SEC-037

Networks, Systems, and Facilities Access & Revocation and the Issue & Return of Tangible Personal Property

Effective Date Friday, February 5, 2016

Status Final

Last Revised Wednesday, February 15, 2023

Policy Type University

Contact Office
Executive Vice President and Chief Operating Officer (Office of the)

Oversight Executive
Executive Vice President and Chief Operating Officer Executive Vice President and Provost

Applies To
Academic Division The College at Wise

Table of Contents

Reason for Policy

The University is committed to protecting the safety, security, privacy, and property of the institution. This policy sets forth responsibilities for authorization and revocation of access to University systems and networks and the use and return of University tangible property upon transfer or separation.

Definition of Terms

Data Stewards

University officials who have operational oversight for the life cycle of a specific data domain including the definition, intake, and usage of the data. Data Stewards will oversee the development, maintenance, and enforcement of appropriate policies, standards, and procedures for the use of data in their functional areas, including defining criteria for data access authorization and have final sign-off authority for users seeking to access, retrieve, manipulate, or view data for their respective data domains.

Data Stewards are assigned by, and are accountable to, Data Trustees. Institutional data stewards help define, implement, and enforce data management policies and procedures within their specific data domain. Institutional data stewards have delegated responsibility for all aspects of how data is acquired, used, stored and protected throughout its entire lifecycle from acquisition through disposition.

Data Domain

The entire collection of data for which a University employee assigned the role and responsibilities of a Data Trustee, Data Steward, or Deputy Data Steward is responsible. Each Data Domain (or subdomain) has a Data Trustee and a Data Steward. Deputy Data Stewards are appointed as needed by Data Stewards to complete data stewardship activities. The data domain also includes rules and processes related to the data.

Highly Sensitive Data

Data that require restrictions on access under the law or that may be protected from release in accordance with all applicable laws or regulations, such as Virginia Code § 18.2-186.6. Breach of Personal Information Notification. Highly Sensitive data (HSD) currently include personal information that can lead to identity theft. HSD also includes health information that reveals an individual's health condition and/or medical history.

Specific examples include, but are not limited to:

- *Any store or file of passwords or user-ids and passwords* on any multi-user system or computer.
- *Personal information that, if exposed, can lead to identity theft.* This may include a personal identifier (e.g., name, date of birth) as well as one of the following elements:
    - Social security number;
    - Driver's license number or state identification card number issued in lieu of a driver's license number;
    - Passport number;
    - Financial account number in combination with any required security code, access code, or password that would permit access to a financial account;
    - Credit card or debit card number, including any cardholder data in any form on a payment card; or
    - Military Identification Number.
- *Health information, which is any information that, if exposed, can reveal an individual's health condition and/or history of health services use, including information defined by* Health Insurance Portability and Accountability Act *(HIPAA) as protected health information (PHI).*
- **Cardholder Data (CHD):** Primary cardholder account number that identifies the issuer and a particular cardholder account, which can include cardholder name, expiration date and/or service code.

Note: Credit card numbers must never be stored either alone or in combination with any other identifiers.

Also considered HSD are any form of personally identifying information in combination with social security number (SSN), driver's license number, passport number, financial account number and required security code, and/or military ID number. For example, computing ID and driver's license number, or home address and SSN.

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.

Supervisor

Any person who has authority to undertake or recommend tangible employment decisions affecting an employee or academic decisions affecting a student; or to direct an employee’s work activities or a student’s academic activities. Examples include faculty members to whom work-study students report and team lead workers who, from time to time, monitor other employees’ performance or direct their work.

Tangible Personal Property (1)

Property, other than real property, which may be seen, weighed, measured, felt, or touched, or is in any other manner perceptible to the senses. Under Virginia law, the term "tangible personal property" does not include stocks, bonds, notes, insurance, or other obligations or securities (as defined in VA Code § 58.1-602).

Unaffiliated Persons

Any person or party who is not an affiliated person (e.g., businesses, non-profit organizations, independent contractors).

University Equipment

University owned or leased property used to assist in performing an activity or function (e.g., hand tools, power tools, audio-visual equipment). University equipment does not include University infrastructure (e.g., networks, buildings); office furnishings that remain in the location designated for their use (e.g., desks, file cabinets, bookcases); or telephone and computing resources that are covered by other specific policies.

University Facility

Any defined space of the University, including a room, lab, series of labs, building, or controlled outdoor area.

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).

University-Associated Organization (UAO)

An independent and separately incorporated legal entity, officially recognized by the University, subject to an executed UAO- Memorandum of Understanding (MOU), and meeting all the following criteria:

- Organized and exists under Virginia law and in good standing with the State Corporation Commission.
- Qualifies as a tax-exempt organization.
- Exists and operates for the benefit of the University or one or more of its units by providing one or more of the following support functions: fundraising, asset management, programs, and services.
- Not an agency, organization, corporation, or unit of the University or the Commonwealth of Virginia.

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.

Volunteer

An individual permitted under specific conditions to perform agreed upon activities on behalf of the University, but not in an employment capacity and therefore is not entitled to compensation and employment benefits.

Policy Statement

Regulating access to and use of University resources (e.g., University equipment, IT resources, tangible personal property, records, and facilities) is critical to responsible stewardship and effective internal control. Procedures for initial authorization, renewal, and revocation of access or use privileges must be risk-based and consistent with all applicable University policies, laws, regulations, and contractual requirements.

1. **Responsibilities:**
   Information Technology Services (ITS) is responsible for:

   - Providing a tool and technical support to facilitate periodic campaigns to review and reauthorize or revoke user access privileges for *University IT Systems*.

     > A *University IT System* is an electronic system used to conduct University business (i.e., academic, financial, human resources, research/scholarship, and other operations), including any *system of record*, whether or not the associated hardware and software are owned and maintained by the University (e.g., on premises (on-prem), cloud or vendor-provided, and software-as-a-service (SaaS) solutions). A *System of Record* is a subset of University IT Systems used to transact institutional business and serve as the authoritative data source for institutional business records (i.e., human resources, financial and academic records).

   - Providing a tool and technical support to facilitate maintenance of an inventory of *systems of record* that at a minimum identifies the following:

    - A *Functional Owner* – the leader of the University unit responsible for the business processes performed by a *University IT system*.
    - A *Technical Contact* - the system administrator or technical lead responsible for maintaining the security and functionality of a *University IT system*.
    - The sensitivity level of the data within the system (i.e., University data classification for the most sensitive data with the system).

Functional Owners are responsible for:

- Designating the *Technical Contact* and providing adequate resources to maintain the functionality and security of the *University IT system(s)* in compliance with applicable University policies and standards, laws, regulations, and other external requirements.
- Registering *systems of record* in the inventory and updating or reconfirming the required information at least annually.
- Coordinating with data stewards to establish processes and procedures for initial access (may be automated or by request) and timely removal/revocation when access is no longer required or appropriate (e.g., change in job duties or position, abuse or misuse of the system or data, or separation from the University).
- Designating conflicting user roles/privileges and establishing procedures to maintain appropriate segregation of duties, including review and approval or denial of exception requests and management of potential conflicts when necessary.

Supervisors, including any sponsor of an unaffiliated person (e.g., contractor, consultant, visiting faculty, research collaborator, government official, etc.), volunteer, or employee of a University-Associated Organization (UAO) who requires University credentials (username and password, i.e., a sponsored account) to access networks, systems, and facilities and/or will be issued University tangible personal property (including University equipment) to fulfill their commitment to the University, are responsible for:

- Initiating requests to enable or revoke access privileges to University IT systems as well as other University IT resources and University facilities consistent with job duties and assigned tasks.
- Issuing University tangible personal property necessary for the performance of job duties and assigned tasks and facilitating its return when warranted (e.g., internal transfer, separation from the University, or end of assigned tasks).
- Following UVA Human Resources (UVA HR) policies and procedures related to the onboarding and offboarding of employees including, but not limited to, making sure a termination is entered into the human resources management system on or before the employee's last day.
- Following Information Technology Services procedures to appropriately end-dated sponsored accounts and deprovision access to all University IT system privileges granted in association with the activities for which the sponsored account was originally issued.
- Identifying and managing potential conflicts in an employee's technology-related responsibilities to prevent potential systems misuse. (See policy GOV-002: Reporting and Investigation of Fraudulent Transactions.)
- Taking corrective action to address any identified misuse of University resources.

Users are responsible for disclosing to their supervisor, any potential conflicts related to their access to University records or ability to transact in a University IT system. For example, an individual who has access to a University IT system that records grades or student financial information and is also a parent of an enrolled student must disclose that potential conflict.

2. **Additional Requirements for Systems of Record:**
   Systems of record are critical to University operations and typically contain Highly Sensitive Data (HSD) for a large population of individuals and therefore warrant additional safeguarding measures.

   The Functional Owner of a system of record must either 1) administer a process at least annually (beginning the first full fiscal year after go-live for new systems) to review and reauthorize or revoke user privileges (excluding self-service) providing access to HSD or elevated system privileges (e.g., system administrators); or 2) implement business process that achieve the following:

   - Immediately/automatically remove access when an individual leaves their position (e.g., internal transfer or separation from the University).
   - Assure ongoing segregation of duties (or waiver thereof).
   - Monitor for and address potential instances of misuse (e.g., inappropriate access or use of HSD, unauthorized changes to HSD, or fraud).

   Regardless of the method used (i.e., annual review and reauthorization of user privileges or compensating controls via business processes), the functional owner must maintain documentation of the process(es) followed, results, and actions taken. If using an ITS tool to conduct an annual review and reauthorization of user privileges, (campaign) such documentation may be retained within the ITS tool.

   For the purposes of compliance with this section, the following positions are designated as the Functional Owners of the system(s) of record for their respective business areas:
   - Assistant Vice President for Financial Operations, UVAFinance
   - Assistant Vice President for HR Service, UVA Human Resources
   - Vice Provost for Enrollment, Provost’s Office
   - Vice Chancellor for Finance and Operations, College at Wise

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

   Questions about this policy should be directed to the appropriate Functional Owner as listed in Section 2 above.

Procedures

IT Checklist for Leaving UVA
Onboarding and Offboarding Procedures
Information on Sponsored Accounts (e.g., how to request, modify, and revoke)
Vendor Security Review Standard (e.g., required review of third-party vendors handling HSD and/or delivering mission-critical services)

Related Information

This list is not comprehensive as requirements will vary among systems and data types.
FIN-021: Internal Controls
FIN-044: Use of the University Travel and Expense Card

FIN-054: Employee Obligation to Report Potential Conflicts of Interest
GOV-002: Reporting and Investigation of Fraudulent Transactions
HRM-002: Issuance and Use of University Identification Cards
IRM-002: Acceptable Use of the University's Information Technology Resources
IRM-003: Data Protection of University Information
SEC-038: Management of the University Keyed System (Key and Lock Policy)

Parking & Transportation – for parking permits, including service vehicle parking.
University ID Card Office

ACC-001: Health System Identification Badges
ACC-002: Access Control to Health System Facilities
HR405: Separation from Employment

Major Category Safety, Security and Environmental Quality

Next Scheduled Review Sunday, February 15, 2026

Revision History

Revised 2/15/23; Edited Section 7 4/15/20; Revised 2/21/20; Updated definition 5/15/19.

Applies To Text

Academic Division and the College at Wise.

Category Cross Reference

Human Resource Management

Supercedes Policy Text

SEC-037: Access Privileges and Return of University Property; Responsibility of Managers and Other UVa Officials for Access Privileges

Last modified March 12, 2024 - 10:45am

Approved By Policy Review Committee

Approved Date February 5, 2016 - 12:00pm