CHAPTER 1

GENERAL PROVISIONS

Article.

--

URL: https://nitc.nebraska.gov/standards/1-Chapter.pdf

ARTICLE 1

DEFINITIONS AND GENERAL MATTERS

Section.

1-101. Definitions.

Subject to additional definitions contained in subsequent chapters which are applicable to specific chapters or parts thereof, and unless the context otherwise requires, in the 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) "Authenticator" means something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. This was previously referred to as a token. [Source: NIST SP 800-53, REV. 5]

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

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

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

(10) "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.

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

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

(13) "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.

(14) "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.

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

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

(17) "CIS" is an abbreviation for Center for Internet Security, Inc., a nonprofit entity, which develops controls, benchmarks, and best practices for securing IT systems and data. [https://www.cisecurity.org/]

(18) "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]

(19) "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."

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

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

(22) "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)]

(23) “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)]

(24) “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.

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

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

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

(28) “Cookie” has the same meaning as web cookie.

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

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

(31) “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.

(32) “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.

(33) “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.

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

(35) “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.

(36) “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.

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

(38) “DNS” is an abbreviation for Domain Name System, a hierarchical decentralized naming system for computers, services, or other resources connected to the internet or a private network.

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

(40) “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]

(41) “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.

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

(43) “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.

(44) "External service provider" means a non-agency consultant, contractor, or vendor.

(45) "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/]

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

(47) "Firewall" means a security mechanism that creates a barrier between an internal network and an external network.

(48) "FTI" is an abbreviation for Federal Tax Information, meaning 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.

(49) "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.

(50) "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.

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

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

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

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

(55) "HIGH IMPACT" (written in all capital letters) means the data classification category defined in section 8-902.

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

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

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

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

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

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

(62) "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.

(63) "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.

(64) "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.

(65) "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]

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

(67) "Information technology project" means an endeavor undertaken over a fixed period of time using information technology. An information technology project includes all aspects of planning, design, implementation, project management, and training related to the endeavor. [Source: based on Neb. Rev. Stat. § 86-506]

(68) "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.

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

(70) "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.

(71) "Internal network" means an internal, non-public network that uses the same technology and protocols as the internet.

(72) "Internet Protocol" means a packet-based protocol for delivering data across networks.

(73) "IP" is an abbreviation for Internet Protocol.

(74) "IT" is an abbreviation for information technology.

(75) "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.

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

(77) "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.

(78) "LOW IMPACT" (written in all capital letters) means the data classification category defined in section 8-902.

(79) "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.

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

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

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

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

(84) "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.

(85) "Mobile device" means a portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable data storage; and is powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers. [Source: NIST SP 800-53, REV. 5]

(86) "MODERATE IMPACT" (written in all capital letters) means the data classification category defined in section 8-902.

(87) "Multi-factor authentication" means an authentication system or an authenticator that requires more than one authentication factor for successful authentication. Multi-factor authentication can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are. See *authenticator*. [Source: NIST SP 800-53, REV. 5]

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

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

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

(91) "NebraskaMAP portal" means the state government website (https://www.nebraskamap.gov/) dedicated to providing Nebraska related geospatial data and information. The website provides a centralized location to search and locate relevant authoritative geospatial data layers in Nebraska, and to print maps and data tables. The website is hosted and maintained by the Office of the CIO, and agencies contribute authoritative data to the website.

(92) "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.

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

(94) "NIC" is an abbreviation for network interface card.

(95) "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.

(96) "NITC" is an abbreviation for Nebraska Information Technology Commission.

(97) "NO IMPACT" (written in all capital letters) means the data classification category defined in section 8-902.

(98) "Not recommended" has the same meaning as should not.

(99) "OCIO" is an abbreviation for Office of the Chief Information Officer.

(100) "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.

(101) "Office of the CIO" is an abbreviation for Office of the Chief Information Officer.

(102) "Optional" has the same meaning as may.

(103) "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.

(104) "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.

(105) "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.

(106) "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.

(107) "Portable storage device" means a system component that can communicate with and be added to or removed from a system or network and that is limited to data storage—including text, video, audio or image data—as its primary function (e.g., optical discs, external or removable hard drives, external or removable solid-state disk drives, magnetic or optical tapes,

flash memory devices, flash memory cards, and other external or removable disks). [Source: NIST SP 800-53, REV. 5]

(108) "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.

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

(110) "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.

(111) "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.

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

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

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

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

(116) "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.

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

(118) "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.

(119) “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.

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

(121) “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.

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

(123) “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.

(124) “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.

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

(126) “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.

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

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

(129) “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.

(130) “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.

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

(132) “SMTP” is an abbreviation for Simple Mail Transfer Protocol, an internet standard for email transmission.

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

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

(135) “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.

(136) “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.

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

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

(139) “State network” means the public or private IP space that is owned, registered to, or managed by the State of Nebraska wherein restrictions are established to promote a secured environment.

(140) “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.

(141) “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.

(142) “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.

(143) “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.

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

(145) “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.

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

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

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

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

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

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

(152) “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.

(153) “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.

(154) “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).

(155) “VLAN” is an abbreviation from virtual local area network.

(156) “VPN” is an abbreviation for virtual private network.

(157) “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.

(158) “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.

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

(160) "Web cookie" means a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing.

(161) "Web page" means a non-embedded resource obtained from a single Universal Resource Identifier (URI) using Hypertext Transfer Protocol (HTTP) plus any other resources that are provided for the rendering, retrieval, and presentation of content.

(162) "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.

(163) "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.

(164) "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.

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

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

(167) "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; July 12, 2018; November 8, 2018; November 14, 2019; November 4, 2021; November 10, 2022; and July 14, 2023.
URL: https://nitc.nebraska.gov/standards/1-101.pdf

1-102. Authority; applicability.

(1) Authority. These technical standards and guidelines are adopted pursuant to Neb. Rev. Stat. § 86-516, which provides:

> "The commission shall: … (6) Adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. Such standards and guidelines shall not unnecessarily restrict the use of new technologies or prevent commercial competition, including competition with Network Nebraska; …."

(2) Applicability. These technical standards and guidelines apply to all state agencies, boards, and commissions, except the following:

(a) The Legislature;

(b) The Supreme Court and other judicial branch entities;

(c) Offices of the constitutional officers established in article IV of the Nebraska Constitution;

(d) Educational entities established in article VII of the Nebraska Constitution; and

(e) Such other agencies or entities established by the Nebraska Constitution.

(3) For the agencies and entities listed in subsections (2)(a) through (2)(e), standards or other mandatory requirements contained in these technical standards and guidelines should be treated as guidelines or recommendations.

--

History: Adopted on March 12, 2020.
URL: https://nitc.nebraska.gov/standards/1-102.pdf

1-103. Waiver policy.

(1) Purpose. There may be circumstances that justify noncompliance with a standard issued by the commission. This policy authorizes the Technical Panel, upon a determination of good cause shown, to issue waivers relating to the commission's technical standards.

(2) Request. An agency may request a waiver by submitting the following information to the Technical Panel:

(a) The specific section(s) at issue;

(b) A description of the problem and justification for the waiver; and

(c) A description of the agency's preferred solution.

Requests may be submitted by email to: ocio.nitc@nebraska.gov.

(3) Temporary Waiver. The state information security officer may grant a temporary waiver, subject to further review as provided in this section.

(4) Review. The Technical Panel will consider the request at their next regularly scheduled meeting. The panel may ask for additional information from the submitting agency and may postpone their decision for one meeting. After reviewing the request, and any comments received, the panel may approve the request, approve the request with conditions, or deny the request.

(5) Appeal. A denial or an approval with conditions by the Technical Panel may be appealed to the commission.

--

History: Adopted on March 4, 2008. Amended on July 12, 2018 and July 12, 2024.
URL: https://nitc.nebraska.gov/standards/1-103.pdf

ARTICLE 2

PLANNING AND PROJECT MANAGEMENT

Section.

1-201. Information technology plans.

Neb. Rev. Stat. § 86-524.01 provides:

> “On or before September 15 of each even-numbered year, all state agencies, boards, and commissions shall report to the Chief Information Officer, in a format determined by the commission, an information technology plan that includes an accounting of all technology assets, including planned acquisitions and upgrades."

The form posted at the following URL is the approved format for information technology plans: https://cioapps.nebraska.gov/ITPlan.

--

History: Adopted on June 18, 2008. Amended on July 12, 2010; May 29, 2012; August 14, 2014; July 14, 2016; and July 12, 2018.
URL: https://nitc.nebraska.gov/standards/1-201.pdf

1-202. Project reviews; information technology projects submitted as part of the state biennial budget process.

Neb. Rev. Stat. § 86-516 provides, in pertinent part:

> "The commission shall: …. (5) Adopt guidelines regarding project planning and management and administrative and technical review procedures involving state-owned or state-supported technology and infrastructure. Governmental entities, state agencies, and noneducation political subdivisions shall submit all projects which use any combination of general funds, federal funds, or cash funds for information technology purposes to the process established by sections 86-512 to 86-524. The commission may adopt policies that establish the format and minimum requirements for project submissions. The commission may monitor the progress of any such project and may require progress reports; …. (8) By November 15 of each even-numbered year, make recommendations on technology investments to the Governor and the Legislature, including a prioritized list of projects, reviewed by the technical panel pursuant to section 86-521. The recommendations submitted to the Legislature shall be submitted electronically; …."

This policy provides the format, minimum requirements, and review procedures for information technology projects submitted as part of the state biennial budget process. The requirements are as follows:

(1) Format. Budget requests for information technology projects that meet the minimum requirements set forth in subsection (2) must include a completed information technology project proposal form. The form provided in the Nebraska Budget Request and Reporting System is the approved format for information technology project proposals.

(2) Minimum Requirements for Project Submissions.

(a) Information technology projects that meet the following criteria are subject to the project review requirements of this section: (i) the estimated total project costs are more than $500,000, or (ii) the estimated total project costs are more than $50,000, and the project will have a significant effect on a core business function or multiple agencies.

(b) Exceptions. The following information technology projects are not subject to the project review requirements of this section and do not require the submission of a project proposal: (i) multi-year projects that have been reviewed as part of a previous budget submission; or (ii) projects utilizing the enterprise content management system managed by the Office of the CIO.

(3) Technical Review Procedures. The technical review of information technology projects submitted pursuant to this section will consist of the following steps:

(a) Individual Technical Reviewers. Each project will be reviewed and scored by three individual technical reviewers using review and scoring criteria approved by the Technical Panel. Qualified reviewers include: members of the Technical Panel, members and alternates of the advisory councils chartered by the commission, and such other individuals as approved by the Technical Panel.

Assignment of Reviewers. Individual technical reviewers will be assigned to projects as follows: (1) staff will assign three reviewers for each project based on the subject matter of the project; (2) staff will notify Technical Panel members by email of the initial assignment of reviewers; (3) members will have 24 hours to object to any of the reviewer assignments, objections to be made by email to the other members noting the specific assignment for which there is an objection and the reason(s) for the objection; (4) if there are objections, reassignments will be made and communicated in the same manner as the initial assignment, or the Technical Panel chairperson may call a special meeting of the Technical Panel to assign reviewers; (5) staff will provide the assigned reviewers with the project review documents; (6) in the event a reviewer is unable to complete an assigned review, a new reviewer will be assigned using the same process as the initial assignment; and (7) if for any reason less than three individual reviews are completed prior to the Technical Panel's review referenced in subsection (3)(d), the Technical Panel may complete the project review without regard to the requirements of this subsection.

(b) Agency Response. The requesting agency will be provided with the reviewer scores and comments. The agency may submit a written response to the reviewer scores and comments. The deadline for submitting a response will be one week prior to the Technical Panel review referenced in subsection (3)(d).

(c) Advisory Council Review. Depending on the subject matter of a project, one or more of the commission's advisory councils may review the project and provide recommendations to the Technical Panel and commission.

(d) Technical Panel Review. The Technical Panel will review each project including the reviewer scores and comments, any agency response, and any recommendations by the advisory councils. The Technical Panel will provide its analysis to the commission.

(e) Commission Review and Recommendations. The commission will review each project including any recommendations from the Technical Panel and advisory councils. The commission will make recommendations on each project for inclusion in its report to the Governor and the Legislature.

--

History: Adopted on June 18, 2008. Amended on June 16, 2010; August 15, 2012; August 14, 2014; July 14, 2016; July 12, 2018; and July 14, 2023.

URL: https://nitc.nebraska.gov/standards/1-202.pdf

1-203. Project progress reports.

Neb. Rev. Stat. § 86-516 provides, in pertinent part:

> "The commission shall: …. (5) Adopt guidelines regarding project planning and management and administrative and technical review procedures involving state-owned or state-supported technology and infrastructure. Governmental entities, state agencies, and noneducation political subdivisions shall submit all projects which use any combination of general funds, federal funds, or cash funds for information technology purposes to the process established by sections 86-512 to 86-524. The commission may adopt policies that establish the format and minimum requirements for project submissions. The commission may monitor the progress of any such project and may require progress reports; …."

(1) The commission shall determine which information technology projects are required to submit progress reports.

(2) The Technical Panel is responsible for all logistical matters relating to the submission of progress reports pursuant to this section, including the frequency and format of the reports. The panel will coordinate with the reporting agency to ensure compliance with this section. The panel will provide regular reports to the commission on the status of projects.

--

History: Adopted on November 12, 2008. Amended on July 12, 2018.
URL: https://nitc.nebraska.gov/standards/1-203.pdf

1-204. Procurement review policy.

(1) Purpose. Pursuant to Neb. Rev. Stat. §§ 81-1117, 81-1120.17, and 81-1120.20, certain state agency purchases of communications equipment and information management items require the approval of the Office of the CIO. This policy provides guidance to agencies for compliance with these statutory requirements.

(2) Information Needed for Procurement Reviews.

(a) Agency Information Technology Plan. The agency information technology plan, which is submitted in conjunction with the biennial budget request, provides the general context for procurement decisions. In some cases, a diagram and explanation of the technical architecture is necessary for determining the appropriate technology for the purpose. Technical architecture describes the hardware, software and network infrastructure needed to support the deployment of core, mission-critical applications. The specific documentation that is useful depends on the type of purchase.

(b) Documentation for Purchase Requisitions and Purchase Orders in NIS Using Document Types ON and 06. Agencies must attach sufficient information in NIS that allows the reviewer to determine what is being purchased, the purpose being served, total cost, and a contact for additional information. This information can be provided as either a text note or an attachment to the header in NIS. In addition, the following types of documents are helpful, if available: (1) bill of materiel from the vendor, or (2) quotation from the vendor.

(c) Documentation for Competitive Solicitations Request for Proposals ("RFP"), Requests for Information ("RFI"), and Invitations to Bid ("ITB"). Agencies must provide a draft copy of the solicitation—RFP, RFI, or ITB—to the Office of the CIO at least 30 days prior to its planned release.

(d) Documentation for Requests for Deviation from the Competitive Process. Agencies must document the reasons for not following the competitive process.

(3) Review Criteria. In making the decision to approve or deny the procurement request, the decision of the Office of the CIO shall be based upon, but not necessarily limited to: (a) compliance with NITC technical standards and enterprise architecture; (b) avoidance of unnecessary expenditures; (c) opportunities for collaboration or data sharing, if applicable; (d) appropriate technology for the task; and (e) needed skills or resources within the capability of the agency to provide or acquire.

(4) Review Timelines. The timelines for reviews to be complete are as follows:

(a) Routine purchases recorded in NIS (using document types ON and 06), such as computers, laptops, printers, and low cost items will be reviewed and acted upon within one workday;

(b) Procurement requests that are more complex will be reviewed and acted upon within three workdays. The action may be a request for clarification or additional information. The goal is to resolve all issues and provide a final action within ten workdays, excluding the time an agency requires to respond to requests for additional information; and

(c) Reviews of major solicitations (RFPs, RFIs, ITBs) will be reviewed and acted upon within seven workdays. The action may be a request for clarification or additional information. The goal is to resolve all issues and provide a final action within 12 workdays, excluding the time an agency requires to respond to requests for additional information.

(5) Pre-Approved Items for Purchase. The Office of the CIO will create, and update as needed, a list of pre-approved items for purchase by agencies. The list will identify communications equipment and information management items that by their nature pose little risk of violating the criteria established in subsection (3). The list will be posted as section 1-205 of these standards. Agencies have prior approval to purchase items on this list. (See section 1-205, http://nitc.nebraska.gov/standards/1-205.pdf)

--

History: Adopted on March 4, 2008. Amended on November 30, 2009 and July 12, 2018.
URL: https://nitc.nebraska.gov/standards/1-204.pdf

1-205. List of pre-approved items for purchase.

For the purpose of procurement reviews conducted pursuant to Neb. Rev. Stat. §§ 81-1117, 81-1120.17, and 81-1120.20, the following items are pre-approved for purchase by an agency:

(1) cables for connecting computer components;

(2) KVM switches;

(3) microphones;

(4) speakers;

(5) smart board overlays;

(6) projectors;

(7) digital voice recorders;

(8) flash drives;

(9) logic boards and computers that are integral parts of equipment that serves a primary purpose other than information management, including digital cameras, lab equipment, and motor vehicles; and

(10) such other items as specified on the Office of the CIO website at: https://bit.ly/3yxkF5Y.

--

History: Adopted on March 4, 2008. Amended and renumbered on July 12, 2018 (previously was § 1-204-Attachment A). Amended by the Office of the CIO on May 13, 2008; November 30, 2009; February 14, 2012; May 13, 2014; September 13, 2018; January 31, 2019; August 5, 2021; and July 1, 2022.

URL: https://nitc.nebraska.gov/standards/1-205.pdf

1-206. Enterprise projects.

Neb. Rev. Stat. § 86-526 provides:

> "The commission shall determine which proposed information technology projects are enterprise projects. The commission shall create policies and procedures for the designation of such projects. The commission shall evaluate designated enterprise project plans as authorized in section 86-528."

(1) Designation. The commission will use the following factors when considering whether to designate an information technology project as an enterprise project: (a) the definition from Neb. Rev. Stat. § 86-506, "[e]nterprise 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…."; (b) whether the project is funded from the Information Technology Infrastructure Fund; (c) recommendations from the Technical Panel or the advisory councils; (d) the size, scope, and complexity of the project; and (e) such other factors as the commission deems appropriate.

(2) Progress Reports. The responsible agency for each enterprise project must submit periodic progress reports pursuant to the requirements of section 1-203.

(3) Requirements for Enterprise Projects with an Appropriation from the Information Technology Infrastructure Fund ("ITIF"). Enterprise projects receiving funding from the ITIF are subject to additional requirements codified in Neb. Rev. Stat. § 86-528. The Technical Panel will coordinate with the responsible agency on matters relating to compliance with this subsection.

(a) Project Plan. The responsible agency for an ITIF-funded enterprise project must submit a project plan to the commission. The project plan shall include, but not be limited to, the objectives, scope, and justification of the project; detailed specifications and analyses that guide the project from beginning to conclusion; technical requirements; and project management.

(b) Project Plan Review and Approval. The commission shall review each project plan submitted pursuant to subsection (3). The commission may request clarification or require changes to the project plan. In its review, the commission shall determine whether the objectives, scope, timeframe, and budget of the project are consistent with the proposal authorized by the Legislature in its allocation from the ITIF. The commission may also evaluate whether the project plan is consistent with the statewide technology plan and the commission's technical standards and guidelines. At the conclusion of its review, the commission may either approve or conditionally approve a project plan.

--

History: Adopted on November 12, 2008. Renumbered on July 12, 2018 (previously was § 1-205). Amended on July 12, 2018.
URL: https://nitc.nebraska.gov/standards/1-206.pdf

RESOURCE DOCUMENTS

Section.

1-RD-01. Table: Statutory references; cross references.

NITC Section	References to	Referred to in
1-101	Neb. Rev. Stat. §§ 81-1120.02, 81-2402, 84-1201 to 84-1228, 86-505, 86-506, 86-507, 86-509, 86-515, 86-516, 86-519, 86-521, 86-526 and 86-5,100. NITC § 8-902.	
1-102	Neb. Rev. Stat. § 86-516.	
1-103		NITC § 8-104.
1-201	Neb. Rev. Stat. § 86-524.01.	
1-202	Neb. Rev. Stat. § 86-516.	
1-203	Neb. Rev. Stat. § 86-516.	NITC § 1-206.
1-204	Neb. Rev. Stat. §§ 81-1117, 81-1120.17, and 81-1120.20. NITC § 1-205.	
1-205	Neb. Rev. Stat. §§ 81-1117, 81-1120.17, and 81-1120.20.	NITC § 1-204.
1-206	Neb. Rev. Stat. §§ 86-506, 86-526, and 86-528. NITC § 1-203.	
3-201	Neb. Rev. Stat. § 86-516.	
3-301	Neb. Rev. Stat. § 76-2502.	
3-202	Neb. Rev. Stat. §§ 76-2502 and 86-516.	
7-101	Neb. Rev. Stat. §§ 49-14,101.01, 49-14,101.02, and 81-1120.27.	NITC § 8-201.
7-201	Neb. Rev. Stat. § 86-520.01.	
8-104	NITC § 1-103.	
8-201	Neb. Rev. Stat. § 49-14,101.01. NITC § 7-101.	
8-202		NITC § 8-602.
8-209	NITC §§ 8-210 and 8-211.	

NITC Section	References to	Referred to in
8-210		NITC § 8-209.
8-211		NITC § 8-209.
8-504		NITC § 8-508.
8-508	NITC § 8-504.	
8-602	NITC § 8-202.	
8-902		NITC § 1-101.

--

Date: November 8, 2024.
URL: https://nitc.nebraska.gov/standards/1-RD-01.pdf

1-RD-02. Tables: Waivers.

(1) Waivers; current.

Agency / Entity	Section	Status
Commission on Public Advocacy	5-201	(7/14/2009) Technical Panel approved waiver with condition.
Dept. of Revenue	7-104	(11/12/2013) Technical Panel approved waiver.
Collaborative Aggregation Partnership	7-104	(7/8/2014) Technical Panel approved waiver.
Game and Parks Commission	7-104	(10/14/2014) Technical Panel approved waiver.
Nebraska Tourism Commission	7-104	(4/14/2015) Technical Panel approved waiver.
Dept. of Transportation	8-502(1)	(4/11/2017) Technical Panel approved waiver. (7/12/2017) Section number updated to reflect change made in Proposal 17-01.
Dept. of Correctional Services	8-504(9)	(12/12/2017) Technical Panel approved in part and denied in part the request for waiver. Approved waiver for "STA" with a condition and denied waiver for "CCC-L" and "CCC-O." (11/10/2022) Section number updated to reflect change made in Proposal 28.
Dept. of Veterans' Affairs	8-303(1); 8-303(3); and 8-504(10)	(10/30/2020) Technical Panel approved Request for Waiver 20-01. (11/10/2022) Section number updated to reflect change made in Proposal 28.
Nebraska State Patrol	8-403(3)	(10/26/2021) Technical Panel approved Request for Waiver 21-01.
Nebraska State Patrol	8-403(3)	(6/14/2022) Technical Panel approved Request for Waiver 22-01.
Dept. of Administrative Services	8-[redacted]; 8-[redacted]; 8-[redacted]; and 8-[redacted]	(8/13/2024) Technical Panel approved Request for Waiver 24-01.

(2) Waivers; archive.

Agency / Entity	Section	Status
Commission on Public Advocacy	5-201	(9/13/2005) Technical Panel approved waiver with conditions. (9/13/2007) Waiver expired.

Agency / Entity	Section	Status
Dept. of Roads	8-302	(9/13/2005) Technical Panel approved waiver with conditions. (9/13/2007) Waiver expired.
Laurel-Concord Public Schools, et al	7-403	(4/8/2008) Technical Panel approved waiver covering 2007-08 school year.
Educational Service Unit #10	7-403	(4/8/2008) Technical Panel tabled until 5/13/2008 meeting. (5/13/2008) Technical Panel approved a temporary waiver from the device control requirements of section 1.1, for a period of no more than one year beginning 7/1/2008.
Dept. of Correctional Services	8-301	(8/12/2008) Technical Panel approved temporary waivers for multiple applications. Security Work Group to recommend revision to standard to address issue. (11/12/2008) Standard amended; waivers concluded.
Dept. of Labor	8-301	(6/8/2010) Technical Panel denied with comments to agency and SISO.
Dept. of Roads	8-302	(5/8/2012) Technical Panel approved waiver; waiver expires on 11/7/2013. (11/12/2013) Technical Panel extended to 11/11/2014. (11/12/2013) Request withdrawn by agency.
Dept. of Labor	8-301	(12/14/2010) Technical Panel approved waiver; waiver expires on 6/15/2012. (6/12/2012) Technical Panel extended to 6/13/2013. (7/9/2013) Technical Panel extended to 1/10/2014. (1/10/2014) Waiver expired.
Dept. of Revenue	8-301	(8/14/2012) Technical Panel approved waiver. (2/15/2014) Waiver expired.
Kronos Steering Committee (NDCS/HHSS/OCIO)	8-301	(2/14/2012) Technical Panel approved waiver with conditions. (3/11/2014) Technical Panel revoked.
Dept. of Correctional Services	8-301	(9/10/2013) Technical Panel approved waiver. (3/11/2014) Technical Panel revoked.
Game and Parks	8-301	(1/8/2008) Technical Panel approved waiver with conditions. (4/8/2008) Conditions met. (3/11/2014) Technical Panel revoked.
Dept. of Correctional Services	8-301	(4/8/2008) Technical Panel approved waiver. (3/11/2014) Technical Panel revoked.
Office of the Capitol Commission	7-104	(7/9/2013) Technical Panel tabled consideration until requestor reviewed options with their contractor. (2/10/2015) Technical Panel dismissed.
Dept. of Economic Development	7-104	(12/9/2014) Technical Panel tabled consideration. (2/10/2015) Technical Panel dismissed.
Nebraska Wheat Board	7-104	(12/9/2014) Technical Panel tabled consideration. (2/10/2015) Technical Panel dismissed.

Agency / Entity	Section	Status
Nebraska State Historical Society	7-104	(2/10/2015) Technical Panel dismissed.
Secretary of State	5-101	(9/8/2015) Technical Panel denied.
Dept. of Health and Human Services	8-302	(7/14/2015) Technical Panel approved waiver; waiver expires on 6/30/2016. (6/30/2016) Waiver expired.
Dept. of Health and Human Services (Edifecs system)	8-301	(10/14/2014) Technical Panel approved waiver; waiver expires on 7/1/2016. (7/1/2016) Waiver expired.
Dept. of Correctional Services	8-301	(10/11/2016) Technical Panel postponed consideration. (10/12/2016) Request withdrawn by agency.
Coordinating Commission for Postsecondary Education	8-302	(9/8/2015) Technical Panel approved waiver; waiver expires on 6/30/2016. (6/14/2016) Technical Panel approved extension until 6/30/2017 with condition. (6/13/2017) Technical Panel extended to 8/8/2017. (8/8/2017) Technical Panel extended to 10/10/2017. (10/10/2017) Waiver expired.
Nebraska Judicial Branch	8-303	(6/14/2016) Technical Panel approved waiver; waiver expires on 6/13/2017. (6/13/2017) Technical Panel extended to 8/8/2017. (8/8/2017) Technical Panel extended to 10/10/2017. (10/10/2017) Waiver expired.
Nebraska Accountability and Disclosure Commission	8-103; 8-302	(6/14/2016) Technical Panel approved waiver; waiver expires on 6/13/2017. (6/13/2017) Technical Panel extended to 8/8/2017. (8/8/2017) Technical Panel extended to 10/10/2017. (10/10/2017) Waiver expired.
Dept. of Revenue	5-101	(10/10/2017) Technical Panel denied.
Dept. of Labor	7-301	(10/11/2016) Technical Panel approved waiver with condition; waiver expires on 10/31/2017. (10/31/2017) Waiver expired.
Nebraska Interactive (Nebraska.gov)	4-201	(5/8/2012) Technical Panel approved waiver. (11/9/2017) Section amended making waiver unnecessary.
Dept. of Correctional Services	8-504(8)	(12/12/2017) Technical Panel approved in part and denied in part the request for waiver. Approved waiver for "STA" with a condition and denied waiver for "CCC-L" and "CCC-O."
Dept. of Labor	5-101	(2/13/2018) Technical Panel denied. (3/8/2018) Commission denied appeal.
Game and Parks	8-302	(1/8/2008) Technical Panel approved waiver. (4/10/2018) Technical Panel revoked.

Agency / Entity	Section	Status
Dept. of Agriculture	8-302	(11/8/2011) Technical Panel approved waiver; SISO to review and report back to the Technical Panel. (2/14/2012) SISO report on file. (4/10/2018) Technical Panel revoked.
Dept. of Health and Human Services (Vital Records)	8-302	(10/14/2014) Technical Panel approved waiver. (4/10/2018) Technical Panel revoked.
Dept. of Health and Human Services	8-301; 8-302	(8/9/2016) Technical Panel approved waiver; waiver expires on 6/30/2018. SISO to update Panel by 7/31/2017. (4/10/2018) Technical Panel revoked.
Dept. of Veterans' Affairs	8-303(1); 8-303(3); and 8-504(9)	(4/10/2018) Technical Panel approved waiver; waiver expires on 4/30/2020. (4/30/2020) Waiver expired.
Dept. of Transportation	7-104	(2/9/2021) Technical Panel approved Request for Waiver 20-03; waiver expires on 11/1/2021. (11/1/2021) Waiver expired.
Nebraska State Patrol	5-101	(10/9/2012) Technical Panel approved waiver; waiver is effective for the duration of the contract. (7/14/2023) Section at issue repealed.
Dept. of Health and Human Services	7-104	(2/12/2013) Technical Panel approved waiver. (10/10/2023) Technical Panel revoked waiver.
Dept. of Economic Development	7-104	(8/8/2017) Technical Panel approved waiver. (10/10/2023) Technical Panel revoked waiver.

--

Date: August 13, 2024.
URL: https://nitc.nebraska.gov/standards/1-RD-02.pdf