1-101. General definitions.

Subject to additional definitions contained in subsequent articles which are applicable to specific articles or parts thereof, and unless the context otherwise requires, in the NITC Technical Standards and Guidelines:

(1) "Agencies, boards, and commissions" has the same meaning as agency.

(2) "Agency" means any agency, department, office, commission, board, panel, or division of state government. [Source: based on Neb. Rev. Stat. § 81-2402(1)]

(3) "Agency information security officer" means the individual employed by an agency with the responsibility and authority for the implementation, monitoring, and enforcement of information security policies for the agency.

(4) "AISO" is an abbreviation for agency information security officer.

(5) "Authentication" means the process to establish and prove the validity of a claimed identity.

(6) "Authenticity" means the exchange of security information to verify the claimed identity of a communications partner.

(7) "Authorization" means the granting of rights, which includes the granting of access based on an authenticated identity.

(8) "Availability" means the assurance that information and services are delivered when needed.

(9) "Biometrics" means 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.

(10) "Breach" means any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

(11) "Business risk" means the combination of sensitivity, threat and vulnerability.

(12) "Chain of custody" means the protection of evidence by each responsible party to ensure against loss, breakage, alteration, or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence.

(13) "Change management process" means 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.

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

(15) "CIO" is an abbreviation for Chief Information Officer.

(16) "CJI" is an abbreviation for Criminal Justice Information, the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII. [Source: *Criminal Justice Information Services (CJIS) Security Policy*, Version 5.6, 06/05/2017]

(17) "CJIS" is an abbreviation for Criminal Justice Information Services Division, the FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies. [Source: *Criminal Justice Information Services (CJIS) Security Policy*, Version 5.6, 06/05/2017] See also "CJI."

(18) "Classification" means the designation given to information or a document from a defined category on the basis of its sensitivity.

(19) "Commission" means the Nebraska Information Technology Commission.

(20) "Communications" means any transmission, emission, or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, radio, optical, or other electromagnetic systems. [Source: Neb. Rev. Stat. § 81-1120.02(4)]

(21) "Communications system" means the total communications facilities and equipment owned, leased, or used by all departments, agencies, and subdivisions of state government. [Source: Neb. Rev. Stat. § 81-1120.02(3)]

(22) "Compromise" means the unauthorized disclosure, modification, substitution, or use of sensitive information, or the successful action to invade system by evading its security. For example, a computer had been compromised when a Trojan horse has been installed.

(23) "CONFIDENTIAL" (written in all capital letters) means the data classification category defined in section 8-902.

(24) “Confidentiality” means the assurance that information is disclosed only to those systems or persons that are intended to received that information.

(25) “Continuity of operations plan” means a plan that provides for the continuation of government services in the event of a disaster.

(26) “Controls” means countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

(27) “COOP” is an abbreviation for continuity of operations plan.

(28) “Critical” means a condition, vulnerability or threat that could cause danger to data, a system, network, or a component thereof.

(29) “Cyber security incident” means any electronic, physical, natural, or social activity that threatens the confidentiality, integrity, or availability of state information systems, or any action that is in violation of the Information Security Policy.
For example:
- Any potential violation of federal or state law, or NITC policies involving state information systems.
- A breach, attempted breach, or other unauthorized access to any state information system originating from either inside the state network or via an outside entity.
- Internet worms, Trojans, viruses, malicious use of system resources, or similar destructive files or services.
- Any action or attempt to utilize, alter, or degrade an information system owned or operated by the state in a manner inconsistent with state policies.
- False identity to gain information or passwords.

(30) “Data” means 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.

(31) “Data security” means the protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information.

(32) “Data owner” means an individual or a group of individuals with responsibility for making classification and control decisions regarding use of information.

(33) “Denial of service” means 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.

(34) “Disaster” means 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's business objectives.

(35) “DMZ” is an abbreviation for demilitarized zone, and means a semi-secured buffer or region between two networks such as between the public Internet and the trusted private state network.

(36) “Encryption” means the cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

(37) “Enterprise” means one or more departments, offices, boards, bureaus, commissions, or institutions of 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. [Source: Neb. Rev. Stat. § 86-505]

(38) “Enterprise project” means an endeavor undertaken by an enterprise over a fixed period of time using information technology, which would have a significant effect on a core business function or which affects multiple government programs, agencies, or institutions. Enterprise project includes all aspects of planning, design, implementation, project management, and training relating to the endeavor. [Source: Neb. Rev. Stat. § 86-506] Pursuant to Neb. Rev. Stat. § 86-526, the NITC is responsible for determining which proposed information technology projects are enterprise projects.

(39) “Executive management” means the person or persons charged with the highest level of responsibility for an agency.

(40) “External network” means 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.

(41) “External service provider” means a non-agency consultant, contractor, or vendor.

(42) “FedRAMP” is an abbreviation for the Federal Risk and Authorization Management Program, a government wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. [http://www.fedramp.gov/]

(43) “FERPA” is an abbreviation for the Family Educational Rights and Privacy Act, a federal act addressing the privacy of educational information.

(44) “Firewall” means a security mechanism that creates a barrier between an internal network and an external network.

(45) "FTI" is an abbreviation for Federal Tax Information, and means return or return information received directly from the IRS or obtained through an authorized secondary source, such as the Social Security Administration, Federal Office of Child Support Enforcement, Bureau of the Fiscal Service, Centers for Medicare and Medicaid Services, or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) agreement.

(46) "Geographic information system" means 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 geographic information system must also include a focus on people, organizations, and standards.

(47) "Geospatial data" means 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.

(48) "GIS" is an abbreviation for geographic information system.

(49) "GLBA" is an abbreviation for the Gramm-Leach-Bliley Act, a federal act requiring privacy standards and controls on personal information for financial institutions.

(50) "Guideline" means an NITC document that aims to streamline a particular process. Compliance is voluntary.

(51) "Health Insurance Portability and Accountability Act" is a federal act that addresses the security and privacy of health data.

(52) "HIPAA" is an abbreviation for the federal Health Insurance Portability and Accountability Act.

(53) "Host" means a system or computer that contains business and/or operational software and/or data.

(54) "Incident" means any adverse event that threatens the confidentiality, integrity or accessibility of information resources.

(55) "Incident response" means an organized approach to addressing and managing the aftermath of a security incident.

(56) "Incident response team" means a group of professionals within an agency trained and chartered to respond to identified information technology incidents.

(57) "Information" means the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

(58) “Information assets” means (a) All categories of automated information, including but not limited to: records, files, and databases, and (b) information technology facilities, equipment (including microcomputer systems), and software owned or leased by the state.

(59) “Information security” means the concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or temporary or permanent loss.

(60) “Information system” means a system or application that consists of computer hardware, software, networking equipment, and any data. Such systems include but are not limited to desktop computers, servers, printers, telephones, network infrastructure, email, and web based services.

(61) “Information technology” means computing and telecommunications systems and their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store, and disseminate information electronically. [Source: Neb. Rev. Stat. § 86-507]

(62) “Information technology infrastructure” means the basic facilities, services, and installations needed for the functioning of information technology. [Source: Neb. Rev. Stat. § 86-509]

(63) “Information technology resources” means the 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.

(64) “Integrity” means the assurance that information is not changed by accident or through a malicious or otherwise criminal act.

(65) “Internet” means 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.

(66) “Internal network” means an internal, non-public network that uses the same technology and protocols as the Internet.

(67) “Internet Protocol” means a packet-based protocol for delivering data across networks.

(68) “IP” is an abbreviation for Internet Protocol.

(69) “IT” is an abbreviation for information technology.

(70) "IT devices" means desktop computers, servers, laptop computers, personal digital assistants, MP3 players, tablet computers, mainframe computers, printers, routers, switches, hubs, portable storage devices, digital cameras, cell phones, smart phone, multi-functional devices, and any other electronic device that creates, stores, processes, or exchanges state information.

(71) "LAN" is an abbreviation for local area network.

(72) "Local area network" means 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, local area networks are defined as restricted to rooms or buildings.

(73) "Malicious code" means 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.

(74) "MAC address" is an abbreviation for media access control address.

(75) "MAN" is an abbreviation for metropolitan area network.

(76) "MANAGED ACCESS PUBLIC" (written in all capital letters) means the data classification category defined in section 8-902.

(77) "May" means that an item is truly optional.

(78) "Media access control address" means a unique identifier assigned to network interfaces for communications at the data link layer of a network segment.

(79) "Metropolitan area network" means a data communications network that (a) covers an area larger than a local area network and smaller than a wide area network, (b) interconnects two or more local area networks, and (c) usually covers an entire metropolitan area, such as a large city and its suburbs.

(80) "Must" means an absolute requirement of the specification.

(81) "Must not" means an absolute prohibition of the specification.

(82) "Nebraska Information Technology Commission" means the information technology governing body created in Neb. Rev. Stat. § 86-515.

(83) "Network interface card" means 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.

(84) “Network Nebraska” means the network created pursuant to Neb. Rev. Stat. § 86-5,100.

(85) “NIC” is an abbreviation for network interface card.

(86) “NIST” is an abbreviation for National Institute of Standards and Technology, a federal government entity, part of the U.S. Department of Commerce, which develops technical standards, guidelines, and frameworks.

(87) “NITC” is an abbreviation for Nebraska Information Technology Commission.

(88) “Not recommended” has the same meaning as should not.

(89) “OCIO” is an abbreviation for Office of the Chief Information Officer.

(90) “Office of the Chief Information Officer” means the 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 division are part of the Office of the Chief Information Officer.

(91) “Office of the CIO” is an abbreviation for Office of the Chief Information Officer.

(92) “Optional” has the same meaning as may.

(93) “PCI” is an abbreviation for Payment Card Industry. The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for credit card account data protection.

(94) “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.

(95) “Physical security” means 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.

(96) “Policy” means an NITC document that establishes a set of consistent rules and the means of achieving them that support the business objectives for the state.

(97) “Principle of least privilege” means a framework that requires users be given no more access privileges 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.

(98) “Privacy” means the right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

(99) “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: (a) social security number; (b) driver's license number or non-driver identification card number; or (c) 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.

(100) "Privileged access account" means the user ID or account of an individual whose job responsibilities require special system authorization, such as a network administrator or security administrator. Special authorizations are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator.

(101) "Procedures" means the specific operational steps that individuals must take to achieve goals stated in the NITC standards and guidelines documents.

(102) "PUBLIC" (written in all capital letters) means the data classification category defined in section 8-902.

(103) "Recommended" has the same meaning as should.

(104) "Records Management Act" means the Nebraska records management statutes codified at Neb. Rev. Stat. §§ 84-1201 to 84-1228.

(105) "Records Officer" means the agency representative who is responsible for the overall coordination of records management activities within the agency.

(106) "Recovery" means a defined step or process within an incident response plan with the goal of returning the affected or compromised systems to normal operations.

(107) "Required" has the same meaning as must.

(108) "RESTRICTED" (written in all capital letters) means the data classification category defined in section 8-902.

(109) "Risk" means 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.

(110) "Risk assessment" means 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.

(111) "Risk management" means the process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

(112) "Router" means 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.

(113) “Security management” means the responsibility and actions required to manage the security environment including the security policies and mechanisms.

(114) “Security policy” means 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.

(115) “Sensitive information” means data, which if disclosed or modified, would be in violation of law, or could harm an individual, business, or the reputation of the agency.

(116) “Sensitivity” means the measurable, harmful impact resulting from disclosure, modification, or destruction of information.

(117) “Separation of duties” means the concept that no individual should have control over two or more phases of an operation or areas of conflicting responsibility.

(118) “Shall” has the same meaning as must.

(119) “Shall not” has the same meaning as must not.

(120) “Should” means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighted before choosing a different course.

(121) “Should not” means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighted before implementing any behavior described with this label.

(122) “SISO” is an abbreviation for state information security officer.

(123) “SNMP” is an abbreviation for Simple Network Management Protocol, a common protocol for network management.

(124) “Staff” means state employees and other persons performing work on behalf of the state.

(125) “Standard” means a set 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.

(126) “Standards and guidelines” means 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

(127) “State” means the State of Nebraska.

(128) “State information security officer” means the individual employed by the state with such title.

(129) “State network” has the same meaning as communications system.

(130) “Switch” means 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.

(131) “System” means 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.

(132) “System development life cycle” means a software development process that includes defining the system requirements, the design specifications, the software development, installation and training, maintenance, and disposal.

(133) “TCP/IP” is 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.

(134) “Technical panel” means the panel created in Neb. Rev. Stat. § 86-521.

(135) “Threat” means 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.

(136) “Token” means a device that operates much like a smart card but is in a physical shape that makes its use easier to manage.

(137) “Trojan horse” means code hidden in a legitimate program that when executed performs some unauthorized activity or function.

(138) “UID” is an abbreviation for user ID.

(139) “Unauthorized access or privileges” means access to network or computer resources without permission.

(140) “User” means a person who is authorized to use an information technology resource.

(141) “User ID” is an abbreviation for user identifier, and means a system value, when associated with other access control criteria, used to determine which system resources a user can access.

(142) “Virtual local area network” means 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.

(143) "Virtual private network" means 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.

(144) "Virus" means 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).

(145) "VLAN" is an abbreviation from virtual local area network.

(146) "VPN" is an abbreviation for virtual private network.

(147) "Vulnerability" means 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.

(148) "Vulnerability scanning" means 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.

(149) "Web application" means an application that is accessed with a web browser over a network such as the Internet or an intranet.

(150) "Web page" means 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.

(151) "Web site" or "website" means 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.

(152) "Wide area network" means 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 and is usually spread over a larger geographic area.

(153) "Wireless local area network" means the linking of two or more computers without using wires. A wireless local area network 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.

(154) "WAN" is an abbreviation for wide area network.

(155) "WLAN" is an abbreviation for wireless local area network.

(156) "Worm" means a program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.

--

History: Adopted on March 4, 2008. Amended on July 12, 2017.
Operative Date: Subsections (23), (76), (102) and (108) become operative on December 1, 2017.
URL: http://nitc.nebraska.gov/standards/1-101.pdf