UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-4009	**Policy Title:**	Identity and Access Management Policy
Effective:	10/10/2025	**Responsible Office:**	Information Services
Date Approved:	10/10/2025	**Approval:**	Vice President for Information Services and Chief Information Officer
Replaces Policy Dated:	N/A	**Responsible University Official:**	Vice President for Information Services and Chief Information Officer

PURPOSE:

To establish a framework that facilitates appropriate access by authorized individuals and entities to university electronic systems, data, and resources at the right time, and for legitimate academic, research, and administrative purposes.

SCOPE:

This policy applies to anyone who accesses University of Richmond (UR) data, electronic systems, software applications, or data networks as well as those who design, implement, or manage associated information services.

INDEX:

POLICY STATEMENT:

IRM-4009.1 – Definitions

Access: Access is the ability to utilize various university electronic systems, services, and resources. This includes accessing cloud- and campus-hosted data and applications, data networks, computing devices, and others.

Application: Software designed to address various needs, ranging from simple utilities and productivity tools to complex enterprise system solutions. Typically, they have a user interface that allows people to digitally interact with them, and they may also rely on data processing, storage and communication functionality to accomplish their intended purpose.

Authentication: Authentication is the process by which an electronic system or software application confirms that a person or device really is who or what it is claiming to be and through which access to the requested resource is authorized. Strong authentication protocols help both to protect personal and university information and prevent misuse of university resources.

Authorization: Authorizations are implicit or explicit permissions to use a resource associated with a digital account. Once the user of an account is authenticated, a system or resource determines if the person requesting access is authorized to use it.

Deprovisioning: The removal of computing accounts associated with an identity. The process can be automated or manual, or a mixture of both.

Directory Services: Systems for storing and maintaining information about identities and resources. Directory services are often referred to as directories, user stores, or identity stores, and they store information such as usernames, passwords, and user preferences. Directory services are used to provision user accounts, manage access privileges and monitor and control access to software applications. Active Directory and OpenLDAP are two examples of directory services.

Entitlements: Entitlements, also known as authorizations, privileges, or permissions, are access policies used to manage electronic access to data, information services, and software applications. They define what a given identity is authorized to access and what actions can be performed.

- Birthright entitlements are granted automatically either implicitly or explicitly in the account creation process and are often related to an individual's affiliation with the university (e.g., employee, student, alumni).
- Application entitlements are requested by an individual but require approval by an application owner or data steward before being granted.

Identity: Digital credentials and characteristics that uniquely represent a person, device, or application within an organization's network. A digital identity can consist of multiple accounts, credentials, and entitlements associated with a single entity or person.

Identity and Access Management (IAM): a security and business discipline that combines policies, processes, and technologies to ensure the right people or devices gain appropriate access to the right assets at the right time for the right reasons, while preventing unauthorized access and fraud.

Least Privilege: The principle of least privilege dictates that users should be granted the minimum necessary access rights to perform their tasks and nothing more. This security concept aims to minimize potential damage from compromised accounts, accidental errors, or malicious attacks by limiting the scope of permissions.

Multi-factor Authentication (MFA): Multi-factor authentication (MFA) is a security measure that requires users to provide more than one form of identification to access an account or system. MFA is a layered approach to security that makes it harder for unauthorized users to gain access to a system, even if one credential is compromised.

Permissions: Specific operations or actions that an authenticated user or entity is allowed to perform on a resource or system. Permissions are a fundamental part of authorization, which determines what an authenticated user can do, after authentication verifies who they are. Permissions are typically assigned to roles, which are then assigned to users, creating a system of access control.

Privileges: The right of an account to perform certain actions on pieces of data in an information service. Elevated privileges are rights that exceed the privileges of a typical user of the system.

Provisioning: The creation, ongoing maintenance, and removal of computing accounts associated with an identity. The process can be automated or manual, or a mixture of both.

Service Accounts**:** A service account is used when it is necessary for electronic systems or software applications to authenticate to other electronic systems or software applications without any association with a person.

User Accounts: A user account is a unique identity assigned to a specific person that allows that person to access a computer, network, or software application. The account may either exist in a central repository to which software applications may connect to consume identity and authentication information, or it may be managed locally on an information system or device.

IRM-4009.2 – Policy Statement

1. Accounts
    a. User Accounts: When supported by the system or application, all user accounts should be created centrally in the directory services repositories hosted by Information Services. If the system or application does not support central authentication, then accounts may be created locally, in which case the creation, deletion, and maintenance of local accounts is the sole responsibility of the appropriate application owner(s).
    b. Service Accounts**:** These accounts should be created sparingly and documented. Their use must be reviewed annually. The password requirements for service accounts must be no less stringent than those for user accounts. Service accounts may not be used by individuals to authenticate. After initial testing, service accounts must be configured to be non-interactive if possible.
    c. Privileged Accounts**:** Certain accounts may have extra privileges related to the management of a device or application. Administrative privilege can be added to either user or service account types. Privileged accounts must utilize Multifactor Authentication (MFA) if that security capability can be configured for the relevant system or application. Accounts with elevated privileges must be closely monitored by Information Services and/or application owners for potential abuse.

2. Authentication

    Information Services (IS) maintains centralized authentication services for the use of both on-premise and cloud-based applications. These services are enumerated in the Authentication Standard associated with this policy. In addition to traditional password-based authentication, IS also provides a centralized multifactor authentication (MFA) service.

Some software applications support their own local credential stores for the purpose of user authentication. This method is often referred to as native or application-level authentication. Applications that are small in scope, with a very limited number of users, may be configured for local authentication. However, central authentication is always preferred. The operational department creating local accounts must define the procedures by which local accounts will be approved and created. The procedures must be consistent with this policy as well as with the University's Acceptable Use Policy.

3. Authorization

The management and maintenance of authorizations is a shared responsibility of Information Services and local application administrators and data stewards. All authorizations must be granted in accordance with the concept of least privilege. Only authorizations that are necessary to perform job tasks should be granted. All others should be denied/disabled.

4. Provisioning
    a. Birthright Entitlements: When an account is created in the University's central identity system, certain authorizations are immediately created with it, such as the ability to authenticate against UR's enterprise authentication systems, access to UR's data network, and several online resources. Accounts are granted these authorizations automatically during the account creation process managed by Information Services and are often related to an individual's affiliation with the university. Changes in affiliation will automatically result in changes to birthright entitlements.
    b. Requestable Entitlements: These are entitlements that are requested by an individual but that require approval by an application owner or data steward before being granted. All requests should be made, tracked, and fulfilled through the online ticketing application (e.g., SpiderTechNet) maintained by Information Services.
    c. Deprovisioning: Information Systems shall be designed and deployed in a way that facilitates timely removal of a person's authorizations and accounts at appropriate times.
    d. Centrally Managed Accounts and Authorizations: Enterprise level accounts or authorizations that are listed in the enterprise directory service and have authentication credentials in UR's enterprise authentication services shall be deprovisioned in accordance with the User Life Cycle Standard associated with this policy.
    e. Local Accounts and Authorizations: When accounts or authorizations are created outside of the central enterprise authentication system, the operational department creating the accounts must define a mechanism to deprovision the accounts in a timely fashion (generally within a few business days unless a specific time frame is requested) and consistent with the conditions expressed in the associated User Life Cycle Standard.

        NOTE: Deprovisioning local accounts must occur promptly upon role change, separation, or termination. It is insufficient to rely on central deprovisioning of accounts as a method of terminating locally deployed authorizations, as the timeliness of account deprovisioning is dependent on factors that are beyond the control of local application administrators.

IRM-4009.3 –Roles and Responsibilities

Information Services – Information technology experts dedicated to maintaining identity management systems that centrally manage digital accounts shall have the following responsibilities:

- create, remove, and maintain digital accounts in centralized enterprise directory services.
- create, remove, and monitor central service accounts.
- create, remove, and monitor central privileged accounts.
- provide and maintain centralized authentication services, including multi-factor authentication.
- manage and maintain authorizations for enterprise software applications.
- manage and maintain a service that grants and revokes birthright entitlements, as appropriate.
- manage and maintain a service for requestable entitlements.
- manage and maintain an auditing service
- maintain a list of enterprise and departmental applications and their respective application owners (available upon request)

Human Resources – Serves as the authoritative source for faculty, staff, student worker, retiree, contractor, and volunteer employment data. Humans Resources has the following responsibilities:

- Ensures timely and accurate entry and update of personnel records in the employee system-of-record to trigger corresponding identity life cycle events for employees (e.g., account provisioning, role changes, and deprovisioning).
- Collaborates with Information Services to verify employment data changes are correctly reflected in identity and access management systems in accordance with institutional policy and regulatory requirements.
- Notifies Information Security immediately of any urgent employee account termination needs (e.g., involuntary separations).

Registrar's Office – Serves as the authoritative source for student academic status and enrollment data. The Registrar's Office has the following responsibilities:

- Ensures timely and accurate entry and update of student records in the student information system-of-record to trigger corresponding identity life cycle events for students (e.g., account provisioning, status changes, and deprovisioning).
- Collaborates with Information Services to verify student data changes are correctly reflected in identity and access management systems in accordance with institutional policy and regulatory requirements.
- Notifies Information Security immediately of any urgent student account termination needs.

Application Owners – For purposes of this policy, application owners are typically operational managers in a functional area responsible for the administration of a departmental software application or computer system. Application owners shall have the following responsibilities:

- manage and maintain all local accounts required on software applications or computer systems that they administer (i.e., provisioning, deprovisioning, auditing, etc.)

- review and approve requests for access to software applications or computer systems that they administer.

Data Stewards – Data stewards are typically senior operational managers in a functional area responsible for a Data Stewardship Domain as defined by the University's Administrative Data Management Policy. Data stewards shall have the following responsibilities:

- review and approve requests for access to data in their assigned Data Stewardship Domain.

Data Management Committee – The Data Management Committee (DMC) is a university-wide committee primarily composed of Data Stewards and Data Supervisors. The DMC is co-chaired by the Director, Institutional Effectiveness and the Assistant Vice President for Systems and Networks. The DMC shall have the following responsibilities:

- reviewing the operational effectiveness of Identity and Access Management policies and procedures and making recommendations for improvement and change.
- providing oversight of all university processes and systems which create, maintain, and report on Identity and Access Management data.
- ensuring regular and appropriate collaborative communication with the IT Governance Steering Committee on operational changes related to Identity and Access Management that may impact business processes.

RELATED POLICIES:

IRM-4004 - Data Security Policy
IRM-4008 - Access to Electronic Files Policy
IRM-4007 - Administrative Data Management Policy
IRM-2001 - Acceptable Use Policy
IRM-4003 - Information Security Policy

POLICY BACKGROUND:

Policy approved on 10/10/2025 following review by President's Cabinet

POLICY CONTACTS:

Vice President for Information Services and Chief Information Officer