IRM-002

Acceptable Use of the University's Information Technology Resources

Effective Date Monday, October 23, 2017

Status Final

Last Revised Tuesday, October 29, 2024

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

Reason for Policy

Use of the University's information technology (IT) resources shall support the mission of the University in teaching, research, public service, and healthcare. Users of the University's IT resources are responsible for using these resources appropriately and respecting the rights of others.

Definition of Terms

Information Technology (IT) Resources

Description

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.

Non-Student Users

Description All users except for those whose sole affiliation with the University is student or applicant.

Public Information Technology (IT) Resources

Description

IT resources that are available to broad groups of users within the University community. They include but are not limited to: public-access computer facilities, shared multi-user computing systems, and the network services that Information Technology Services (ITS) and all other University schools and departments manage. The word “public,” in this context, describes a resource that is available broadly to members of the University community. It does not imply that these resources are available to persons from outside the University community.

University Records

Description

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, messaging (texts, instant messaging, etc.), posts (social media or collaboration software), databases, electronic files, paper, audio, video, and images (digital and printed).

User

Description

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

All users of University IT resources are required to use them in an ethical, professional, and legal manner. This policy applies to all users of the University's information technology (IT) resources, regardless of location or person's affiliation.

Users must be granted University IT resource accounts in accordance with the Accounts Provisioning and De-provisioning Standard.

1. **Acceptable Use Requirements:**
   All users agree to ensure the confidentiality and integrity of the University's IT resources. All users must:

   - Abide by the policies, standards, and procedures for appropriate usage for the University's IT resources that they access, including the Acceptable Use Standards and Procedures.
   - Respect the intended use of all the University's IT resources and public IT resources, typically for supporting the mission of the University. All unauthorized use is prohibited. Unauthorized use includes, but is not limited to bitcoin mining, circumventing IT resources safeguards (i.e., hacking), or impeding the IT activities of others. With the exception of GenAI tools, incidental personal use is permitted. (See policy PRM-011: Use of Working Time and University Equipment for Personal or Commercial Purposes.)
   - Follow the rules and regulations governing the use of public IT resources and University equipment. The University expects all users to cooperate in using public IT resources for their intended purposes and in discontinuing their access when requested to do so.
   - Report known or reasonable suspicion of misuse of University IT resources. (See policies: GOV-002: Reporting Fraudulent Transactions, HRM-002: Issuance and Use of University Identification Cards, FIN-044: Use of the University Travel and Expense Card, STAF-003: Statement of Students' Rights and Responsibilities.)
   - Complete all required security training required to obtain and/or maintain access, which includes all users of the High Security Virtual Private Network (HSVPN) and all users of systems governed by legal, regulatory, or contractual obligations requiring security training.

   Users should:

   - Complete either the University's or Health System's online security awareness training at least annually.

   Users must not:

   - Divulge or share passwords, PINs, private keys, hardware tokens, or similar authentication elements with anyone else.
   - Obtain or attempt to obtain unauthorized access to the University's IT resources.
   - Circumvent or attempt to circumvent security controls on the University's IT resources.
   - Allow unauthorized users access to the University's IT resources.
   - Exploit sessions left open, or otherwise misappropriate, assume, or steal the "identity" of another user. (See Authentication Standard and UVA Health System Policy IT-002: Use of Electronic Information and Systems.)
   - Violate the privacy of others through access or use of the University's IT resources. (See policy IRM-012: Privacy and Confidentiality of University Information and UVA Health System Policy INM-001: Requirements Concerning Confidential Information.)

- Use the University's IT resources to access, use, copy, distribute, or otherwise reproduce or make available to others any copyright-protected materials, including digital materials and software, except as permitted under copyright law (especially with respect to "fair use") or specific license. (See Copyright Act.)

In addition to the above, all Non-Student Users:

- Must not utilize University-owned or University-leased computer equipment to access, download, print or store any information infrastructure files or services having sexually explicit content except to the extent required in conjunction with a bona fide, University-approved research project or other University-approved undertaking. (See § 2.2-2827. Restrictions on State Employee Access to Information Infrastructure.)
- Must not download or use any application, including TikTok or WeChat, or access any website developed by ByteDance Ltd. or Tencent Holdings Ltd. (i) on any University-issued device or University-owned or University-leased equipment or (ii) while connected to any wired or wireless Internet network owned, operated, or maintained by the University, except to the extent authorized (by the Superintendent of State Police or the chief law-enforcement officer of the appropriate locality or institution of higher education) for the purpose of allowing participation in law-enforcement-related matters. (See § 2.2-5514.1. Prohibited applications and websites.)
- Are subject to State Policy 1.75: Use of Electronic Communications and Social Media.
- Must disclose to their supervisor any potential conflicts related to their access to information or ability to transact in a University system containing sensitive or highly sensitive data. (See policy IRM-003: Data Protection of University Information for the definitions of sensitive data and highly sensitive data.) For example, an individual who has access to a University system that records grades or student financial information and is also a parent of an enrolled student must disclose that potential conflict. (Supervisors should consult SEC-037: Networks, Systems, and Facilities Access & Revocation and the Issue & Return of Tangible Personal Property for what to do with reported conflicts.)
- Are prohibited from commercial use of IT Resources and University Records, but, with the exception of GenAI tools, incidental personal use is permitted. (See policy PRM-011: Use of Working Time and University Equipment for Personal or Commercial Purposes.)

2. **University IT Resources:**
   All users agree to protect the University's IT resources.
   - Only Information Technology Services (ITS), Health Information and Technology, or their designees are authorized to:
     - Attach networking equipment (including, but not limited to, routers, switches, wireless access points, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) servers, etc.) to the University network or modify University network infrastructure (e.g., building copper and fiber cable plant, outlet wiring) (see Network Equipment Standard); or
     - Provide for external physical connections to the University's network (e.g., connections to an external internet service provider) (see Network Equipment Standard).
   - Persons responsible for the University's IT resources must maintain these resources in a secure state in accordance with applicable legal, regulatory, and contractual requirements, as well as University policies, standards, and procedures. (See policy IRM-004: Information Security of University Technology Resources and UVA Health System policy IMN-001: Requirements Concerning Confidential Information.)
   - Users must protect all data accessed or used. Users must recognize that certain data are sensitive and must limit their access to such data to authorized uses in direct performance of their official duties. (See policy IRM-003: Data Protection of University Information.)

- Users must recognize that the use of certain IT resources and data is restricted by legal, regulatory, and/or contractual requirements, as well as other University policies (such as IRM-006: Mass Digital Communications; IRM-013: Issuance of an Emergency Notification; and EXT-015: Endorsement of External Entities and Products).

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

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

Procedures

Acceptable Use	
Standards and Procedures	
Standards	**Procedures**
Accounts Provisioning/Deprovisioning	
Authentication	
Connecting Network Equipment	Connecting Network Equipment
Copyright of Digital Materials	Copyright of Digital Materials
Electronic Access Requirements	Exceptions
Email Alias	
Responsible Disclosure	

Virginia.edu Subdomain Naming Standard	

Responsible Computing Handbook for Faculty and Staff
Responsible Computing Handbook for Students

Related Information

IRM-003: Data Protection of University Information
IRM-004: Information Security of University Technology Resources
IRM-006: Mass Digital Communications
IRM-012: Privacy and Confidentiality of University Information
IRM-017: Records and Information Management
PRM-011: Use of Working Time and University Equipment for Personal or Commercial Purposes
SEC-037: Networks, Systems, & Facilities Access and Revocation and Issuance and Return of Tangible Personal Property

UVA Health System Policy: IT-002: Electronic Information and Systems Use
UVA Health System Policy: IMN-001: Requirements Concerning Confidential Information

State Policy 1.75: Use of Electronic Communications and Social Media
§ 2.2-2827. Restrictions on State Employee Access to Information Infrastructure
§ 2.2-5514.1. Prohibited applications and websites
§ 18.2-374. Production, publication, sale, possession, etc., of obscene items
United States Copyright Act

Major Category Information Resource Management

Next Scheduled Review Sunday, December 21, 2025

Revision History

Updated list of Standards 10/29/24; Removed External Physical Network Standard/Procedure 7/16/24; External Physical Network Connections standard and procedure Added GenAI tools to definition of IT Resources, 2nd and last bullets in Section 1 3/6/24; Added 14th bullet in Section 1 (SB 1459 bars official use of TikTok and WeChat) 7/1/23; Revised 12/21/22, 5/16/20.

Supercedes Policy Text

Ethics in Computer Usage, Obscene Material, Sexually Explicit Material, Communications Systems Policy, Copyright Protection, Digital Copyright Protection, Information Access

Approved By Policy Review Committee

Approved Date Tuesday, June 27, 2017