Virginia Tech Glossary of Information Technology Terms Found in Policies and Standards

Acceptable use	Refers to the guidelines and rules that define appropriate and lawful behavior when using university computer systems and networks. It is similar to a code of conduct for the digital realm, outlining what users can and cannot do with the organization's technology resources.	Policy 7000 (Acceptable Use and Administration of Computer and Communication Systems)
Access credential	A means of gaining physical access including physical keys, Hokie Passport Cards, fobs, and other access mechanisms provided by the DoIT or the university.	DOIT Facilities Physical Security Standard
Accessibility	As defined by the Americans with Disabilities Act as amended, refers to a site, facility, work environment, service, or program that is easy to approach, enter, operate, participate in, and/or use safely and with dignity by a person with a disability.	Information Technology Accessibility Policy
Assistive technology	Any item, piece of equipment, or product system, whether acquired commercially, modified, or customized, that is used to increase, maintain, or improve functional capabilities of individuals with disabilities.	Information Technology Accessibility Policy
Authentication	The process or action of verifying the asserted identity of an individual, account, or entity.	Enterprise Identity and Access Management Policy
Authentication error	Authentication error is the misuse of credentials, either malicious or intentional, where the person using a credential is not the person to whom the credential was issued.	Standard for Personal Digital Identity Levels of Assurance
Authentication factors	Authentication factors are elements that are used in forming digital credentials to verify a person's identity. The number of different factors used for authentication is directly related to the level of trust a process can place in the validity of the digital credential. As the number of factors increases, so does the level of trust in the credential.	Standard for University Enterprise Electronic Login Credentials Standard for Personal Digital Identity Levels of Assurance
Authenticator	A mechanism or authentication system used to verify a person's digital identity in order to access a secured online resource. Typically, an authenticator is a passphrase or encryption device.	Enterprise Identity and Access Management Policy Standard for Personal Digital Identity Levels of Assurance
Authorized user or visitor	An individual possessing a physical access credential or who is authorized to use or visit the facility, as evidenced by a visitor badge and/or being escorted at all times by a DoIT employee. Visitors are authorized by proxy when on the premises together with one or more authorized persons.	DOIT Facilities Physical Security Standard
Biometric measure	A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.	Standard for University Enterprise Electronic Login Credentials
Computer administrator/ administrative access	An administrator is someone whose account credentials allows them to make changes on a computer/server that will affect other users of the resource. Administrators can change security settings, install software and hardware, access all files on the computer, and make changes to other user accounts.	University Computer Administrator Access Standard

	For example, a managerial role could have administrative access.	
Cookies	Digital cookies, also called browser cookies, are small files that websites store on a user's device to remember information about their browsing session, such as browsing history, login details, and more.	Policy 7030 (Policy on Privacy Statements on Virginia Tech Websites)
Covered data	Refers to the six covered data elements—those university nonpublic data elements specified in this standard (Social Security number, credit card number, debit card number, bank account number, driver's license number, or passport number)—and the covered combination, the occurrence of name and date of birth carried together in a document.	Standard for Securing Web Technology Resources
Custodial relationship	The institution is responsible for the safekeeping and protection of electronic communications data and records.	Policy 7035 (Privacy Policy for Employees' Electronic Communications)
Cybersecurity breach	An event (either intentional or accidental in nature) that jeopardizes the integrity, confidentiality, and/or availability of information or an information system.	Policy 7000 (Acceptable Use and Administration of Computer and Communication Systems)
Data experts	Data experts are operational managers in a functional area with day-to-day responsibilities like managing business processes and establishing the business rules for the production transaction systems.	Standard for Administrative Data Management
Data stewards	Data stewards oversee the capture, maintenance, and dissemination of data for a particular operation, and are appointed by the respective data trustee.	Standard for Administrative Data Management
Data trustees	Data trustees are senior university officials who have planning and policy-making responsibilities for university data.	Standard for Administrative Data Management
Data users	Any individual who accesses university data, whether it's to perform an assigned duty, fulfill their role in the university community, or any other reason	Appropriate Use of Electronic Personnel and Payroll Records
Data vs. information	Data is a building block which, when used in combination and given meaning and context, becomes information. For example, data is like an individual puzzle piece, whereas information is the completed puzzle: the big picture.	Policy on Privacy Statements on Virginia Tech Websites
Department	An organizational unit of the university, typically specializing in a specific field or academic sector.	Policy for Securing Technology Resources and Services
Digital credential	The identifying character strings, plus authentication factors, that are presented to authenticate a person to electronic services. For example, a username (identifier) and an authenticator (passphrase).	Enterprise Identity and Access Management Policy Standard for Personal Digital Identity Levels of Assurance
Domain name	The name of a website that follows "www." For example, "VT" in "www.vt.edu."	Policy 7030 (Policy on Privacy Statements on Virginia Tech Websites)
Email address	Virginia Tech provides basic email service to many of its affiliated groups. Individuals with email service will have an email address comprised of a designated username and password that allows it to authenticate and log in to email.	Standard for University Enterprise Electronic Login Credentials

End-user device	A desktop, laptop, tablet, mobile, or other networked device which a person directly interacts with. See also 'endpoints'.	Standard for Information Technology Logging
Endpoints	University-owned desktops and laptops that connect to the university network or to university resources.	Policy 7100 (Policy for Securing Technology Resources and Services)
Enterprise	The university's large-scale systems and services that support its business and academic operations: the entirety of the Virginia Tech business entity.	Enterprise Identity and Access Management Policy Policy 7100 (Policy for Securing Technology Resources and Services)
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.	Enterprise Identity and Access Management Policy
Entity	Includes, but is not limited to, a person, system, robot, device, or organization.	Enterprise Identity and Access Management Policy
Firewall	A network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.	Policy 7025 (Safeguarding Nonpublic Customer Information)
High risk data	Pertains to data where protection is required by law or regulation. Virginia Tech is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed. See Virginia Tech Risk Classification Standard for more information.	Standard for Information Technology Logging Standard for Personal Digital Identity Levels of Assurance
Identity assertion	A statement, often digitally signed, that declares a subject's identity, typically from one system to another. This declaration is used to verify the subject's identity for access control or personalization purposes.	Standard for Personal Digital Identity Levels of Assurance
Identity proofing	Identity proofing is the process by which an applicant verifies the subject's association with their real-world identity. The subject's eligibility for an institutional personal digital identity is often evaluated during the identity proofing phase. The level of assurance is the degree of confidence that the person who presents a digital credential representing an identity is, in fact, that person.	Standard for Personal Digital Identity Levels of Assurance
IT Project	A project designed to create a unique information technology project, service, or result.	Information Technology Project Management Policy
Moderate risk data	See Virginia Tech Risk Classification Standard.	Standard for Information Technology Logging
Non-repudiation	The assurance that someone cannot deny the validity of something such as a transaction in an IT system.	Enterprise Identity and Access Management Policy
Personal digital identity	An online representation of a real-world identity. A personal digital identity is a person's asserted identity—typically named with associated attributes—along with the digital credentials that represent that identity in an online environment. When used for online approvals and digital signatures, a personal digital identity reflects a level of trust in a person's identity.	Standard for Personal Digital Identity Levels of Assurance
Project management	The application of knowledge, skills, tools, and techniques to mitigate risk, control budget, and manage scope of tasks.	Information Technology Project Management Policy

Project manager	An individual with professional credentials and/or project management training or experience, responsible for achieving the project goals and objectives.	Policy 7210 (Information Technology Project Management)
Pseudo-random passcode	Refers to a passcode that appears random but is generated by a deterministic algorithm.	Standard for University Enterprise Electronic Login Credentials
Risk assessment	A process of identifying, analyzing, and evaluating potential risks and their potential impacts to organizational operations.	Virginia Tech Risk Assessment Standard
Risk management	The process of identifying, assessing, and controlling threats to an organization's assets, data, and reputation.	Virginia Tech IT Vendor Risk Management Standard
Sensitive university information	Includes all university information that could cause physical, financial, or reputational harm to the university or to members of the university community if released inappropriately. Under Policy 7100, data classified as university-internal or as limited-access may be sensitive information.	Standard for Securing Web Technology Resources
Service	A set of computer and network applications that perform work, often operating on data using standard protocols.	Policy for Securing Technology Resources and Services
Social Security number (SSN)	Include those issued to persons by the United States Social Security Administration, and also those issued to individuals by the United States government in lieu of an SSN. SSNs also include nation-based identification numbers issued to individuals by other countries. SSNs also include railroad numbers. SSNs do not include tax IDs issued to corporations.	Standard for High Risk Digital Data Protection
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 cloud services and for 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	Policy for Securing Technology Resources and Services
Terminated	Refers to an account holder being prohibited from using their login credentials in the university-provided authentication system. The username and/or its associated password may be in one of several states in which the username/password combination will not permit such authentication.	Standard for University Enterprise Electronic Login Credentials
The IAM function	The collective service offering of identity and access management (IAM) services and capabilities across the entire university regardless of which unit is offering or operating the service or product.	Enterprise Identity and Access Management Policy
Third party systems	As defined, refer to hosted systems and vendor-provided services running on servers external to Virginia Tech, regardless of whether the system is purchased, leased, or donated. The definition does NOT include partners that receive transmissions of university data under requirements of law or regulation (e.g., the Internal Review Service or the State Council of Higher Education for Virginia).	Standard for Securing Web Technology Resources
University information	Includes information collected by or used by university personnel in the conduct of their university responsibilities. Includes information collected and used for learning, discovery, engagement, support, and administration.	Standard for Securing Web Technology Resources

	University information in digital form may exist in a variety of formats, ranging from highly structured elements in a database to unstructured, narrative information. University information includes information within the control of university personnel in the conduct of their job responsibilities, whether the information resides in university-owned digital systems or elsewhere. Further, university information may be gathered or used at the direction of the university but residing in applications hosted by vendors or other third parties.	
University IT service	Any IT service provided by the university for the university community.	Enterprise Identity and Access Management Policy
Vendor	Third-party company, service provider, or any entity not under control of the university and from whom information technology products and services are purchased or licensed.	Virginia Tech IT Vendor Risk Management Standard
Virginia Tech constituent	Refers to an individual with an existing relationship to the university, such as a student, parent, alumni, and more.	Policy 7040 (Enterprise Identity and Access Management)
Virginia Tech websites	Refers to online pages maintained by or under the direction of the university or its departments and other organizational units.	Policy on Privacy Statements on Virginia Tech Websites
Web applications	Refer to any application that has an interface accessible through a web browser.	Standard for Securing Web Technology Resources
Web servers	Refers to software, hardware, or a combination of both that is intended to serve content to an Internet browser using the Hypertext Transfer Protocol (HTTP) or Hypertext Protocol Transfer Secure (HTTPS), including but not limited to: Apache HTTP Server, Microsoft IIS.	Standard for Securing Web Technology Resources
Web services	Refers to a software programming interface that can be accessed over a network. A web application typically communicates with a web service.	Standard for Securing Web Technology Resources
Web technology or web technology resource	Includes, but is not limited to, any web application or device used in the hosting, storage, or transmission of any Virginia Tech or affiliated information. Web technology resources include web applications, web services, and web servers.	Standard for Securing Web Technology Resources
Web-based service	A combination of web software technologies – web application, web service, web server – that collectively provide a service to the end user.	Standard for Securing Web Technology Resources

NOTE: IT acronyms are defined in the Division of IT acronyms glossary found here.