IRM-012

Privacy and Confidentiality of University Information

Effective Date Monday, October 23, 2017

Status Final

Last Revised Wednesday, December 21, 2022

Policy Type University

Contact Office University Information Security (InfoSec)

Oversight Executive
Vice President and Chief Information Officer

Applies To
Academic Division, the Medical Center, the College at Wise, and University-Associated Organizations.

Table of Contents

Policy Statement
I. Monitoring and Access
1. Monitoring and/or Access without further Authorization or Notification
2. Monitoring and/or Access Requiring Official University Review and Approval
3. Accessing Electronically Stored Information of a Deceased Person
II. Compliance with Policy
Procedures

Reason for Policy

The University may access *records* or monitor *record systems or communications* that are under the control of its employees. Furthermore, because the University permits some latitude for employees to use University resources to conduct University business off-grounds and to conduct incidental personal matters at their work sites, *work-related records* and employees' *personal records* may be located in the same place.

The University is committed to the privacy of individuals and safeguarding information about individuals subject to limitations imposed by local, state, and federal law and other provisions described herein.

No user has any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the Commonwealth's equipment and/or access. The University has the right to monitor any and all aspects of their computer systems and to do so at any time, without notice, and without the user's permission.

The University holds as core values the principles of academic freedom and free expression. This policy takes into consideration these principles.

Definition of Terms

Access (to data)

The capacity for data users to enter, modify, delete, view, copy, or download data.

Data Users

Individuals who acknowledge acceptance of their responsibilities, as described in this policy, and its associated standards and procedures, to protect and appropriately use data to which they are given access; and meet all prerequisite requirements, e.g., attend training before being granted access.

Authorizing Official (2)

An individual at the University who is authorized to grant a request to access Electronically Stored Information (ESI). This may include an individual who has been designated, either permanently or temporarily, by another individual to serve in the role of authorizing official on their behalf. The authorizing official (approver) typically would be from within the same department, business unit, or reporting area, and must be at least two levels above the affected individual(s) on an organizational chart (except where the affected individual is the president or vice-president). The authorizing official is a person in a higher-level position of authority who is able to determine appropriateness and reasonableness after reviewing the applicable policies and standards related to the request. For most situations, the authorizing official will be either a department chair or head, or their assigned designee; or the President or delegated representative, such as the Vice-Presidents and Deans or their assigned designee, depending on the affected user and requested access.

Electronic Communications

Includes telephone communications, "phone mail," or voicemail, e-mail, computer files, text files, and any data traversing the University network or stored on University IT resources.

Electronically Stored Information (ESI)

Information created, manipulated, stored, or accessed in digital or electronic form.

Employee (5)

An individual who is an *employee (2)*, *contractor employee*, *medical center employee*, and/or *affiliated organization employee*, as well anyone else to whom University IT resources have been extended. These include, but are not limited to, recently terminated employees whose access to University IT resources have not yet been terminated, deleted, or transferred, and individuals whose University IT resources continue between periods of employment. This also includes student workers, volunteers, and other individuals who may be using state-owned or University IT resources and carrying out University work.

Affiliated Organization Employee

An individual who is an employee of one of the officially recognized University-Affiliated Organizations.

Contractor Employee

An individual who is an employee of a firm that has a formal contractual relationship with the University and has been assigned to work at the University for the duration of the contract.

Employee (2)

As used in this policy, includes all faculty (teaching, research, administrative and professional), professional research staff, university and classified staff employed by the University in any capacity, whether full-time or part-time, and all those employees in a wage or temporary status.

Medical Center Employees

Individuals employed by the University of Virginia Medical Center in any capacity.

Information Technology (IT) Resources

All resources owned, leased, managed, controlled, or contracted by the University involving networking, computing, electronic communication, and the management and storage of electronic data regardless of the source of funds including, but not limited to:

- Networks (virtual and physical), networking equipment, and associated wiring including, but not limited to: gateways, routers, switches, wireless access points, concentrators, firewalls, and Internet-protocol telephony devices.
- Electronic devices containing computer processors including, but not limited to: computers, laptops, desktops, servers (virtual or physical), smart phones, tablets, digital assistants, printers, copiers, network-aware devices with embedded electronic systems (i.e., “Internet of things”), and supervisory control and data acquisition (SCADA) and industrial control systems.
- Electronic data storage devices including, but not limited to: internal and external storage devices (e.g., solid state and hard drives, USB thumb drives, Bluetooth connected storage devices), magnetic tapes, diskettes, CDs, DVDs.
- Artificial intelligence tools, including generative AI tools such as UVA Copilot and UVAChat+.
- Software including, but not limited to: applications, databases, content management systems, web services, and print services.
- Electronic data in transmission and at rest.
- Network and communications access and associated privilege.
- Account access and associated privileges to any other IT resource.

Inquiry

Gathering information and initial fact-finding to determine whether an allegation or apparent instance of research misconduct warrants an investigation.

Investigation

The formal development of a factual record and the examination and evaluation of that record to determine if misconduct has occurred, and, if so, to determine the responsible person and the seriousness of the misconduct.

Protected Information

Refers to information that is linked to a person’s identity, such as Social Security Number (SSN), driver’s license number, financial information, and/or protected health information (PHI).

Record

Any document, file, computer program, database, image, recording, or other means of expressing information in either electronic or non-electronic form.

University Record

Recorded information that documents a transaction or activity by or with any appointed board member, officer, or employee of the University. Regardless of physical form or characteristic, the recorded information is a University record if it is produced, collected, received or retained in pursuance of law or in connection with the transaction of university business. The medium upon which such information is recorded has no bearing on the determination of whether the recording is a University record. University records include but are not limited to: personnel records, student records, research records, financial records, patient records, and administrative records. Record formats/media include but are not limited to: email, electronic databases, electronic files, paper, audio, video, and images (photographs).

Research Record

One type of University record that includes, but is not limited to: grant or contract applications, whether funded or unfunded; grant or contract progress and other reports; laboratory notebooks; notes; correspondence; videos; photographs; X-ray film; slides; biological materials; computer files and printouts; manuscripts and publications; equipment use logs; laboratory procurement records; animal facility records; human and animal subject protocols; consent forms; medical charts; and patient research files. In addition, research records include any data, document, computer file, computer diskette, or any other written or non-written account or object that reasonably may be expected to provide evidence or information regarding the proposed, conducted, or reported research that constitutes the subject of an allegation of research misconduct.

User

Everyone who uses University IT resources. This includes all account holders and users of University IT resources including, but not limited to: students, applicants, faculty, staff, medical center employees, contractors, University-Associated Organization employees, guests, and affiliates of any kind.

Policy Statement

The University, as steward of public resources and electronic information, shall respond to requests for electronic information in an orderly manner consistent with state and federal law. This policy applies to all users of the University's information technology resources, regardless of location or affiliation.

Release of Information: Except as provided below, the University may not release protected information about any aspect of an individual's association with the University without the prior written consent of the individual concerned or unless legally required (e.g., Virginia Freedom of Information Act (FOIA) or legal request). Within the University, access to such records shall be restricted to authorized personnel for authorized reasons, as determined by the President or their delegated representative, such as the Vice-Presidents and Deans, and such others as are agreed to in writing by the individual concerned.

Except as provided below, the employees of the University will not monitor the content of electronic communications of its users including personal and University records, files, and data, nor will it examine the content of a user's electronic communications or other electronic files stored on its systems except under approved circumstances**.**

I. **Monitoring and Access:**

1. **Monitoring and/or Access without further Authorization or Notification:**
   Legal or administrative circumstances where monitoring and/or access may occur without further

authorization or notification include:

- Communications or files subject to legal orders or demands (e.g., subpoena, warrants, and national security letter) or requested in accord with FOIA.
- Supervisor and/or Internal Audit review of University telephone system local or long-distance call records.
- Electronic communications or files that have been inadvertently exposed to technical staff who are operating in good faith to resolve technical problems. When technical staff inadvertently discovers potentially illegal content in communications or files, they are required to report it. Otherwise, the University expects technical staff to treat such communications and files of users as private.
- Routine administrative functions, such as security tests to maintain and/or verify the security and/or integrity and/or availability of the University's IT resources, e.g., password testing to identify guessable passwords, investigations of attempted access into systems by unauthorized persons, or email scanning for malware. See policy IRM-004, Information Security of University Technology Resources for additional details.
- Officially sanctioned research projects or projects authorized by the University to be conducted under a data use agreement that limits the disclosure of protected information.

2. **Monitoring and/or Access Requiring Official University Review and Approval:**
Circumstances where monitoring and/or access requires official University review and approval by an authorizing official who is the President or the relevant vice president (or delegate) responsible for the affected user (e.g., employee or student):
    - Business continuity of the University to proceed [e.g., access to data associated with a user (e.g., employee) who has been terminated, separated, is pending termination or separation, is deceased, is on extended sick leave, or is otherwise unavailable].
    - An inquiry, assessment, or investigation into violation(s) of law or policy, or in response to potential or actual litigation.
    - Requests for electronically stored information (ESI) from members of the University's Honor Committee or Judiciary Committee, the Title IX Coordinator and/or designee acting under the University's Policy on Sexual and Gender-Based Harassment and Other Forms of Interpersonal Violence, or faculty conducting individual student-academic-issue investigations.
    - Emergency situations involving a potential threat of harm to persons or property as determined by an authorizing official who is the President or the relevant vice president (or delegate) in consultation with University Counsel.
    - Those units of the University that engage in routine monitoring or examination of employee(s) electronic communications or files as part of the work environment must inform the affected employee(s) in advance, via a written communication (e.g., policy statement) that such monitoring or examination will be taking place.

3. **Accessing Electronically Stored Information of a Deceased Person:**
The University will not grant access to personal data from a deceased user's electronically stored information in the custody of the University without the prior written consent of the deceased individual or as required by law or legal requests [e.g., Uniform Fiduciary Access to Digital Assets Act (UFADA)]. University Records within that electronically stored information may be accessed in accordance with the Electronically Stored Information Release Procedures.

II. **Compliance with Policy:**
Any misuse of data or IT resources may result in limitation or revocation of access to University IT resources. In addition, failure to comply with requirements of this policy and/or its standards may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies, and may also violate federal, state, or local laws.

Questions about this policy should be directed to University Information Security (InfoSec).

Procedures

Privacy and Confidentiality	
Standards and Procedures	
Standards	**Procedures**
ESI Release	ESI Release
	Exceptions

Responsible Computing Handbook for Faculty and Staff

Related Information

See related Guidance for Vice Presidents on Policy on Monitoring/Review of Employee Electronic Communications or Files document
The Commonwealth of Virginia Human Resource Policy 1.75: Use of Electronic Communications and Social Media
Commonwealth of Virginia Freedom of Information Act (FOIA)
Stored Wire and Electronic Communications And Transactional Records Access
Uniform Fiduciary Access to Digital Assets Act (UFADA)

Major Category Information Resource Management

Next Scheduled Review Sunday, December 21, 2025

Revision History Revised 12/21/22; Updated definition 5/15/19; Revised 10/23/17.

Supercedes Policy Text

Employee Electronic Communication/File Monitoring and/or Review; Virginia.edu Privacy Statement; Information Release (Requests for Electronically Stored Information).

Approved By Policy Review Committee

Approved Date Tuesday, June 27, 2017