff with system administrator privileges for any given system is limited to the number required for operations, effective recovery, cross training, and coverage.

The University respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations. Therefore, the University does not routinely monitor or access the content of electronic communications, computer files, or voice mail whether stored on university equipment or in transit on the University network. However, monitoring or access may be necessary under certain circumstances. This policy outlines the legal or administrative circumstances under which access and/or monitoring may occur.

Conditions under which Email May be Monitored and Accessed

Email mailboxes and stored files are considered private to the account holder and all members of the University are to treat them as such; however the University may inspect, monitor or disclose the contents under the circumstances defined below under the headings of (A) System Administration, (B) Legal Compliance, (C) Emergency Situations, and (D) Other Compelling Circumstances.

A. System Administration

When managing email and file systems, network administrators primarily deal with system logs and email headers. Information Services personnel may not intentionally access the content of email or stored files without the permission of the account holder unless there is a situation that threatens the operation of the system. Occasionally, however, because of the way the systems identify and handle problems, Information Services personnel cannot avoid observing the

contents of email and other files. Information Services personnel shall peruse these emails and/or stored files as little as possible in order to perform the necessary task. If Information Services personnel must observe content, they shall treat the information or content with strict confidentiality.

B. Legal Compliance

The University is required to comply with all valid court orders, search warrants, subpoenas, discovery requests, and statutory or regulatory requirements for preservation or production of documents, including e-mail messages. The University's legal obligations may include preservation, inspection, monitoring, and/or disclosure of email and/or stored files.

If the University is subject to a court order, search warrant, subpoena, discovery request or other legal obligation to preserve, inspect, monitor or produce email and/or stored files, the appropriate University official and the account holder shall be notified, unless the order obligates non-disclosure. For faculty accounts the appropriate University official is the Provost; for staff accounts the appropriate University official is the Associate Vice President of Human Resources; for student accounts the appropriate University official is the Registrar.

When the University is involved or anticipates involvement in litigation or a government investigation or when University officials have reason to believe that there has been a violation of applicable law or policy, it may become necessary to preserve certain documents and records, including emails and electronic files. In such event, the University General Counsel will send a document preservation memo to all members of the faculty and staff who may be in possession of relevant documents and records. All recipients of the document preservation memorandum must take all reasonable precautions to ensure that the documents and records described in the memorandum are preserved, without modification, until further notice.

C. Emergency Situations

The University may access electronic files or email when access or disclosure is needed to prevent the likelihood of imminent significant harm to persons or property. Even though the situation is deemed an emergency, authorization shall still be sought from the appropriate official. Depending on the emergency and circumstances, notification may not occur until after the situation is resolved. For faculty accounts the appropriate University official is the Provost; for staff accounts the appropriate University official is the Associate Vice President of Human

Resources; for student accounts the appropriate University official is the Registrar. Notification of the actions taken shall be given to the account holder.

D. Other Compelling Circumstances

i. In the circumstance when access to stored files or email is necessary to conduct University business and the employee is no longer working at the University or cannot be contacted, an appropriate University official may authorize access to an employee's email account or electronic files. For faculty accounts the appropriate University official is the Provost; for staff accounts the appropriate University official is the Associate Vice President of Human Resources.

ii. Upon request, access to a deceased person's email and electronic files will be granted to the appropriate University Official. After proper review that Official may, where appropriate, distribute information contained therein to the executor or administrator of a deceased person's estate. For deceased faculty and staff the appropriate University Official is the Associate Vice President of Human Resources, for deceased students the appropriate University official is the Vice President for Student Development. The responsible University Official will consult University Counsel, the Registrar, and the Provost as appropriate.

iii. In the event that an employee is terminated, resigns from or abandons their position at the University the appropriate University official may authorize access to that employee's email account or electronic files if needed to conduct University business. For faculty accounts the appropriate University official is the Provost; for staff accounts the appropriate University official is the Associate Vice President of Human Resources.

Preservation of Email

Users of the University's electronic mail system should be aware that, even though the sender and recipient have discarded their copies of a particular email, back-up copies of discarded email exist for a while, and can be retrieved if necessary. Systems are routinely "backed up" to protect system reliability and integrity, and to prevent potential loss of data. The back-up process results in the copying of data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of the email. As a rule, backup tapes of the email system are kept for

approximately 30 days. Non-standard system backup tapes may be kept longer. Please refer to the Computer Systems Backup Policy.

No Guarantee of Confidentiality

Information Services staff follow sound professional practices in providing for the security of the email, data, application programs, and system programs under their control. However even best professional practices and protections are not infallible and the security and confidentiality of our systems and data cannot be guaranteed. In addition, the recipient of an email message may forward it to persons who were not intended to see it. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters. Confidential Information should never be sent in an unencrypted email message.

7. Data Exposure Plan

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. The Data Exposure Policy outlines an action plan for our initial response.

Policy Revision History

Version	Date Revised	Author	Comments
1.0	8/1/2011	Kathy Monday	Original version
1.1	12/30/2012	Anthony Head	Minor revisions and web links added.
1.2	2/26/2014	Melody Kimball	Formatting and updated links
1.3	2/26/2014	Kathy Monday	Bullet #6 added to section 3. Responsibilities Related to the Storage, Access, and Use of University Administrative Information
1.4	9/11/2015	Kathy Monday	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.