Effective: *08/08/2022*
Last Revised: *03/12/2024*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
IT Security Services
security@nebraska.edu

ITS-00: Information Technology Definitions Standard

Standard Contents

1. Purpose

This document will contain all definitions relevant to ITS Standards, and technology related Executive Memorandums. This standard serves as a single point for information technology terms used within policies, standards, and executive memorandums.

2. Scope

This standard shall apply to all The University of Nebraska System ("University") technology policies, standards, and executive memorandums.

3. Standard Statement

It is the intention of this Standard to establish a library of terms and their definitions related to the University's Executive Memoranda, Policies, Standards, and Procedures throughout the University. The following subsections outline the Definitions Standard.

4. Definitions

Access
The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any electronic system resource.

Affiliated Personnel
Individuals who have sponsored access to University systems such as contractors or consultants as well as third party vendors and/or suppliers.

Authorizing Official
The Vice President of Information Technology is the primary Authorizing Official for all Information Technology standards and programs belonging to the University of Nebraska System. This position maintains the authority to formally assume the responsibility of operating a system at an acceptable level of risk ("Risk Acceptance Authority") and makes all authorization decisions for testing and operations of IT assets. This position may delegate risk determination authority for medium and low risk categories of data classification. This position is responsible for the training and appointment of the Authorizing Official's Delegated Representatives (AODR). The AO and AODR review security packages and exception requests presented by the IT Security Exception Team and security controls assessors in order to make an authorization decision to accept or deny risk (in conjunction with any proposed compensating controls).

Authorizing Official's Delegated Representative (AODR)
This position is designated by the Authorizing Official (AO) in writing and receives delegated duties for risk decision making at assigned classification levels. This position acts on behalf of the AO to make risk decisions for the University's IT assets and programs. Delegations for the AODR include but are not limited to: initial security authorization decisions, risk assessments and acceptance decisions (at delegated level), approval and monitoring of exceptions to vulnerability management, configurations, and standards (also known as Plan of Action and Milestones (POAM)).

Application
A software program funding on a server that is remotely accessible, including mobile applications.

Business Associate
A person or entity who creates, receives, maintains, or transmits PHI or provides services on behalf of a covered entity.

Business Associate Agreement
A contract between a HIPAA covered entity and a business associate that outlines the responsibilities of the business associate, including HIPAA compliance.

Bring Your Own Device "BYOD"
Shall pertain to personally owned laptops, desktops, and mobile devices used to connect to and access information systems. For purposes of this standard, personally owned includes devices for which a user receives a university subsidy or stipend as well as those wholly owned by the employee.

Business Continuity
The capability of the organization to continue the delivery of services at pre-defined acceptable levels following a disruptive event.

Cardholder Data
At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

Cardholder Data Environments (CDE)
The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.

Colleague
Individuals in full- or part-time regular status, unscheduled professionals, consulting employees as well as full- or part-time temporary workers.

Confidential Disclosure Agreements (CDAs)
Legal agreements between two or more parties which outline information the parties wish to share with one another for a specific purpose but wish to restrict from wider use and dissemination. Also referred to as nondisclosure agreements (NDAs) or secrecy agreements.

Controlled Unclassified Information (CUI)
Government created or owned information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies. CUI is not classified information and is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. CUI is not corporate intellectual property unless created for or included in requirements related to a government contract.

Covered Components
An operating unit of the University that conducts activates that make it subject to HIPPA.

Covered entity
A health plan, health care clearinghouse, or healthcare provider who transmits any health information in electronic form in connection with a transaction covered under the HIPAA regulations.

CVE
CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. Security advisories issued by vendors and researchers almost always mention at least one CVE ID. CVEs help IT professionals coordinate their efforts to prioritize and address these vulnerabilities to make computer systems more secure.

Cybersecurity Maturity Model Certification (CMMC)
A Department of Defense (DoD) Cybersecurity framework that is designed to protect sensitive unclassified information held by DoD contractors and subcontractors in the Defense Industrial Base (DIB).

Data Use/Data Transfer Agreements (DUAs/DTAs)
Contractual documents for the use of a portion of data or transfer of a portion or complete set of data where the data is nonpublic or is subject to some restrictions. Universities must ensure that DUA/DTA terms protect confidentiality and security when necessary but permit appropriate publication and sharing of research results in accordance with federal, state, and University regulations.

Designated Record Set
A group of records maintained by or for the covered component that consists of medical and billing records about an individual that are use, in whole or in part, by or for the covered component to make decisions about the individual.

Device
A device is an object with the ability to engage in computational operations, including the accessing or storing of electronic data.

Directory Information
Board of Regents' Policies define data elements designated as student public directory information in Regents' Policy 5.10; and faculty and staff public directory information in Regents' Policy 6.7.

Disclose/Disclosure
Releasing, transferring, giving access to or divulging PHI outside of the entity holding the information.

Electronic Communications
Shall mean and include the use of information systems in the transmitting, receiving, storing, or posting of information or material by way of email, message boards, forums, chat, web sites, institutional social media accounts, or other such electronic tools over the Internet or other networks.

Endpoints
Shall refer to desktops, laptops, tablets, mobile devices, printers, or any other device, excluding servers, capable of connecting to the University network or accessing University data.

Enterprise-Wide Systems and Networks
Networks, and Systems including but not limited to software, storage, licensed platforms, cloud-based services, and other similar technologies that are administered, owned, or operated by the Office of the President or for which the University of Nebraska System is responsible, and made available to the University community.

Examples Include:

- Networks
- Email
- File Storage
- Virtual Servers & Applications
- IT Security Systems
- Identity/Authentication Systems
- Endpoint Management
- Remote Access
- Learning Management Systems
- Academic Video Management Systems

FERPA
Family and Educational Rights and Privacy Act, a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FIPS PUB 199
Federal Information Processing Standards Publication Standards for Security Categorization of Federal Information and Information Systems

HIPAA
Information or data protected by the Health Insurance Portability and Accountability Act of 1996. This legislation provides data privacy and security for safeguarding medical information.

Hybrid Entity
A single legal entity that performs covered, and no-covered, functions under HIPAA.

Hybrid Entity Designation
A written statement the University utilized to memorialize the University units that meet the definition of a covered component and supporting components that support the covered components.

Inactive User/Account
An inactive user/account is an account that has not been accessed during a specified duration as defined in ITS-02 or has never been logged into. Inactive accounts will be disabled but could be reactivated by a user who has an active role within the University.

Information Assets
Refers to all non-hardware / software data assets such as institutional and research data.

Information Systems
Endpoints, Networks, Systems, and other similar devices that are administered, owned, or operated by the University or for which the University is responsible.

Information Technology Systems
See Information Systems.

Institutional Data
Information created, collected, maintained, transmitted, or recorded by or for the University to conduct University business. It includes data used for planning, managing, operating, controlling, or auditing University functions, operations, and mission. Institutional data includes, but is not limited to, information in paper, electronic, audio, and visual formats.

Institutional Data Classification Matrix
Defines the appropriate data classification levels for data elements and identifies which classifications of data are permitted for specific data user's activities.

Institutional Data Stewards
Subject matter experts and operational managers in a functional area with day-to-day responsibilities for managing business processes and establishing the business rules for that area and its related institutional data.

Institutional Data Classification, Use, and Policy Committee
University-wide committee established in ID-01: Institutional Data Use Policy which is charged with establishing data definitions, risk classifications, and data standards for institutional data.

ITAR
Protected information or data regarding International Traffic in Arms Regulations and export controls, typically found in university research environments.

Internet of Thing (IoT)
Internet of Things describes physical object (or groups of such objects) that are embedded with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the internet or other communications networks.

ITS
University of Nebraska (NU) or University of Nebraska Medical Center (UNMC) Information Technology Services

Material Transfer Agreements (MTAs)
Contractual documents used for the acquisition of various biological and research materials and occasionally data. Universities must ensure that MTAs protect confidentiality, security, and intellectual property when necessary, but permit appropriate publication and sharing of research results in accordance with federal, state, and University regulations.

Metadata
Information describing the characteristics of data, including descriptions of data format, syntax, and semantics (structural metadata) and data describing contents such as security labels (descriptive metadata).

Minimum Necessary
The amount of PHI that is required to accomplish the particular purpose(s) for which the PHI is being used, disclosed, or requested.

Minimum Security Standards
A set of standards that protect physical and electronic data and IT systems from intentional or accidental destruction, modification, access, or disclosure. Minimum security standards are applied using a range of techniques, including administrative controls, physical security, logical controls, organizational standards, and other safeguarding techniques that limit access to unauthorized or malicious users or processes.

Multi-Factor Authentication
A security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction.

Networks
Shall mean and include wired and wireless video, voice, and data infrastructure, including security devices.

NIST
The National Institute of Standards and Technology (NIST) develops cybersecurity frameworks, standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public.

NTP
Network Time Protocol is an Internet protocol used to synchronize the clocks of computers to a specific time reference.

PCI DSS
Payment Card Information Data Security Standards. These standards address the information related to payment cards and the security of the information for university departments engaging in e-commerce.

Personnel
Individuals in full- or part-time regular status, unscheduled professionals, consulting employees as well as full- or part-time temporary workers.

Personal Data
Information created, collected, maintained, transmitted, or recorded by University-owned devices, media, or systems in accordance with Executive Memorandum No. 16 that is personal in nature and not related to University business.

Personally Owned Device
See Bring Your Own Device “BYOD”

Plan of Action and Milestones (POAM)
A document or form that identifies a security issue, problem, or change (example: vulnerability or configuration) which needs to be corrected accompanied by a plan to accomplish. The document or form details the work and resources required to accomplish the elements of the plan and must include the scheduled milestones for implementation.

Playbook
A playbook will contain the defined process a team will follow to meet the requirements laid out in the respective Procedures. A playbook will not be published outside the required team.

Primary Account Number (PAN)
Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Privileged Account
An account that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform as defined by NIST 800-171. Privileged accounts can be a human or machine credentials with the ability to:

- Modify the configuration of an Information System
- Install Information System hardware or software
- Modify user privileges of an Information System
- Integrate/connect Information Systems
- Access Confidential (High Risk) Data in an Information System

Procedure
Procedure documents are the high-level processes that will be needed to comply with a Standard, Policy, or Executive Memorandum. Procedures will be published to University employees.

Protected Health Information (PHI)
Individually identifiable information (oral, written, or electronic) that (1) is created or received by a covered entity or covered component and (2) relates to a patient’s past, present, or future physical or mental health; the receipt of health

care; or payment for that care. This includes the PHI of deceased individuals unless the individual has been deceased for more than 50 years.

Personal Cloud Services and Personal Cloud Storage
Personal Cloud Services and Personal Cloud Storage refers to personally subscribed public cloud services and personal cloud storage offered by third parties not affiliated with the University or a party to a University negotiated contract, including free service offerings, regardless of the source of funds used to purchase or secure the services or storage that are intended to interact with or store University records and/or data. Such Personal Cloud usage is not authorized by the University because it places the University at risk due to limited technical safeguards and security controls, no contractual oversight, protections or limitations, unspecified accessibility requirements, and no evaluation or enforcement over data integrity.

Public Cloud ~~Storage~~
Cloud services offered by providers to the general public that may or may not be contracted with or by the University. Examples include Amazon Web Services, Microsoft Azure, Google Compute Platform, Box, DropBox, Google Workspace, iCloud, CrashPlan, BackBlaze, and many more. These services are not approved to store University data unless they are contracted for and managed by the University.

Public Domain
A work of authorship is in the public domain if it is no longer under copyright or if it failed to meet the requirements for copyright protection. Works in the public domain may be used freely without permission of the copyright owner. Information which is generally accessible or available to the public. For export control requirements, the definition of public domain and publicly available information should be referenced to International Traffic in Arms Regulations (ITAR) or Export Administration Regulation (EAR). The ITAR states that information in the public domain that is published and that is generally accessibly or available to the public is excluded from control as ITAR technical data.1 The EAR excludes from its control publicly available technology and software, except software classified under ECCN 5D002 on the Commerce Control List (certain encryption software), that are already published or will be published. Campus research offices must be contacted when dealing with data subject to ITAR or EAR.

Records
Information of any kind and in any form including writings, drawings, graphs, charts, images, prints, photographs, microfilms, audio and video recordings, data and data compilations, and electronic media, including email.

Records and Data
Are defined in Executive Memorandum 41, Executive Memorandum 42, ID-01 Institutional Data Policy, and Regents Policy 6.7 and include institutional and research data.

Recovery Point Objective (RPO)
Describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan’s maximum allowable threshold or “tolerance.”

Recovery Time Objective (RTO)
The duration of time within a service must be restored after a disaster in order to avoid unacceptable consequences associated with a break in service availability. This time is calculated for when all dependent services are available.

Removable Media
Shall mean devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. Examples can be found in the ITS Removable Media/Media Protection Standard.

Research Data
All information in any physical or electronic form collected, obtained, and/or generated in the course of a research project conducted at the University, under the auspices of the University, or with University resources. This includes original and derivatives of research data, regardless of form or funding, physically housed at the University of Nebraska or stored remotely, including recordings of such data. Examples of research data include, but are not limited to:

- Data, analytical programs, procedures, and records necessary for the reconstruction and evaluation of the results of research
- Laboratory notebooks

- Data collected using instrumentation or systems and stored in an electronic format
- Source documentation and reporting forms for human participant research studies.

Research data does not include data generated or acquired by students in their academic work, unless the research data are generated or acquired within the scope of their employment at the University, generated or acquired through use of substantial University resources, or subject to other agreements that supersede this right (e.g., research data ownership agreements signed by the student and PI).

Research Data Steward
Any University of Nebraska campus or system personnel with day-to-day responsibilities for managing research data, processes, and security

Research Health Information (RHI)
Information collected about research participants that pertains to their health or healthcare which either (1) is created or received in connection with research that does not involve a covered component or (2) has been reclassified and is no longer subject to HIPAA requirements due to a disclosure from a covered component or external covered entity pursuant to a valid HIPAA research disclosure, such as a valid authorization or waiver or alteration of authorization.

Research Oversight Bodies
A committee, council, office, or other unit that has responsibility for research activities.

Research Personnel
Principal investigators, program/project directors, investigators, co-directors, research associates, visiting scientists, postdoctoral fellows, technicians, graduate students, undergraduate students, or any other person involved in the design, conduct, or reporting of research.

Responsible Party
Individual or group of people that are responsible for a decision or action.

SIEM
Security Information and Event Monitoring

Sensitive Authentication Data
Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Server
A system entity that provides a network accessible service in response to a request from a client device.

Service Account
A service account is a non-shared local or domain account, not associated with a human, that is associated with a specific information system for use by an automated process, executable service, or application to interact with the operating system or access databases, run batch jobs or scripts, or provide access to other applications, such as application programming interface (API) calls.

Service Offerings
Consists of one or more service commitments that uniquely define the level of service in terms of availability, scope, pricing, and packaging options. Customers can choose to receive different levels of performance and features for a given service through service offerings (typically made available as distinct items in the service catalog).

Service Owner (SO)
The service owner is accountable for the delivery of an IT service and the service offerings within. The purpose of this leadership role is to ensure that the service receives strategic attention and appropriate resources to support the mission and needs of the institution. The SO is responsible for the service as a whole through its entire life cycle and is accountable to the person in charge of overall IT service delivery. The SO’s accountability for a service is independent of where the underpinning technology components, processes, or professional capabilities needed to deliver the service and its offerings reside.

Service Offering Manager (SOM)
The service offering manager is responsible for the delivery of an IT service offering. The purpose of this role is to ensure comprehensive, efficient, and transparent management of and communication about the IT service offering in accordance

with the service strategy. This role is accountable to the SO for the design, implementation, and ongoing maintenance and support of the offering. As with the service owner, the SOM's responsibility for a specific service offering is independent of where the underpinning technology components, processes, or professional capabilities reside.

Shared Account
A shared account provides multiple users anonymous access to an Information System by sharing the same login identity and credentials to accomplish a single shared function in support of a specific process, endpoint, or system.

Substantial University Resources
Resources provided by the University that go above and beyond what is customarily provided to University employees or students. These resources may vary by department/unit and context, but include resources provided from extramural sources, internal grants, startup funds, and targeted campus/University investments in a program or unit.

System
Shall mean and include software, servers, storage, licensed platforms, and cloud-based services.

System Security Plan (SSP)
A system security plan is a document that outlines how an organization implements its security requirements, of which outlines the roles and responsibilities of security personnel, as well as the varying security standards and guidelines to be followed.

Tailgating
Tailgating occurs when one or more individuals follow an authorized individual into a secure location without verifying the authorization of each individual, resulting in a physical security breach. (also referred to as piggybacking)

University devices
Shall mean and include any device purchased with University funds (including but not limited to state, foundation, grant, contract, etc.) capable of connecting to University networks directly or through a gateway. Examples include, but are not limited to, desktops, laptops, tablets, printers, IoT devices, servers, appliances, and sensors.

Use
The sharing, employment, application, utilization, examination, or analysis of PHI within the entity holding the information.

Verification
An evaluation of an organization's information technology infrastructure, policies, and operations. Information technology reviews conducted to determine whether IT controls protect institutional assets, ensure data integrity, and are aligned with the goals and mission of the University.

Waiver or alteration of HIPAA authorization
The documentation that the covered component obtains from a researcher establishing that an institutional review board or HIPAA privacy bard has waived or altered HIPAA's regulatory requirement that an individual must authorize a covered entity to use or disclose the individual's PHI for research purposes.

Workforce
Employees, volunteers, trainees, and other persons who conduct or perform work for the covered component or business associate, whether or not they are paid by the covered entity.

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Roles and Responsibilities

For the purposes of all IT Polices, Executive Memoranda, Standard, and Procedures, the following roles and responsibilities apply:

Stakeholder	Responsibilities
Board of Regents	• Approve, act in accordance with and formally support this Standard.
Chief Information Officer	• Approve and formally support this Standard.
Chief Information Security Officer	• Review, approve, and track any exceptions to the requirements of this Standard. • Proactively enforce compliance of all stakeholders of this Standard. • Build and maintain regulation compliant programs in their respective units. • Determine whether an incident is a reportable breach under their respective regulation
IT Security Services	• Develop and maintain this Standard. • Identify and analyze risks associated with the exceptions. • Assessment of compliance status and enforcement of policies. • Security requirement development as aligned to the policies.
University Researchers	• Maintain PHI and RHI according to University data classification requirements. • Follow University standards and procedures surrounding data security incident response management, including promptly and appropriately reporting potential breaches of any information.
Management & Supervisors	• Support all employees in the understanding of the requirements of this Standard. • Immediately assess and report any non-compliance instance with this Standard.
Legal / Procurement / Privacy Officer	• Ensure that the responsibilities and security obligations are documented in the business associate agreement executed between the University and the contractor/sub-contractor. • All business associate agreements must be reviewed by the Office of the Vice President and General Counsel and an executed copy provided to the Privacy Officer.
Human Resources	• Present each new employee or contractor with the relevant IT and Security standard, upon the first day of commencing work with The University. • Formally support all employees in the understanding of the requirements of this Standard.
All Colleagues	• Report all non-compliance instances with this Standard (observed or suspected) to their Supervisor or CISO as soon as possible.

7. Compliance

Intentionally left blank

8. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

9. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	03/12/2024
Approved by:	Bret Blackman	IT CIO	03/12/2024

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published
1.1	03/20/2023	Added definition for personal cloud and modified definition for public cloud.
1.2	03/12/2024	Definitions updated for Privileged Account, Service Account, and Shared Account