Virginia Polytechnic Institute and State University

Enterprise Identity and Access Management

No. 7040

Policy Effective Date:
1/29/2018

Policy Revision Date:
April 11, 2024

Policy Owner:
Sharon Pitt
Vice President for IT & CIO

Policy Author:
(Contact Person)
Brenda van Gelder
Executive Director, IT Policy & Strategic Engagement

Affected Parties:
Undergraduate
Graduate
Faculty
Staff
Other

1.0 Purpose

This policy governs Virginia Tech's Identity and Access Management (IAM) functions including digital identities, authenticators, and authorizations of all entities affiliated with the university. The policy and its associated standards, guidelines, procedures, and technical specifications promote enterprise strategic and operational success through ensuring the confidentiality, integrity, and accessibility of university data. This policy also is a part of Virginia Tech's compliance with national and state laws, regulations, and mandates.

2.0 Policy

The IAM function at Virginia Tech is defined, implemented, and led by the Division of Information Technology (DoIT). The IAM function includes any and all IAM services provided by Virginia Tech.

IAM services include any service providing the functions or capabilities regarding technology resources including account management, password management, identity lifecycle management, authentication, authorization management, access provisioning and de-provisioning, affiliation management, access policy management, and access request processing.

2.1 Scope of Policy

This policy applies to administrative, academic units, or other Virginia Tech organizations as well as all end users that utilize enterprise IAM services, digital identities, authenticators, credentials, and authorizations used for authentication or authorization to university IT services, IT services that support physical access controls, or access to university data.

2.2 IAM Governance

The Division of Information Technology will consult the relevant IT Governance bodies on changes to this policy and its associated standards that carry significant university-wide resource implications as appropriate.

Centralized IAM service and capabilities shall be used by university IT services whenever possible within the bounds of technical and compliance limitations and allowing for approved exceptions in the context of research, instructional, and compliance use cases.

Virginia Tech shall not implement or provide any IAM services except with approval from the Office of the Vice President of Information Technology and CIO which is informed by the relevant IAM Governance Framework working groups. The Division of IT maintains an inventory of registered and approved IAM services.

IT services authorized by data stewards and managers are delegated the responsibility to ensure that directives from the Division of Information Technology and Virginia Tech's IT Governance are effectively implemented and that identity and role-based access data are reliable, available and secure.

All IAM services shall operate in compliance with the defined IT standards for IAM services and under the strategic oversight of the IAM Governance Framework.

2.3 Roles and Responsibilities

In enterprise identity and access management (IAM), IT resource enablement and information security are both critical layers. Every constituent at Virginia Tech uses Virginia Tech identities to one degree or another and therefore has responsibilities in safeguarding university identities and data.

For the responsibilities of each party, see the chart below which delineates the level of accountability for stakeholders that are Responsible (R); Accountable (A); Consulted (C); and Informed (I). This type of chart is often referred to as a "RACI" chart and is provided here to clarify roles that are required to act on this policy and those who need to be consulted or informed but do not need to take specific action.

Division of Information Technology's Secure Identity Services (DoIT)

Role: As the university's central identity and access management unit, SIS is accountable for providing IAM services, capabilities, digital identities that enable secure and appropriate access to university IT resources and data.

Deans, Directors, Department Heads (DDDH)

Role: Those with top level divisional, departmental, or service authority.

Technology/IT Resource Owners

Role: System owners are functional or technical staff responsible for systems run within their organization or by other IT organizations on their behalf.

IT Professionals

Role: IT professionals are any personnel in any organization responsible for the operation of IT systems and services.

End Users

Role: Individual users of VT digital identities.

RACI Chart: A = Accountable, R = Responsible, C = Consulted, I = Informed

Responsibility	DOIT	DDDH	IT Pro	System Owners	End Users
Provide secure enterprise IAM services	A, R	I	C	C	I
Oversee and lead IAM governance framework	A, R	I	C	C	I
Provide consultation and guidance on how to comply with university IAM policies and standards.	A, R	I	C	I	I
Provide information on this policy, standards, and relevant procedures related to this policy and all other responsibilities.	A, R	I	I	I	I
Ensure IT resources are integrated with enterprise IAM services or otherwise approved IAM services	C	I	R	A	I
Obtain approval for running IAM services	C	A	R	I	I
Ensure products implemented (purchased or built) comply with IAM standards	C	A	R	R	I
Ensure all service accounts are used in compliance with all university IAM standards	C	A	R	R	R
Use all VT identities in compliance with all university IAM standards	C	A	R	R	R
Select IT products that comply with IAM standards	C	A	R	R	I

2.4 Ownership of Identity and Access Data: Identifiers, Authenticators, and Authorizations

Identifiers, authenticators, and enterprise authorizations issued and/or assigned by Virginia Tech remain the property of Virginia Tech, and Virginia Tech reserves the right to add, change, delete or revoke identities, authenticators, credentials, or supporting identifiers, attributes, or authorization objects or assignments.

3.0 Procedures

Administrative, academic units, or others needing to register an IAM service can find procedural instructions here: https://sis.vt.edu/governance/iam_service_offerings.html.

4.0 Definitions

Applicant: party that will go through the identity proofing process in order to become a subscriber.

Authentication: the process or action of verifying the asserted identity of an entity.

Authenticator: a mechanism or authentication system used to authenticate (verify) that the entity in a transaction is the owner of the asserted digital identity.

Digital Identity: a digital representation of an entity's real world identity.

Digital Credential: A coupling of an *identifier* and an *authenticator*. An example is a username (identifier) and an authenticator (passphrase). The identifier is used to associate the transaction with a digital identity and an authenticator is used to authenticate the subject of the transaction.

Enterprise: Enterprise in the context of this policy means the entirety of the Virginia Tech business entity. An "Enterprise identifier" is one that is issued by Virginia Tech and/or used broadly across the entirety of Virginia Tech.

Enterprise Authorizations: Authorizations that grant an enterprise digital identity access to university data and/or IT services provided by the university and/or containing university data.

Enterprise Digital Identities: a university created digital representation of a real-world entity or purely digital entity consisting of one or more collected or university generated and assigned data attributes that can be used to differentiate one entity from another.

Entity: In the context of this policy includes but is not limited to a person, system, robot, device, or organization.

The IAM Function: the collective service offering of IAM services and capabilities across the entire university regardless of which unit is offering or operating the service or product.

Identification: the process of differentiating one entity from another.

Identity Proofing: The process by which an applicant verifies the subject's association with their real-world identity.

Non-repudiation: the assurance that someone cannot deny the validity of something such as a transaction in an IT system.

Technology/ IT Resource: Any item such as a computer, tablet, smartphone, or similar device and associated peripherals owned by Virginia Tech or used to store university data, including those in research contracts or private activities associated with the university, and privately owned technology devices that are connected to the Virginia Tech network or used to store university data.

Subscriber: When an applicant successfully completes an identity proofing process, they become a subscriber.

University IT Service: Any IT Service provided by the university for the university community.

5.0 References

Administrative Data Management and Access Policy—University Policy 7100
http://www.policies.vt.edu/7100.pdf

Standard for Administrative Data Management
http://it.vt.edu/content/dam/it_vt_edu/policies/AdministrativeDataManagementStandard.pdf

Acceptable Use and Administration of Computer and Communication Systems—University Policy 7000
http://www.policies.vt.edu/7000.pdf

Acceptable Use Standard
http://www.vt.edu/about/acceptable-use.html

Standard for High Risk Digital Data Protection
https://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf

Standard for Digital Identity Levels of Assurance
https://it.vt.edu/content/dam/it_vt_edu/policies/Standard_for_Personal_Digital_Identity_LOA.pdf

Standard for High Risk Digital Data Protection
(https://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf)

Information Technology Governance Structure and Process
(https://evpcoo.vt.edu/Initiatives/information-technology-governance.html)

6.0 Approval and Revisions

Approved March 30, 2005 by the Vice President for Information Technology, Earving L. Blythe.
September 7, 2006: Technical revisions – (1) policy renumbered to Information Technology Policy 7040 from former General University Policy 2040; (2) – Personnel Services updated to "Human Resources"; (3) references updated.

- Revision 1

  April 1, 2008: Updates to position titles and/or responsibilities due to university reorganization.

- Revision 2

  August 24, 2009: Updates to

  1. reflect unit name change from Information Resource Management (IRM) to Identity Management Services (IMS);
  2. reflect name change from 'Acceptable Use Guidelines' to 'Acceptable Use Standard';
  3. add requirements to the treatment of PID passwords; and
  4. add reference to PID Procedures.

- Revision 3

  Updates to add authentication requirement, add hyperlinks, and move procedural/ implementation details to the Standard for University Enterprise Electronic Login Credentials.

  Approved January 29, 2018 by Vice President for Information Technology and Chief Information Officer, Scott F. Midkiff.

- Revision 4

  Until 2023, policy 7040 governed only the personal identifier known as the University PID; however, there are now multiple personal identifiers and credentials that are used for various University purposes. To be inclusive of the multiple ways in which Virginia Tech identifiers are created, used, and managed, policy 7040 required a comprehensive revision encompassing all aspects of identity credentials.

  Approved April 11, 2024 by Vice President for Information Technology and Chief Information Officer, Sharon Pitt.