NITC 01-101 (DRAFT)

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 01-101 (Draft)

Title	Definitions
Category	General Provisions
Applicability	These definitions apply to all NITC Standards and Guidelines

1. General Provision

For purposes of the NITC Standards and Guidelines documents, the definitions found in this document apply. Some NITC Standards and Guidelines documents may contain additional definitions which will only apply to the document in which they appear.

2. Definitions

Agency: Any agency, department, office, commission, board, panel, or division of the state.

Agencies, Boards, and Commissions: Agencies, Boards, and Commission has the same meaning as "Agency."

Authentication: The process to establish and prove the validity of a claimed identity.

Authenticity: This is the exchange of security information to verify the claimed identity of a communications partner.

Authorization: The granting of rights, which includes the granting of access based on an authenticated identity.

Availability: This is the ‘property’ of being operational, accessible, functional and usable upon demand by an authorized entity, e.g. a system or user.

Biometrics: Refers to the use of electro-mechanical devices that measure some physical, electrical or audio characteristic of an individual and make use of that specific measurement to verify identity.

Business Risk: This is the combination of sensitivity, threat and vulnerability.

Change Management Process: A business process that ensures that no changes occur on a computing resource without having gone through a methodology to ensure that changes will perform as expected, with no unexpected repercussions.

Chief Information Officer (CIO): Chief Information Officer means the Nebraska state government officer position created in Neb. Rev. Stat. § 86-519.

Classification: The designation given to information or a document from a defined category on the basis of its sensitivity.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls: Countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

Critical: A condition, vulnerability or threat that could cause danger to data, a system, network, or a component thereof.

Data: Any information created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media, including all records as defined by the Records Management Act. Data may include, but is not limited to personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Data Security: The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information.

Data Owner: An individual or a group of individuals with responsibility for making classification and control decisions regarding use of information.

Denial of Service: An attack that takes up so much of the company’s business resource that it results in degradation of performance or loss of access to the company’s business services or resources.

Disaster: A condition in which information is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of the State of Nebraska’s business objectives.

DMZ: Demilitarized zone; a semi-secured buffer or region between two networks such as between the public Internet and the trusted private State network.

Encryption: The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

Enterprise: Enterprise means the entirety of all departments, offices, boards, bureaus, commissions, or institutions in the state for which money is to be appropriated for communications or data processing services, equipment, or facilities, including all executive, legislative, and judicial departments, the Nebraska state colleges, the University of Nebraska, and all other state institutions and entities. Neb. Rev. Stat. § 86-505.

Enterprise Project: Enterprise project means an endeavor undertaken over a fixed period of time using information technology, which would have a significant effect on a core business function and affects multiple government programs, agencies, or institutions. Enterprise project includes all aspects of planning, design, implementation, project management, and training relating to the endeavor. Neb. Rev. Stat. § 86-506.

Executive Management: The person or persons charged with the highest level of responsibility for an Agency (e.g. Agency Director, CEO, Executive Board, etc.).

External Network: The expanded use and logical connection of various local and wide area networks beyond their traditional Internet configuration that uses the standard Internet protocol, TCP/IP, to communicate and conduct E-commerce functions.

Family Educational Rights and Privacy Act (FERPA): Federal law regarding the privacy of educational information. For additional information visit: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Firewall: A security mechanism that creates a barrier between an internal network and an external network.

Geographic Information System (GIS): A system of computer hardware, software, and procedures designed to support the compiling, storing, retrieving, analyzing, and display of spatially referenced data for addressing planning and management problems. In addition to these technical components, a complete GIS must also include a focus on people, organizations, and standards.

Geospatial Data: A term used to describe a class of data that has a geographic or spatial nature. The data will usually include locational information (latitude/longitude or other mapping coordinates) for at least some of the features within the database/dataset.

Gramm-Leach-Bliley Act (GLB): Federal regulation requiring privacy standards and controls on personal information for financial institutions. For additional information visit: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Guideline: An NITC document that aims to streamline a particular process. Compliance is voluntary.

Health Insurance Portability Accountability Act (HIPAA): A Congressional act that addresses the security and privacy of health data. For additional information visit: http://www.hhs.gov/ocr/hipaa/

Host: A system or computer that contains business and/or operational software and/or data.

Incident: Any adverse event that threatens the confidentiality, integrity or accessibility of information resources.

Incident Response: The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.

Information: Information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

Information Assets: (1) All categories of automated information, including but not limited to: records, files, and databases, and (2) information technology facilities, equipment (including microcomputer systems), and software owned or leased by the State.

Information Security: The concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or temporary or permanent loss (See Availability).

Information Technology: Information technology means computing and telecommunications systems and their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store, and disseminate information electronically. Neb. Rev. Stat. § 86-507.

Information Technology Infrastructure: Information technology infrastructure means the basic facilities, services, and installations needed for the functioning of information technology. Neb. Rev. Stat. § 86-509

Information Technology Resources: Hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities including but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

Integrity: The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Internet: A system of linked computer networks, international in scope, which facilitates data transmission and exchange, which all use the standard Internet protocol, TCP/IP, to communicate and share data with each other.

Internal Network: An internal (i.e., non-public) network that uses the same technology and protocols as the Internet.

Internet Protocol (IP): A packet-based protocol for delivering data across networks.

Local Area Network (LAN): A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. For State agencies, LANs are defined as restricted to rooms or buildings. An interconnection of LANs over a citywide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas is commonly called a wide area network (WAN).

Malicious Code: Malicious Code refers to code that is written intentionally to carry out annoying, harmful actions or use up the resources of a target computer. They sometimes masquerade as useful software or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses and computer viruses.

Metropolitan Area Network (MAN): A data communications network that (a) covers an area larger than a local area network (LAN) and smaller than a wide area network (WAN), (b) interconnects two or more LANs, and (c) usually covers an entire metropolitan area, such as a large city and its suburbs.

Nebraska Information Technology Commission (NITC): The information technology governing body created in Neb. Rev. Stat. § 86-515. See http://nitc.ne.gov/

Network Interface Card (NIC): A piece of computer hardware designed to allow computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

Network Nebraska: The network created pursuant to Neb. Rev. Stat. § 86-5,100.

Office of the Chief Information Officer (OCIO): A division of Nebraska state government responsible for both information technology policy and operations. Statutorily, the duties previously assigned to the Division of Communications and Information Management Services are part of the OCIO.

Personal Information: Personal information means any information concerning a person, which, because of name, number, personal mark or other identifier, can be used to identify such natural person.

Physical Security: The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

Policy: An NITC document that establishes a set of consistent rules and the means of achieving them that support the business objectives for the State of Nebraska.

Principle of Least Privilege: A framework that requires users be given no more access privileges (read, write, delete, update, etc.) to systems than necessary to perform their normal job functions, and those privileges be granted no longer than the time required to perform authorized tasks.

Privacy: The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Private Information: Private Information means personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:
- social security number; or
- driver’s license number or non-driver identification card number; or
- account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual’s financial account

"Private information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Privileged Account: The User ID or account of an individual whose job responsibilities require special system authorization, such as a network administrator, security administrator, etc. Special authorizations are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator, etc.

Procedures: Specific operational steps that individuals must take to achieve goals stated in the NITC Standards and Guidelines documents.

Records Officer: The agency representative from the management or professional level, as appointed by each agency head, who is responsible for the overall coordination of records management activities within the agency.

Records Management Act: The Nebraska records management statutes codified at Neb. Rev. Stat. § 84-1201 through § 84-1228.

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk Assessment: The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

Risk Management: The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

Router: A device or setup that finds the best route between any two networks using IP addressing, even if there are several networks to traverse. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create wide area networks.

Security Management: The responsibility and actions required to manage the security environment including the security policies and mechanisms.

Security Policy: The set of criteria for the provision of security services based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

Separation of Duties: A concept that no individual should have control over two or more phases of an operation or areas of conflicting responsibility.

Sensitive Information: Disclosure or modification of this data would be in violation of law, or could harm an individual, business, or the reputation of the agency.

Sensitivity: The measurable, harmful impact resulting from disclosure, modification, or destruction of information.

Staff: Any State of Nebraska full time and temporary employees, third party contractors and consultants who operate as employees, volunteers and other agency workers.

Standard: Sets of rules for implementing policy. Standards make specific mention of technologies, methodologies, implementation procedures and other detailed factors. Adherence is required. Certain exceptions and conditions may appear in the published standard, all other deviations require prior approval.

Standards and Guidelines: Refers to the collection of documents, regardless of title, adopted by the NITC pursuant to Neb. Rev. Stat. § 86-516(6) and posted on the NITC website at http://nitc.ne.gov/standards/.

State: The State of Nebraska.

State Data Communications Network (SDCN): State Data Communications Network means any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to State computers.

State Information Security Officer: The Information Security Officer appointed by the Chief Information Officer to lead the NITC Security Architecture Workgroup. Responsibilities include creating and maintaining polices for the State of Nebraska, conducting vulnerability / penetration tests at an enterprise level, and to assist Agency Information Security Officer’s.

State Network: The State of Nebraska’s internal, private network, e.g. the State’s 10.x.x.x address space.

Switch: A mechanical or solid state device that opens and closes circuits, changes operating parameters or selects paths for circuits on a space or time division basis.

System(s): An interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, information, data, applications or communications infrastructure.

System Development Life Cycle: A software development process that includes defining the system requirements, the design specifications, the software development, installation and training, maintenance, and disposal.

TCP/IP: An abbreviation for Transmission Control Protocol / Internet Protocol. A protocol for communications between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.

Technical Panel: The panel created in Neb. Rev. Stat. § 86-521.

Third Party: Any non-agency contractor, vendor, consultant, or external entity, etc.

Threat: A force, organization or person, which seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in risk assessment.

Token: A device that operates much like a smart card but is in a physical shape that makes its use easier to manage.

Trojan Horse: Illegal code hidden in a legitimate program that when executed performs some unauthorized activity or function.

Unauthorized Access Or Privileges: Insider or outsider who gains access to network or computer resources without permission.

User: Any agency (ies), federal government entity (ies), political subdivision(s), their employees or third party contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a System for a legitimate government purpose.

Virtual Local Area Network (VLAN): A VLAN is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment. Network reconfiguration can be done through software instead of physically relocating devices.

Virtual Private Network (VPN): A communications network tunneled through another network, and dedicated for a specific network. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features. A VPN may have best-effort performance, or may have a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point. The distinguishing characteristic of VPNs are not security or performance, but that they overlay other network(s) to provide a certain functionality that is meaningful to a user community.

Virus: A program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may damage data in the host’s memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).

Vulnerability: A weakness of a system or facility holding information that can be exploited to gain access or violate system integrity. Vulnerability can be assessed in terms of the means by which the attack would be successful.

Vulnerability Scanning: The portion of security testing in which evaluators attempt to identify physical, network, system or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.

Web Application: An application that is accessed with a web browser over a network such as the Internet or an intranet.

Web Page: A document stored on a server, consisting of an HTML file and any related files for scripts and graphics, viewable through a web browser on the World Wide Web. Files linked from a Web Page such as Word (.doc), Portable Document Format (.pdf), and Excel (.xls) files are not Web Pages, as they can be viewed without access to a web browser.

Web Site or Website: A set of interconnected Web Pages, usually including a homepage, generally located on the same server, and prepared and maintained as a collection of information by a person, group, or organization.

Wide Area Network (WAN): A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and is usually spread over a larger geographic area than that of a LAN.

Wireless Local Area Network (WLAN): A wireless local area network (or wireless LAN, or WLAN) is the linking of two or more computers without using wires. WLAN utilizes technology based on radio waves to enable communication between devices in a limited area. This gives users the mobility to move around within a broad coverage area and still be connected to the network.

Worm: A program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.

VERSION DATE: Draft - December 21, 2007
HISTORY:
PDF FORMAT: (to be added)
