University System of New Hampshire

ENTERPRISE TECHNOLOGY & SERVICES
GLOSSARY OF TERMS

Access: The ability to make use of any information technology resource or to gain entry to a physical area or location.

Access Control: Process or procedure designed to manage, allow, and restrict use of USNH information and information technology resources and/or physical entry to the physical spaces that house them, for the purposes of preventing unauthorized use.

Account: A mechanism used to establish personalized access to a computer, website, or other information technology resource, generally tied to a set of credentials like a username and password.

Administrative/Operational Control: Process or procedure intended to safeguard information or information technology resources that is primarily implemented and executed by people, rather than by other information technology resources.

Administrator: A person who manages an application, a database, a network, or an information technology resource.

Anti-malware Software: A program or tool that detects many forms of malicious software called malware (e.g., viruses and spyware) and prevents them from infecting computers. It may also cleanse already-infected computers.

Asset: A tangible or intangible resource of value that an organization possesses or employs in order to achieve the organization's mission/business objectives.

Audit Log: A chronological record of information technology resource activities, including records of system accesses and operations performed in a given period that is used for operational purposes.

Audit Record: An individual entry in an audit log related to an audited event.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to [information technology] resources.

Authentication Factor: A piece of information used to verify the identity of a community member, device, or information technology resource.

Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges."

Availability: Protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.

Backup: A copy of information, files, and programs made to facilitate recovery, if necessary.

Baseline: Formally approved configuration for an information technology resource.

Birthright Access: Accounts, privileges, and/or authorizations automatically granted based on a community member's coarse-grain role(s).

Breach: A cybersecurity incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, used, modified, or destroyed by an individual unauthorized to do so.

Bulk Email: Sending large quantities of email with similar content to multiple recipients.

Business Application Owner: An individual outside of Enterprise Technology & Services (ET&S) who is responsible for delivery, administration, support, and management of a non-ET&S managed information technology resource, generally, this resource is a vendor cloud-hosted service.

Business Continuity Plan: The procedures and instructions an organization will follow to continue business operations or rapidly recover operational capabilities in the event of a natural or other disaster; it covers business processes, assets, human resources, business partners and more.

Central Authentication: Verification of an identity for the purposes of allowing access to information technology resources that can be leveraged to access many resources. Often referred to as single-sign on or reduces sign-on.

Centrally Managed Account: A type of authorization created and managed in a central directory, allowing access many information technology resources.

Chief Information Officer (CIO): Executive leader responsible for the management, implementation, and usability of information and information technology resources.

Chief Information Security Officer (CISO): Executive leader responsible for the development, implementation, oversight, and maintenance of an organization's information security or cybersecurity program.

Cloud Service: Information technology capability provided for a fee using a third-party provider's infrastructure (e.g., servers, hardware, networking equipment), information system, or application that is accessed over the internet. Includes Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS).

Coarse-grained Role: A designation used to describe a specific relationship with the University System and/or one of its component institutions.

Compensating Control: A management, operational, physical, or technical safeguard or countermeasure employed in lieu of the recommended or required safeguard or countermeasure that provides equivalent or comparable protection or risk mitigation.

Compromised Account: Access to an information technology resource or resources that is known to be vulnerable to attack or misuse by unauthorized parties because of exposure, breach, or intentional/unintentional revelation.

Computer-based Training: An educational delivery mechanism where content is provided via a computer program rather than by a person.

CONFIDENTIAL Information: Tier 5 of the proposed USNH Information Classification Framework which includes information requiring the highest level of protection and most restrictive security controls and safeguards. It includes electronic Personal Health Information (ePHI) covered by HIPAA and specific information/data used in some grant-funded research efforts.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Management: A collection of activities focused on establishing and maintaining the integrity of information technology resources, through control of the processes for initializing, changing, and monitoring the configurations of those resources.

Credentials: A set of USNH attributes, generally represented by a username and password, that uniquely identifies an entity such as a person or a device.

Critical Business Process: Business processes performed by any administrative, academic, and business unit that involve information that is classified as PROTECTED, RESTRICTED, or CONFIDENTIAL per the proposed USNH Information Classification framework.

Cybersecurity: The ability to protect or defend the use of cyberspace from cyber-attacks. The practice of protecting information and information technology resources from "unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Cybersecurity Event: Anomalous or unexpected activity with the potential to adversely impact the confidentiality, integrity, or availability of institutional information, regardless of its format, or any information technology resource.

Cybersecurity Incident: An anomalous or unexpected event, set of events, condition, or situation that actually or potentially jeopardizes the confidentiality, integrity, or availability of institutional information, regardless of format, an information technology resource or the information that resource

captures, processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Data Steward: A business subject matter expert designated as accountable for a specific type or types of institutional information who determines the classification of that information, approves access to and use of that information and provides institutional authority for mandating information security controls to protect that information.

Deprovision: To remove access to an information technology resource or resources.

Disaster Recovery Plan: A plan that, when activated, designates how critical information technology resources will be restored and outlines the resources required to achieve restoration of those resources after a natural or human-induced disaster.

Domain: The portion of an email address that follows the @ symbol that acts as a common suffix to designate email addresses that are under the control of a specific organization.

Elevated Access: Authorization within an application that allow a community member to perform functions within that application that regular users of that application cannot perform, including making configuration changes, authorizing use by other community members, and modification to information stored within the application.

Encryption: The transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Endpoint/Endpoint Device: An electronic computing device that connects to a network and communicates back and forth with that network. Endpoints include desktop computers, laptop computers, tablets, mobile devices, or any similar network enabled device.

Exception: A temporary exemption from being required to comply with a USNH or institutional Policy or Standard.

FAIR™: FAIR, which stands for Factor Analysis for Information Risk, is a cyber risk framework used for quantitative analysis of information security risk.

FERPA: FERPA, which stands for Family Educational Rights and Privacy Act, is a "federal law that protects the privacy of student educational records."

Fine-grained Role: A designation used provide information technology resource access to community members who are part of a specific group, like all students in Chemistry 101 or all incoming students.

Firewall: A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

GLBA: GLBA, which refers to the Gramm Leach Blilley Act, is a federal law that requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. At USNH, GLBA is applicable to information provided for financial aid purposes.

Guest/Lab Account: A type of account that is used to provide access to specific information technology resources for individuals who are participating in an activity, like a summer camp, at a USNH institution or that is used to administer shared devices in a computer lab.

HIPAA: HIPAA, which refers to the Health Insurance Portability and Accountability Act, is a federal law that mandates specific privacy and security requirements for handling and protecting personal health information (PHI).

Host-based Firewall: A firewall that runs on and protects an individual server or endpoint device instead of an entire network.

Identifier: Unique data used to represent an identity and associated attributes. A USNH username and USNH ID number are examples of identifiers.

Identity: The set of physical and behavioral characteristics by which an individual [entity] is uniquely recognizable.

Identity System of Record: An information system that is used to capture, store, process, transmit, and otherwise manage the information contained in identity records. Examples at USNH include the Banner HR system and each of the component institution's student information systems.

Incident: See Cybersecurity Incident

Information: Facts, data, or instructions in any medium or form.

Information Security: See Cybersecurity.

Information Steward: See Data Steward.

Information Technology Resource: Any hardware, software, firmware, equipment, internet of things (IoT) devices, applications, information systems, etc. used to access, capture, store, process, utilize, integrate, interface with, transmit, or otherwise manage information.

Institutional Information: Information, in any format, created, collected, recorded, captured, stored, processed, transmitted, or otherwise managed by or for the University System and its component institutions, to conduct USNH business.

Institutionally Owned Endpoint: A computer or computing device intended for end-user use purchased by the University System or one of its component institutions.

Integrity: Ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine – and of information technology resources – that resources are functioning as intended, without any unauthorized modifications or alterations.

Internet Connected Device: A physical object that can connect to the internet including, but not limited to, desktop computers, laptops, tablets, smart phones, sensors, household appliances, and wearable technology like a smart watch.

Internet of Things (IoT): The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Keystroke Logging: The process used to record the keys struck on a keyboard without the knowledge of the user.

Least Functionality: Configuring information technology resources such that they provide only those capabilities needed to perform the activities assigned to them and restrict the use of capabilities, such as ports, protocols, or services, that are not essential to those activities.

Least Privilege: Access control strategy requiring that community members only be given access to the information, information technology resources, and specific capabilities within those resources, necessary to perform their job duties.

Local Authentication: Verification of an identity for the purposes of allowing access to a single information technology resource.

Locally Managed Account: A type of authorization created and managed on or for a specific information technology resource.

Log: A record of the events occurring within an organization's information technology resources and networks.

Logical Control: Tools and protocols used by information technology resources to enforce security measures.

MAC Address: A media access control address or MAC address is a unique hardware identification number that uniquely identifies each device on a network.

Mitigate: The effort to reduce loss by making a deficiency less severe and lessening the impact of potential damages.

Multi-factor Authentication (MFA): Access that requires the use of two or more different factors including (i) something you know (e.g., password/PIN); (ii) something you have (e.g., authentication app on a mobile device, token); or (iii) something you are (e.g., biometric).

Network Device: A piece of equipment that enables communication and data transmission between information technology resources across a network or networks. Examples include gateways, routers, wireless access points, networking cables, and switches.

Non-Primary Identity: A unique identifier established for a USNH community member that is separate from their primary identity. Examples of non-primary identities are Pool, Secondary, Service, System Administrator.

NTP: Network Time Protocol (NTP) is a protocol used to synchronize time on all participating information technology resources to within a few milliseconds of Coordinated Universal Time (UTC).

Out of Band: A circumstance where a different method (e.g., process, procedure, tool, etc.) or frequency is used or required instead of the standard method or frequency.

Password: A trusted secret compromised of "a string of characters (letters, numbers and other symbols) that are used" as part of confirming the identity of a person, device, or information technology resource.

Patch: An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

PCI-DSS: The Payment Card Industry – Data Security Standard (PCI-DSS) is a set of "operational and technical requirements" developed by the PCI Security Standards Council that defines required security practices for all "organizations accepting or processing payment transactions" or that develop information technology resources used to process them.

Personally Identifiable Information (PII): Any information about an individual that can be used to distinguish or trace an individual's identify and any other information that is linked or linkable to an individual.

Personally Owned Endpoint: A computer or computing device purchased by a USNH community member using money that was not provided by or associated with USNH or one of its component institutions.

Phishing: Tricking individuals into disclosing sensitive information by claiming to be a trustworthy entity in an electronic communication (e.g., internet web sites, email).

Physical Security: Safeguards used to protect the locations where information and information technology resources are stored or housed against unauthorized access.

Policy: High-level statement of principle intended to provide direction to the USNH community.

Portable Device: An endpoint device that is small enough to be carried from one location to another as part of regular use (e.g., laptop, tablet, mobile phone).

Primary Identity: The identity associated with a user's USNH username. Each individual person has only one primary identity across the entire University System of New Hampshire and its component institutions.

Privileged Access: An escalated level of permissions for an information security resource that is granted to community members that are responsible for the administration of those resources. administrative services such as system maintenance, data management, and user support.

Procedure: An established or official way of doing something.

PROTECTED Information: Tier 3 of the proposed USNH Information Classification Framework which includes information requiring safeguards and specific privacy handling procedures. It includes student information and educational records protected under FERPA.

Provisioning: Establishing the authorizations needed to enable access to a specific information technology resource (e.g., creating an account).

PUBLIC Information: Tier 1 of the proposed USNH Information Classification Framework which includes information specifically approved by data stewards for public distribution.

Quarantine: The process of restricting the ability of an information technology resource like an endpoint or a server to connect to network resources.

Remote Access: The ability for community members to access USNH information technology resources from external locations.

Removable Media: Any device whose primary purpose is to electronically store information that can be easily transported. Examples of removable media include USB flash drives, CD-ROM, DVD-ROM, external or portable hard drives, or any other portable computing device with storage capabilities.

Replay-Resistant Authentication: Configuration that protects against reuse of authentication information that is retransmitted with the intent of producing an unauthorized effect or gaining unauthorized access.

RESTRICTED Information: Tier 4 of the proposed USNH Information Classification Framework which includes information requiring specific security controls. It includes personally identifiable information like SSN and passport number, credit card information, and research information.

Risk: The probable frequency and probable magnitude of future loss.

Risk Acceptance: The formal process of documenting an acknowledgement of the details of a known risk that cannot or will not be mitigated.

Risk Assessment: A systematic process of identifying, analyzing, and documenting potential information security risks.

Risk Management: The program and supporting processes to manage risk to organizational operations (e.g., mission, functions, reputation), organizational assets (e.g., information, information technology resources), individuals, .and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result.

Security Categorization: A risk management designation used across the USNH Information Security Program, to consistently express the criticality of an information technology resource or business process, based on the institutional information involved and the breadth of impact if that resource or process were compromised.

Security Configuration Baseline: An agreed configuration for a specific information technology resource designed to safeguard that resource.

Security Control: A safeguard or countermeasure prescribed for an information technology resource designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Security Log: A chronological record of information technology resource activities, including records of system accesses and operations performed in a given period used for information security purposes.

SENSITIVE Information: Tier 2 of the proposed USNH Information Classification Framework which includes information requiring that can be shared when there are valid purposes to do so, but that cannot be shared publicly.

Segregation of Duties: A security principle that requires the use of one account for non-privileged access and a separate account to be used for privileged access to decrease the likelihood of, and potential for, unauthorized use of the privileged access.

Separation of Duties: A security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or access privilege to negatively impact confidentiality, integrity, and/or availability.

Server: A "Server" is any device which provides service to other network devices regardless of the scale of those services. Specifically excluded from this definition for the purposes of this document:

1. Devices that provide individualized service to other devices, such a blue tooth devices. RF externals, etc.
2. Devices that provide service for the purpose of system management only (i.e. a device that provides service (like RDP or SSH) for the purpose of being managed by other systems)

Despite the exclusion of these types of devices, services provided by them must still be run securely and with up-to-date versions of software.

Service Account: An authorization that enables an information technology resource to communicate with and connect to another information technology resource.

Single Sign On (SSO): A capability that allows the use of one set of authentication credentials, like a username and password, to be used to access several information technology resources.

Spam: Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Standard: A published statement on a topic specifying requirements that must be satisfied or achieved in order to comply with a policy.

Susceptible: Likely or liable to be influenced or harmed by a particular thing.

Technology Service Owner: The individual within Enterprise Technology & Services (ET&S) responsible for operation and maintenance of an information technology resource.

Threat: The potential for a threat source to exploit (intentional) or trigger (accidental) a specific vulnerability.

Username: A unique character string used to designate a specific identity.

USNH Community Member: Any individual who has a relationship with the University System of New Hampshire or one of its component institutions including employees, students, applicants, prior students/alumni, donors, and sponsored users.

USNH ID: A unique nine-digit number used to designate a specific identity. Also called "9 Number".

Vendor: A third-party provider of an information technology resource or capability.

Vulnerability: Weakness in an information technology resource security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Waiver: A permanent (longer than one year) exemption from the requirement to comply with a Policy and/or Standard.