NEBRASKA INFORMATION TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

Chapters.

--

Date: Contains amendments through October 10, 2023.
URL: https://nitc.nebraska.gov/standards/standards.pdf

TABLE OF CONTENTS

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) 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.

(4) 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.
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.	
3-202	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.	
8-210		NITC § 8-209.

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

--

Date: July 14, 2023.
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.

(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.
Dept. of Roads	8-302	(9/13/2005) Technical Panel approved waiver with conditions. (9/13/2007) Waiver expired.

Agency / Entity	Section	Status
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.
Nebraska State Historical Society	7-104	(2/10/2015) Technical Panel dismissed.

Agency / Entity	Section	Status
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.
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.

Agency / Entity	Section	Status
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: October 10, 2023.
URL: https://nitc.nebraska.gov/standards/1-RD-02.pdf

CHAPTER 2

ACCESSIBILITY

Article.

1. General Provisions.
2. Technology Access Clause.

--

URL: https://nitc.nebraska.gov/standards/2-Chapter.pdf

ARTICLE 1

GENERAL PROVISIONS

Section.

2-101. Accessibility policy.

(1) Purpose. This policy contains scoping and technical requirements for information and communication technology ("ICT") to ensure accessibility and usability by individuals with disabilities.

(2) Definitions. For the purpose of this section, terms defined in referenced documents and not defined in section 1-101 will have the meaning as defined in the referenced documents.

(3) Standards. ICT that is procured, developed, maintained, or used by state agencies shall conform to the following standards: Revised 508 Standards, 36 C.F.R. § 1194 (2018) [https://www.govinfo.gov/content/pkg/CFR-2018-title36-vol3/xml/CFR-2018-title36-vol3-part1194.xml].

For the State of Nebraska, the Revised 508 Standards referenced in this subsection are revised as follows:

(a) In E103.4, replace the definition of "Existing ICT" with the following: "*Existing ICT.* ICT that has been procured, maintained or used on or before November 14, 2020.";

(b) In E202.2, replace the existing language with the following: "*Legacy ICT.* Any component or portion of existing ICT that complies with an earlier standard adopted by the commission, and that has not been altered on or after November 14, 2020, shall not be required to be modified to conform to the Revised 508 Standards.";

(c) In E202.3, replace the existing language with the following: "*Public Safety Systems.* The Revised 508 Standards do not apply to any ICT operated by state agencies as part of a public safety system.";

(d) In E202.4, replace the existing language with the following: "*State Contracts.* ICT acquired by a contractor incidental to a contract shall not be required to conform to the Revised 508 Standards."; and

(e) In E203.1, replace the existing language with the following: "*General.* Agencies shall ensure that all functionality of ICT is accessible to and usable by individuals with disabilities, either directly or by supporting the use of assistive technology, and shall comply with E203. In providing access to all functionality of ICT, agencies shall ensure the following: A. That state employees with disabilities have access to and use of information and data that is comparable to the access and use by state employees who are not individuals with disabilities; and B. That members of the public with disabilities who are seeking information or data from a state agency have access to and use of information and data that is comparable to that provided to members of the public who are not individuals with disabilities.".

(4) Guidelines. In addition to the web content requirements contained in the referenced standards in subsection (3), the commission recommends compliance with the following guidelines: Web Content Accessibility Guidelines 2.1, W3C World Wide Web Consortium Recommendation 05 June 2018 [https://www.w3.org/TR/2018/REC-WCAG21-20180605/].

--

History: Adopted on October 31, 2001. Amended on November 14, 2019.
URL: https://nitc.nebraska.gov/standards/2-101.pdf

ARTICLE 2

TECHNOLOGY ACCESS CLAUSE

Section.

2-201. [Superseded.]

- The current version of the technology access clause is posted at: https://das.nebraska.gov/materiel/purchase_bureau/vendor-info.html.
- The superseded version is posted at: https://nitc.nebraska.gov/technical_panel/documents/2-201_archive.pdf.

--

History: Approved on December 12, 2000. Amendments approved by the Commission for the Blind and Visually Impaired on April 24, 2021, the Technical Panel of the Nebraska Information Technology Commission on June 8, 2021, and the Chief Information Officer on June 8, 2021. Moved to the Dept. of Administrative Services' website on August 2, 2021.
URL: https://nitc.nebraska.gov/standards/2-201.pdf

CHAPTER 3

GEOGRAPHIC INFORMATION SYSTEMS

Article.

1. GIS; State Government Standards and Guidelines.
2. GIS Data.

--

ARTICLE 1

GIS; STATE GOVERNMENT STANDARDS AND GUIDELINES

Section.

3-101. GIS software.

State agencies shall coordinate all purchases of GIS software and software maintenance through the Office of the CIO. The Office of the CIO will provide guidance to agencies on GIS software that is compatible with the state's enterprise GIS environment.

--

History: Adopted on November 8, 2018.
URL: https://nitc.nebraska.gov/standards/3-101.pdf

3-102. NebraskaMAP portal.

All agency geospatial data and GIS web applications that are available to the public shall be made accessible through the NebraskaMAP portal.

--

History: Adopted on November 8, 2018.
URL: https://nitc.nebraska.gov/standards/3-102.pdf

ARTICLE 2

GIS DATA

Section.

3-201. Geospatial metadata standard.

[Section 3-201 appears after this cover page in a legacy format.]

--

History: Adopted on September 23, 2005. Amended on July 14, 2016.
URL: https://nitc.nebraska.gov/standards/3-201.pdf

1.0 Standard

All state agencies and entities that receive state funding used, directly or indirectly, for geospatial data development or maintenance shall ensure that geospatial data it collects, produces, maintains, or purchases and which is used for policy development, implementation, or compliance review is documented with metadata compliant with the latest version of the ISO 19115:2003 group of metadata standards for geographic information. Metadata created for datasets using Federal Geographic Data Committee (FGDC) Content Standards for Digital Geospatial Metadata or other standards will need to be translated, updated, or recreated using the ISO 19115 standards.

1.1 Steps/Timeline for Implementation

a. State agencies and other applicable state funded entities shall institute procedures for complying with standard for new geospatial data development or acquisition upon adoption of standard by the NITC.

b. State agencies and other applicable state funded entities shall complete initial listing of existing, applicable geospatial data holdings within three months of the adoption of standard by NITC.

c. State agencies and other applicable state funded entities shall complete minimum documentation of existing, applicable geospatial data holdings within six months of the adoption of standard by NITC. More information about minimum requirements are identified in Appendix I. Metadata Categories and Definitions.

d. State agencies and other applicable state funded entities shall complete ISO 19115-compliant metadata documentation of existing and applicable geospatial data holdings within 12 months of the adoption of standard by NITC. Complete metadata categories and definitions are located in Appendix I.

1.2 Maintenance

The reporting of maintained metadata is important to assure correct documentation and support for intended uses of the data. Entities responsible for creating geospatial data will need to assure metadata is updated and maintained on an ongoing basis and in a timely manner. When modifications to the spatial or attribute data is completed the metadata information will also need to be updated. If necessary, these changes will need to be provided to the appropriate entity(s) responsible for performing quality control and maintenance of the metadata.

1.2.1 Reporting Errors and Handling Updates

The reporting of errors need to be directed to the primary contact identified in the metadata in a timely manner. Updated spatial and attribute information in the data will also need to be redistributed. The date field in the metadata when the last record was modified will also need to be updated to ensure proper records management and communication with others in the workflow.

2.0 Purpose and Objectives

The purposes of this standard is to preserve the public's investment in geospatial data, to save public resources by avoiding unnecessary duplication of expensive geospatial data acquisition, to minimize errors through inappropriate application of geospatial data, and to facilitate harmonious trans-agency public policy decision-making and implementation through the use of shared geospatial data.

2.1 Background

Broadly defined, geospatial data is any data that includes locational or positional information about features in the dataset. Geospatial data provides the data foundation for applications of Geographic Information System (GIS) technology.

The development and maintenance of geospatial data is usually the most expensive component in the implementation of GIS technology. In most cases, this high initial investment is justifiable because of the powerful capabilities of the technology and the fact that, if appropriately maintained, the data will be useful for a very long period, and in many cases, for a wide range of applications.

Most geospatial datasets include numerous attributes and parameters that relate to data variables, methodologies and assumptions. Knowledge and understanding of the implications of these variables is a key to the appropriate utilization of that data. Without appropriate documentation, this specialized knowledge usually resides only in the memory of the GIS specialist(s) who developed the original data. Because of the power of the GIS technology, geo-spatial analysis is increasingly being used to develop and implement a wide range of public policy. In many cases, these public policy applications endure long past the availability of the GIS-specialist(s) who developed one or more of the original geospatial datasets upon which the public policy and its subsequent implementation are based. Without appropriate documentation of attributes and parameters of a geospatial dataset assumptions and variables, it may be difficult for an agency to determine the appropriate use of a dataset after the GIS specialist who originally created the data is no longer available. Without this documentation, it may also be difficult to appropriately maintain the dataset and therefore maintain the value of the original public investment in the data. In the case of a legal challenge to a public policy or its implementation, for which geospatial data application is integral, it may be difficult to defend that application if the original data developer is no longer available and the dataset was not appropriately documented.

Due to the relatively high costs of developing and maintaining many geospatial datasets, it is important that public investments in this data are undertaken in a manner to maximize the long-term return on these public investments. Appropriately documenting a dataset is one way to ensure a dataset's long-term usability. It is also a key to enabling the use of that dataset for multiple applications by multiple users. Without documentation, it is difficult for other users within the same agency, in other state agencies, or other public entities at various levels of government to be confident they are appropriately utilizing a geospatial dataset.

One of the great strengths of GIS technology is the ability to integrate and analyze disparate data based on its common or adjacent location. GIS has evolved to be a mainstream technology, used for a very wide range of applications, highly integrated with other information technology, and employed by users with a wide range of technical expertise and knowledge. As GIS has evolved, users now routinely access geospatial data, via the Internet, from multiple sources and integrate that data with other geospatial data and make public policy decisions based on analysis of the interaction of those datasets. Only when a geospatial dataset is adequately documented is it prudent to incorporate that data into a GIS analysis.

To address this wide range of concerns and needs for geospatial data documentation, the Federal Geographic Data Committee (FGDC) has worked with a wide spectrum of geospatial data users to develop a national standard for documenting geospatial data. The FGDC has endorsed and are transitioning users from the Content Standard for Digital Geospatial Metadata (CSDGM) to the ISO Metadata Standards.

2.2 Objectives

This standard requiring the documentation of geospatial data with standardized metadata has the following objectives:

2.2.1 Preserve public investment in data collection/development beyond the tenure or availability of the original data developer.

2.2.2 Preserve the background geospatial information used to justify and make public policy decisions and preserve the information needed to guide appropriate implementation of those decisions beyond the tenure of a particular data developer.

2.2.3 Save public resources by facilitating the sharing of expensive geospatial data among public agencies or sub-divisions of agencies and avoid the costly duplication of developing similar geospatial datasets.

2.2.4 Minimize problems and potential liability that might be caused by the inappropriate use of undocumented geospatial data.

2.2.5 Facilitate harmonious, trans-agency public policy decision-making and implementation by enabling multiple agencies and levels of government to access and appropriately use common geospatial datasets and thereby make it more likely that intersecting public policy decisions, across levels of government, will be based on the same information.

3.0 Definitions

Content Standard for Digital Geospatial Metadata - A comprehensive national metadata standard developed and adopted by the Federal Geographic Data Committee (FGDC) under the authority of Executive Order 12906, "Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure," which was signed on April 11, 1994, by President William Clinton. Section 3, Development of a National Geospatial Data Clearinghouse, paragraph (b) states: "Standardized Documentation of Data, ... each agency shall document all new geospatial data it collects or produces, either directly or indirectly, using the standard under development by the FGDC, and make that standardized documentation electronically accessible to the Clearinghouse network." This standard is the data documentation standard referenced in the executive order. Since its initial development, this metadata content standard has undergone revision as deemed necessary by the FGDC, and will like undergo further revisions in the future.

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

ISO 19115:2003 **–** International Standards Organization (ISO) defines the schema required for describing geographic information and services. It provides information about the identification, the extent, the quality, the spatial and temporal schema, spatial reference, and distribution of digital geographic data. It is applicable to: the cataloguing of datasets, clearinghouse activities, and the full description of datasets; and geographic datasets, dataset series, and individual geographic features and feature properties. It defines: mandatory and conditional metadata sections, metadata entities, and metadata elements; the minimum set of metadata required to serve the full range of metadata applications (data discovery, determining data fitness for use, data access, data transfer, and use of digital data); optional metadata elements - to allow for a more extensive standard description of geographic data, if

required; and a method for extending metadata to fit specialized needs. It is applicable to digital data, its principles can be extended to many other forms of geographic data such as maps, charts, and textual documents as well as non-geographic data.

Metadata - Data describing a GIS database or data set including, but not limited to, a description of a data transfer mediums, format, and contents, source lineage data, and any other applicable data processing algorithms or procedures.

4.0 Applicability

4.1 State Government Agencies

State agencies that have the primary responsibility for geospatial data development, maintenance, or purchasing data which is used for policy development, implementation, or compliance review for a particular jurisdiction(s) or geographic area (e.g. for counties for which it has assumed the primary role) are required to comply with the standards as described in this standard. Those state agencies with oversight responsibilities in this area are required to ensure that their oversight guidelines, rules, and regulations are consistent with these standards.

4.2 State Funded Entities

Entities that are not State agencies but receive State funding, directly or indirectly, for geospatial data development (i.e. Legislative appropriations, Enhanced Wireless 911 Fund, Infrastructure Fund, etc.) are required to comply with this standard.

4.3 Other

Other entities, such as city and local government agencies that receive state funds for geospatial data development, maintenance, or purchasing geospatial data which is used for policy development, implementation, or compliance review are required to comply with this standard.

5.0 Responsibility

5.1 NITC

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. Neb. Rev. Stat. § 86-516(6)

5.2 State Agencies

Each state agency will be responsible for ensuring that geospatial data developed, maintained, or purchased and which is used for policy development, implementation, or compliance review will be documented consistent with this standard. The State of Nebraska, Office of the CIO (OCIO) GIS Shared Services will be responsible for assuring that metadata is completed and the data is registered and available for distribution through NebraskaMAP.

5.3 Granting Agencies and Entities

State granting or fund disbursement entities or agencies will be responsible for ensuring geospatial metadata documentation requirements are included in requirements and regulations related to fund disbursements.

5.4 Other

Local government agencies that have the primary responsibility and authority for developing geospatial datasets with state appropriated funds will be responsible for ensuring that those sub-sections defined in Section 1 will be incorporated in the overall data development efforts and publishing of metadata prior to distribution.

6.0 Authority

6.1 NITC GIS Council

According to Neb. Rev. Stat. § 86-572(2), the GIS Council shall: Establish guidelines and policies for statewide Geographic Information Systems operations and management (a) The acquisition, development, maintenance, quality assurance such as standards, access, ownership, cost recovery, and priorities of data bases; (b) The compatibility, acquisition, and communications of hardware and software; (c) The assessment of needs, identification of scope, setting of standards, and determination of an appropriate enforcement mechanism; (d) The fostering of training programs and promoting education and information about the Geographic Information Systems; and (e) The promoting of the Geographic Information Systems development in the State of Nebraska and providing or coordinating additional support to address Geographic Information Systems issues as such issues arise.

7.0 Related Documents

7.1 Federal Geographic Data Committee (FGDC) Content Standards for Digital Geospatial Metadata (FGDC-STD-001-1998). http://www.fgdc.gov/standards/projects/FGDC-standards-projects/metadata/base-metadata/index_html

7.2 Federal Geographic Data Committee (FGDC) Geospatial ISO Metadata Standards Transition. http://www.fgdc.gov/metadata/geospatial-metadata-standards

7.3 ISO 19115:2003(E) North American Profile (NAP) Metadata Standards. National Oceanic and Atmospheric Administration (NOAA). January 2012.

7.4 International Standards Organization (ISO). ISO 19115:2003. http://www.iso.org

7.5 Technical Support Guides at NebraskaMAP.gov. Guides to translate existing metadata to the new standard, required core elements, and workbook for ISO standards.

Appendix I – Metadata Categories and Definitions

This document provides categories and definitions of metadata information required for State of Nebraska geospatial data layers. The minimum and complete metadata requirements and timelines for completion involve the following:

- **Minimum**, completed within six months of data origination
  (Minimum fields are indicated with a **bold** (**M)** throughout this document.)

  Minimum: A subset of the ISO 19115-compliant metadata used primarily for the purposes of cataloging and enabling the use of automated search tools to find and access available geospatial data. Does not fully document the dataset's variables, assumptions or development process that is commonly needed to guide appropriate use.

- Complete Metadata, optional categories, recommended to be completed within 12 months

  Complete Metadata: Remainder of ISO 19115-compliant metadata beyond minimum as indicated throughout this document.

1. Overview

   a. Item Description
      i. **(M) Title -** ***The name by which the resource is known.***
      ii. Thumbnail - *A small graphic file stored that graphically identifies the resource.*
      iii. Tags - *A set of terms that can be used to search for the resource.*
      iv. Summary(Purpose) - *A summary of the intentions with which the resource was developed.*
      v. **(M) Description (Abstract) -** ***A brief narrative summary of the resources content.***
      vi. Credits - *A recognition of those who created or contributed to the resource.*
      vii. Use Limitation - *Describes limitations affecting the fitness of use of the resource.*
      viii. Appropriate Scale Range - *The range of scales at which this resource should be used.*

   b. Topics & Keywords
      i. **(M) ISO topic categories -** ***Identifies the primary ISO themes associated with the resources content.***

Utilities & Communication	**Military & Intelligence**	**Boundaries**	**Farming**
Atmospheric Sciences	**Economy**	**Elevation**	**Biota**
Environment	**Geoscientific**	**Health**	**Society**
Imagery & Base Maps	**Structure**	**Inland Waters**	**Transportation**
Planning & Cadastral	**Oceans**	**Location**	

      ii. Content Type - *Indicates how you can access a shared copy of the resource.*
      iii. Keywords - *Keywords that associate the resource with a subject or topic.*

   c. Citation
      i. **(M) Title –** ***Title of the map that describes the manner in which the resource is represented. Could represent years and general idea of extent such as county or city.***
      ii. Presentation Form - *Indicates the form in which the resource is provided.*

iii. **(M) Date - *Date when the resource was created, published or revised.***

d. Citation Contacts
   i. Name - *The name of a person associated with the resource.*
   ii. Organization - *The name of an organization associated with the resource.*
   iii. Position - *The name of a role or position associated with the resource.*
   iv. Role - *Identifies the association between the responsible party and the resource.*

2. Metadata

a. Details
   i. **(M) File Identifier - *A unique identifier for the metadata. Typically a GUID, or country code.***
   ii. Parent Identifier - *Unique identifier of the dataset to which this metadata is a subset.*
   iii. Dataset URI - *The Uniform Resource Identifier (URI) of the resource.*
   iv. Function - *Identifies the function available at the specified URI for this resource.*
   v. **(M) Date - *The date when the metadata was created or updated.***
   vi. **(M) Language - *The primary language of the information provided in the metadata.***
   vii. **(M) Country - *The country of the location.***
   viii. Character Set - *The character encoding used for the metadata. Typically UTF-8.*
   ix. Hierarchy Level - *The hierarchical scope to which the metadata applies.*

b. Contacts
   i. **(M) Name - *The name of a person associated with the resource metadata.***
   ii. **(M) Organization - *The name of an organization associated with the resource metadata.***
   iii. **(M) Position - *The name of a role or position associated with the resource metadata.***
   iv. **(M) Role - *Identifies the association between the responsible party and the resource metadata.***

      Roles can include: Resource Provider, Custodian, Owner, User, Distributor, Originator, Point of Contact, Principal Investigator, Processor, Publisher, Author, Collaborator, Editor, Mediator, Rights Holder

   v. **(M) Address – *The address for the point of contact.***
   vi. **(M) Phone – *The primary phone number for the point of contact.***

c. Maintenance
   i. **(M) Update Frequency - *The frequency with which the metadata is updated.***
   ii. Next Update - *The scheduled revision date.*
   iii. Scope - The scope of data for which this maintenance information applies.
   iv. Contact - *Contact information for the individual associated with metadata maintenance.*
   v. Maintenance Note - *Describes the specific requirements for maintaining the metadata.*

d. Constraints
   i. General - *Describes limitations affecting the fitness of use of the metadata.*
   ii. Legal - *Restrictions, limitations, or warnings on using the metadata. (If applicable)*
   iii. Security - *Identifies any handling restrictions on the metadata. (if applicable)*

3. Resource

    a. Details
        i. Status - *The status of the resource. (Ex - Under Development, Ongoing, Completed, etc.)*
        ii. Credit - *A recognition of those who created or contributed to the resource.*
        iii. Language - *The language of the information used within the data.*
        iv. Country - *The country of the location.*
        v. Spatial Representation Type - *Identifies the method used to spatially represent geographic information. (Ex - Vector, Raster, Tin, etc.)*
        vi. Scale/distance Resolution - *Level of detail provided by the resource, expressed as the scale of a comparable hardcopy map or chart.*
        vii. Browse Graphic - *File name of the graphic that provides an illustration of the resource.*
        viii. Processing Environment - *Describes the data's processing environment, including the software and operating system used, and the file name and size.*
        ix. Supplemental Information - *Provides additional descriptive information about the resource.*

    b. Service Details
        i. Name - *A name identifying the type of service provided by the resource. (Ex - WFS)*
        ii. Codespace - *Identifies the authority (Ex - 1.0.0 or 1.1.0)*
        iii. Access Properties
            1. Fees - *Describes any fees or terms for obtaining resource.*
            2. Availability Date/Period - *The date and time when the resource will be available.*
            3. Ordering Instructions - *Describes instructions, terms, and services provided by the distributor.*

    c. Extents
        i. Description - *Describes the extent of the resource. (Ex - Nebraska)*
        ii. **(M) Bounding box - *Extents expressed in decimal degrees longitude and latitude.***
        iii. Temporal Period - *The start and end time period associated with the resources content.*

    d. Points of Contact
        i. Name - *The name of a person associated with the resource.*
        ii. Organization - *The name of an organization associated with the resource.*
        iii. Position - *The name of a role or position associated with the resource.*
        iv. Role - *Identifies the association between the responsible party and the resource.*

    e. Maintenance
        i. Update Frequency - *The frequency with which the resource is updated.*
        ii. Next Update - *The scheduled revision date.*
        iii. Scope- The scope of data for which this maintenance information applies.
        iv. Contact - *Contact information for the individual associated with resource maintenance.*
        v. Maintenance Note - *Describes the specific requirements for maintaining the resource.*

    f. Constraints
        i. General - *Describes limitations affecting the fitness of use of the resource.*
        ii. Legal - *Restrictions, limitations, or warnings on using the resource. (If applicable)*
        iii. Security - *Identifies any handling restrictions on the resource. (if applicable)*

    g. Spatial Reference

i. **(M) Dimension -** ***Horizontal, vertical or temporal.***
ii. **(M) Code -** ***An alphanumeric value that identifies an authoritative reference (WKID)***
iii. **(M) Code Space -** ***An alphanumeric value that identifies an authoritative reference (Ex - EPSG)***
iv. **(M) Version -** ***An numeric value that identifies an authoritative reference (Ex - 8.2.6)***
v. **(M) Authority Citation**
    1. **Title -** ***The name by which the cited resource is known (Ex- NAD_1983_StatePlane_Nebraska_FIPS_2600_Feet)***
    2. **Date -** ***The date the cited resource was created, published or revised.***

h. Spatial Data Representation
    i. Grid Spatial, Georectified, Georeferenceable, Vector or Indirect

i. Content Information
    i. Coverage description- *Identifies the information conveyed by the raster data.(if applicable)*
    ii. Image description - *Identifies the information conveyed by the raster data.(if applicable)*
    iii. Feature Catalogue - *Describes OGC catalogue compliance, name, codespace, language and country. (if applicable)*

j. Quality
    i. Scope Level - *Describes the specific data to which the data quality information applies.*
    ii. Level Description - *Identifies the instance to which the information applies*.
    iii. Extent - Describes the extent of the resource.
    iv. Report
        1. Report Type - *Identifies the characteristic of the data whose quality was measured.*
        2. Dimension - *Identifies the axis to which the spatial quality information applies.*
        3. Description - *A description of the evaluation method.*
        4. Evaluation Method - *Identifies the type of method used to evaluate the quality of the data.*

k. Lineage
    i. Statement -*Provides a general description of the resource's lineage.*
    ii. Data Source - *A detailed description of the source.*
    iii. Process Step -
        1. **(M) Description -** ***Describes the event, transformation, or process that occurred while maintaining the resource, including any parameters or tolerances that were used*****.**
        2. Rationale - *Describes why the process step occurred.*
        3. **(M) Date -** ***Identifies the date when the process step occurred.***
        4. Processor - *The name of a person or organization associated with the process step.*

l. Distribution
    i. **(M) Distribution Format**
        1. **(M) Format Name -** ***The name of the data transfer format.***
        2. **(M) Format Version -** ***The version of the data transfer format (if applicable)***
    ii. Distributor
        1. Contact- *The name of a person or organization that is the distributor.*
        2. Ordering Process - *Fees and availability and instructions.*

3. Distribution Format - *Format name and version.*
4. Digital transfer options- *Units and transfer size, or online resource.*

m. Fields
   i. **(M) Label -** ***The name of the resource.***
      1. Entity Type
         a. Object - *An indication of the resource's type. (Ex. Table, feature class)*
         b. Count - *The number of objects contained by the resource.*
         c. **(M) Definition -** ***A description of the features contained by the dataset.***
         d. **(M) Definition Source -** ***The authority that provided the definition.***
      2. **(M) Attribute** ***(for each column)***
         a. **(M) Label -** ***The name of the field. This must match the name of a column of data in the resource.***
         b. **(M) Definition -** ***The description of the data contained by the field.***
         c. **(M) Definition Source -** ***The authority that provided the description of the field.***
         d. **(M) Type -** ***Indicates the data type used to store values in this field.***
         e. **(M) Width -** ***The number of bytes that will be used to store the data in this column for one row.***
      3. **(M) Domain**
         a. **(M) Value -** ***Describes one of the repeating values that may occur in the field.***
         b. **(M) Definition -** ***A description of the value or code stored in this field.***
         c. **(M) Source -** ***The authority that provided the description of the value.***
   ii. Overview
      1. Summary - *A detailed summary of the information provided by the data.*
      2. Citation - *A reference to the document that provides a complete description of the features, fields, and values that are provided by the resource.*

n. References
   i. Aggregate - *Citation for the aggregate information.*
   ii. Portrayal Citation - *The name by which the cited resource is known.*
   iii. Application Schema Information - *Citation for the schema.*

o. Geoprocessing History

3-202. Land record information and mapping standard.

[Section 3-202 appears after this cover page in a legacy format.]

--

History: Adopted on January 27, 2006. Amended on March 1, 2011.
URL: https://nitc.nebraska.gov/standards/3-202.pdf

1. Standard

These standards/guidelines are primarily focused on those public entities responsible for maintaining property parcel maps for their particular jurisdiction. The last line following each standard or guideline refers to the type(s) of agency or entity to which that standard/guideline applies and whether it is a standard (adherence required) or guideline (adherence voluntary) for each type of entity.

1.1 Data

Local government multipurpose GIS/LIS (Geographic Information System/Land Information System) and their associated geospatial data layers should be based on the North American Datum (NAD) 83 and the North American Vertical Datum (NAVD) 88. Any existing systems developed based on other datums should consider conversion to these datum.

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

1.2 Projection

The Nebraska (State) Plane Coordinate System, NAD 83, should be used as the primary map projection system for the recording of positions in local land-data systems in Nebraska. Selection of any other projection should be done reluctantly and only after most careful consideration. The plane coordinate values for a point on the earth's surface may be expressed in either meters or feet.

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

1.3 Geodetic Control

GIS/LIS systems developed with the goal of providing a multipurpose cadastre for local government use should be referenced to a local geodetic reference framework that is properly connected to the National Spatial Reference System (NSRS).

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

1.4 Public Land Survey System Control

1.4.1 PLSS Geodetic Framework

For all land in Nebraska that is subdivided according to the Public Land Survey System (PLSS), the geodetic reference framework for the cadastre should be the section corners of the PLSS for each section.

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

1.4.2 Locate, Monument, and GPS Primary Corners

At a minimum, local government entities developing a geospatial land information system should initially invest in a precision Global Positioning System (GPS) survey to locate, re-monument as necessary, and obtain the geographic coordinates of the major boundary defining corners that legally define the boundaries of their county jurisdiction(s). These precision GPS survey coordinates for the boundary defining corners should be collected and integrated as framework data into the land information system. This effort should be coordinated with officials from the adjacent county(ies) to ensure agreement on the location of the shared corners.

State Agencies: Standard
State Funded Entities: Standard
Other: Guideline

1.4.3 Progressive Monumentation

In addition, each county (or municipality) that is planning to develop a GIS/LIS-based cadastre program should also consider initiating a progressive program to locate and/or re-monument, as necessary, and collect geographic coordinates on other PLSS corners according to the legally established procedures and properly connect them to the National Spatial Reference System to obtain geodetic coordinates.

State Agencies: Guideline
State Funded Entities: Guideline
Other: Guideline

1.5 PLSS Base Map

Local governments considering the development of a multipurpose GIS, should consult with the Nebraska State Surveyor's Office to locate and access the best available data on the Public Land Survey System (PLSS) for their geographic area. To assist the State Surveyors Office in maintaining a repository of the best available PLSS data, local governments participating in the Nebraska Land Information System Program should share any enhanced PLSS data, for their geographic area, with the State Surveyors Office so that it might be integrated into the PLSS repository database.

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

1.6 Ortho-base (Aerial Layer) or Base Maps

Both a Public Land Survey System base map and an orthophoto (surface features) imagery base map should be used to provide the geospatial reference framework upon which a local government multipurpose land information system is developed. Both base maps should be tied to the National Spatial Reference System and have a level of spatial accuracy appropriate to the range of applications planned for a given area. Jurisdictions should acquire new imagery of urban areas at least every five years and of rural areas at least every ten years. Jurisdictions experiencing rapid or slow growth may need to adjust this timetable (IAAO 2009).

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

1.7 Map Scale and Spatial Accuracy

1.7.1 Minimum Horizontal Accuracy Standard

Public entities developing a GIS/LIS program should conduct data collection and development in a manner to achieve at least the minimum level of horizontal spatial accuracy consistent with the National Horizontal Map Accuracy Standards corresponding to a 1:12,000 (1"= 1,000') scale map (90% of the "well defined" horizontal locations must be within ±33.3 ft. of their real world location).

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

1.7.2 Additional Accuracy Considerations

Beyond this minimum horizontal map accuracy, public entities are encouraged to consider the following recommended map scales and their corresponding National Horizontal Map Accuracy Standards in determining the positional accuracy needed for base maps in the development of a local government GIS/LIS:

Relative Size of Property Parcels	Map Scale	Nat'l Horizontal Map Accuracy Standard	Equivalent Metric Scale
Urban areas	1:600 (1" = 50') 1:1,200 (1" = 100'	±1.7 ft. ±3.3 ft.	1:500 1:1,000
Large urban & suburban	1:2,400 (1" = 200')	±6.7 ft.	1:2,500
Rural areas	1:4,800 (1" = 400') 1:9,600 (1" = 800') 1:12,000 (1"= 1,000')	±13.3 ft. ±26.7 ft. ±33.3 ft.	1:5,000 1:10,000 1:10,000

State Agencies: Guideline
State Funded Entities: Guideline
Other: Guideline

1.8 Legal Lot and Parcel Layers

Data on two interrelated types of land subdivision (i.e. legally subdivided lots and ownership tracts) are necessary to provide the foundation for a wide variety of local government GIS/LIS applications that involve land subdivision and/or ownership.

a. The legal lot feature or layer consists of legal land subdivisions. These are aliquot portions of the PLSS, filed subdivision plats and irregular tracts defined by filed deeds.

b. The parcel feature or layer defines ownership tracts of land. These tracts may group multiple legal lots into one taxable account and that typically represents the boundaries of a landowner's property. These data features or layers include locational coordinates for points representing property corners, lines between property corners representing property boundaries and closed polygons representing the property area.

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

1.9 Parcel Identifiers

a. Each county/region should adopt a system of unique, permanent feature identifiers (PID) that provide the link between each graphic land ownership parcel polygon and the attribute information (ownership, size, situs address, value, etc.) related to that specific land ownership property parcel.

b. A county/region PID system must be designed in a manner such that a unique, statewide PID can be defined and maintained for each property parcel by using the county FIPS code (Federal Information Processing Standards Publications) as a prefix to the county/region's PID system.

c. To maintain this unique one-to-one association between a specific property parcel and its related attribution information, new PIDs should be assigned whenever a property parcel is altered by either splitting it into two or more parcels or by combining two or more parcels to form a new parcel. The previous PIDs should not be used for these new modified parcels, but the historical PID associations should be maintained through a parent/child PID reference table.

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

1.10 Spatial Data Format

A broad range of state and regional applications require property parcel information. Many of these applications require the combining of data across jurisdictional boundaries. To facilitate these applications, the property parcel spatial (graphic) data should be either maintained in a manner that allows it to be readily integrated into a spatial relational database format or be capable of being exported into a common geographic data format (i.e., shapefile), while including the parcel identifiers.

State Agencies: Standard
State Funded Entities: Standard
Other: Guideline

1.11 Metadata

All geospatial land record databases, and their associated attribute databases should be documented with Federal Geographic Data Committee (FGDC) compliant metadata outlining how the data was

derived, attribute field definitions and values, map projections, appropriate map scale, contact information, access and use restrictions, etc.

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

1.11.1 NebraskaMAP Metadata

The NebraskaMAP (http://NebraskaMAP.gov) is a state sponsored GIS web-based portal for finding and accessing a wide variety of GIS/geospatial data related to the geographic area of Nebraska. Many of the NebraskaMAP functions required metadata. All developers of Nebraska-related GIS data are encouraged to use the site to either upload existing metadata and/or use the online tools available on the site to create metadata for your GIS/geospatial land record information and mapping. Before metadata can be either created or uploaded on the site, a brief user registration is necessary.

State Agencies: Guideline
State Funded Entities: Guideline
Other: Guideline

1.12 Attribute Data

To provide the foundation necessary for a wide variety of local government applications, non-graphic, attribute data should be organized within the GIS/LIS, which describes individual property parcels relative to their basic parcel characteristics, tenure, value, history, buildings and units within the parcel, and tax status. In most cases, much of this attribute data will already exist in separate databases within a variety of local agencies and should be referenced to the graphic property parcel via the unique PID. To meet a range of state and regional applications that require property parcel information, the following types of property parcel data should be maintained and be available in a manner that allows it to be harvested, translated, and integrated into a statewide property parcel attribute dataset. These attribute values may be maintained in one or more separate relational databases that are referenced by a unique PID and not directly integrated into a GIS.

PID#: Parcel identifier (county FIPS code plus local government PID)
Situs Address: Address of parcel (may be multiple fields)
Owner Address: Address of property owner (may be multiple fields)
Township: Township #
Section: Section #
Range: Range #
Range Direction: East or West
Legal Description: Narrative legal description of parcel
Assessed Value: Total assessed value of property (land and improvements)
Land Value: Assessed value of land
Area (Deeded): Area of parcel according to the deed
Property Class: (Res, Ag, Com, Rec., Ind.)
Property Sub-class : i.e., Ag (Dryland, Irrigated, Grassland/Pasture, Waste)
Ownership type: Federal, State, County, Private, Tribal, Exempt, Other and Unknown

Tax District: County ID plus Tax Dist. #
School District : State number definition
Landuse : Actual landuse with NPAT defined general categories
Property Parcel Type: NPAT defined categories: (i.e., Single Family, Multi-Family, Commercial, Industrial, Agriculture, Recreational, Mineral Interest-Nonproducing, Mineral Interest-Producing, State Assessed, or Exempt)
Status : NPAT defined categories: (Improved, Unimproved, or IOLL)
Location: NPAT defined: (Urban, Sub-urban, Rural)
City Size: 1st class, 2nd class, primary, metro, or village
Source Document: Sales/transfer reference or document (book & page & date)
Sales Date: Most recent sales/transfer date
Sales Value: Most recent sales value

State Agencies: Standard
State Funded Entities: Standard
Other: Standard

2. Purpose and Objectives

The purpose of these standards and guidelines is to help realize the maximum long-term return on and overall utility of the public's investment in the modernization of how Nebraska's land records are maintained and distributed.

2.1 Background

Land records and land ownership records are public records that are used by wide cross-section of our society and its institutions. Ready access to current and accurate land records is critical to our state's overall economy and the efficient functioning of many of its public and private institutions.

Historically land records have been maintained on paper records and paper maps. This made it very difficult and costly to update and keep current records and maps in areas where there was significant turnover in property ownership. Paper records and maps also made it difficult to share land record information outside of the physical office where they were maintained. Paper records and maps also made it difficult to conduct analyses of broader land ownership and land valuation patterns. Computerization in general, and GIS/geospatial technologies in particular, have revolutionized how land and land ownership records can be maintained, analyzed, shared, and distributed.

Modern computerized land records and maps make it relatively easy to update and keep current land records and maps. Computerization and GIS/geospatial technologies now routinely enable easy, reliable access to land records and maps via the Internet to a wide variety of users. Land records in computerized relational databases and GIS parcel maps have provided a wide array of new information management tools that can be used to integrate land records with other data and analyze and display land ownership, land valuation and other broader land-related patterns. Among other uses, these tools help ensure that all property is on the tax rolls and that the property is taxed equally.

Modern computerized land records and maps can provide a wide array of potential benefits to a wide array of users. However, to realize many of these benefits, it is important that when these databases and maps are originally developed they follow a minimal set of standards and guidelines that support

this potential broad array of applications and benefits. In many instances, it is not this broader array of potential uses that is the immediate stimulus, which causes a local or state agency to undertake a modernization of its land records and maps. Therefore, these standards and guidelines serve the function of raising the awareness of these potential future applications and the related need to incorporate minimal standards beyond those needed for immediate applications.

These standards and guidelines are intended to help ensure that modernized land records are developed on a solid technical foundation. A foundation, which will enable both the original developing agency, and other interested entities, to build on this initial investment and maintain and enhance the data and enable it to be utilized for multi-purposes by multiple users. These standards and guidelines are also intended to facilitate partnerships between local, state, and federal entities to support the development and maintenance of modernized land records.

2.2 Objectives

These standards and guidelines to guide the modernization of land records in Nebraska have the following objectives:

2.2.1

Provide guidance to state and local officials as they work, either in-house or with private contractors, to develop and/or acquire computerized, geospatial data related to land records and maps and thereby increase the likelihood that the data acquired and/or developed will be suitable for the range of intended applications and likely future applications.

2.2.2

Improve public policy development and implementation by helping to make land records more current and readily accessible and by making available to land record management applications the wide range of analytical tools available through GIS/geospatial technology.

2.2.3

Enhance coordination and program management across jurisdictional boundaries by insuring that modernized land records and maps can be readily integrated across jurisdictional boundaries for regional applications (e.g., school districts, NRDs, emergency response, etc.) or statewide applications.

2.2.4

Save public resources by facilitating the sharing of computerized land records among public agencies or sub-divisions of agencies by incorporating data standards and following guidelines which will make it more likely that the computerized land records developed by one entity will also be suitable to serve the multiple needs of other entities and thereby avoid the costly duplication of developing and maintaining similar land records.

2.2.5

Make land records and land ownership maps more readily accessible to the wide range of potential users.

2.2.6

Facilitate harmonious, trans-agency public policy decision-making and implementation by enabling multiple agencies and levels of government to access and appropriately use common geospatial datasets and thereby make it more likely that intersecting public policy decisions, across levels of government, will be based on the same information.

2.2.7

Lay the foundation for facilitating intergovernmental partnership to the modernization of land records by defining standards and guidelines that increase the likelihood that computerized land records will meet the needs of multiple users.

3. Definitions

Attribute Data : Properties and characteristics of property parcel or other spatial data entities.

Datum: A Geodetic Reference System is the true technical name for a datum. A datum is a combination of an ellipsoid, which specifies the size and shape of the earth, and a base point from which the latitude and longitude of all other points are referenced.

Entity: Any object about which an organization chooses to collect data.

Geodetic Control: A set of surveyed monuments used to define a spatial reference system and used to register map sheets and transform coordinates for a particular project.

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

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

Global Positioning System (GPS): GPS is a method for identifying locations on earth using triangulation calculations of satellite positions. Originally created by the United States Military, it has since found numerous commercial applications.

Land Information System (LIS): A special type of GIS that manages and analyzes data related to land ownership (e.g., tax parcels, urban infrastructure, property assessment). A GIS used for municipal or county level applications is typically structured as an LIS.

Map Scale: The scale of a map is the ratio between a distance on the map and the corresponding distance on the earth, with the distance on the map typically expressed as 1. Thus, a scale of 1:100,000 means 1 inch on the map equals 100,000 inches (approximately 1.6 miles) on the earth. Large scale maps depict a small area and show more detail. Small scale maps depict a large area and show less detail.

Metadata: Data describing a GIS database or data set including, but not limited to, a description of a data transfer medium-, format, and contents, source lineage data, and any other applicable data processing algorithms or procedures.

Monumentation of PLSS Corners: Monumentation in surveying refers to the practice of marking known horizontal and vertical control points with permanent structures such as concrete pedestals and metal plaques. Once surveyed and marked, these monuments can be used for further surveying and for the alignment of land-parcel boundaries and infrastructure.

National Spatial Reference System (NSRS): A consistent national coordinate system that defines latitude, longitude, height, scale, gravity, and orientation throughout the Nation, and how these values change with time. Consequently, it ties spatial data to geo-referenced positions.

Nebraska Plane Coordinate System: Nebraska Plane Coordinate System means the system of plane coordinates for designating the geographic position of points on the surface of the earth, within the State of Nebraska, which have been established by the National Ocean Service/National Geodetic Survey, or its successors. The Nebraska Plane Coordinate System is a Lambert conformal conic projection of the North American Datum of 1983, having standard parallels at north latitudes 40 degrees 00 minutes and 43 degrees 00 minutes along which parallels the scale shall be exact. The origin of coordinates is at the intersection of the meridian 100 degrees 00 minutes west of Greenwich and the parallel 39 degrees 50 minutes north latitude. This origin is given the coordinates. N = 0 meters and E = 500,000 meters. (Neb. Rev. Stat. § 76-2502)

Orthophoto: An aerial photo that has been corrected to eliminate the effects of camera tilt and relief displacement. The ground geometry is recreated as it would appear from directly above each and every point. Digital orthophotos can be created by scanning the original photograph and applying a process called differential rectification to each pixel in the image. In creating digital orthophotos, it is also possible to remove the effects of tangential displacement.

Parcel Identifier (PID): A unique number identifying a specific property on the assessment and tax rolls and used as a cross reference between graphic/mapping data and tabular attribute data.

Projection: A system to portray all or part of the earth, which is an irregular sphere, on a planar, or flat surface.

Public Land Survey System (PLSS): The Public Land Survey System (PLSS) is a way of subdividing and describing land in the United States. All lands in the public domain are subject to subdivision by this rectangular system of surveys (townships, ranges, sections, quarter-sections, etc.), which is regulated by the U.S. Department of the Interior, Bureau of Land Management.

Shapefile: A Shapefile is an ESRI digital vector (non-topological) storage format for storing geometric location and associated attribute information that can be generated by a wide variety of GIS software packages.

Spatial Accuracy: The accuracy of a map in representing the geographic location of an object relative to its true location on the surface of the Earth based on geographic coordinates.

4. Applicability

4.1 State Government Agencies

State agencies that have the primary responsibility for maintaining land ownership records and property parcel maps for a particular jurisdiction(s) or geographic area (e.g. Nebraska Dept. of Property

Assessment and Taxation for counties for which it has assumed the primary assessment role) are required to comply with those sub-sections identified as a "Standard" for "State Agencies" in Section 1. Those state agencies with oversight responsibilities in this area are required to ensure that their oversight guidelines, rules, and regulations are consistent with these standards.

4.2 State Funded Entities

Entities that are not State agencies but receive State funding, directly or indirectly, for property parcel mapping and/or property tax assessment and have the primary responsibility for maintaining property parcel maps for a particular jurisdiction or geographic area are required to comply with those sub-sections identified as a "Standard" for "State Funded Entities" in Section 1.

4.3 Other

Other entities, such as local government agencies (e.g. County Assessor, County Register of Deeds, municipalities) that have the primary responsibility for developing and maintaining land ownership records and property parcel maps are required to comply with those sub-sections identified as a "Standard" for "Other" in Section 1.

5. Responsibility

5.1 NITC

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (Neb. Rev. Stat. § 86-516(6))

5.2 State Agencies

The Nebraska Department of Property Assessment and Taxation will be responsible for ensuring that its rules and regulations relative to land ownership records and property parcel (tax) mapping include those subsections in Section 1 that are identified as a "Standard" for "Other" and are consistent overall with those standards.

5.3 Granting Agencies and Entities

State granting or fund disbursement entities or agencies will be responsible for ensuring that these standards are included in requirements and regulations related to fund disbursements as they relate to land (property parcel) records or property parcel mapping.

5.4 Other

Local government agencies that have the primary responsibility for land ownership records and property parcel mapping will be responsible for ensuring that those sub-sections defined for "Other" as a "Standard" in Section 1 will be incorporated in land record modernization and geospatial data development efforts and contracts.

3-203. Lidar standard.

The commission adopts by reference the most recent version of the Lidar Base Specification (LBS) standards released by the U.S. Geological Survey (USGS) [https://www.usgs.gov/ngp-standards-and-specifications/lidar-base-specification-online] for elevation acquisition using lidar.

--

History: Adopted on October 28, 2014. Amended on November 10, 2022.
URL: https://nitc.nebraska.gov/standards/3-203.pdf

3-204. Imagery standard.

[Section 3-204 appears after this cover page in a legacy format.]

--

History: Adopted on October 28, 2014. Amended on July 25, 2019.
URL: https://nitc.nebraska.gov/standards/3-204.pdf

1.0 Standard

1.1 Description

This standard provides requirements necessary for the creation, development, delivery, and maintenance of aerial imagery acquisition to support a statewide Nebraska Imagery Program. There are multiple uses for imagery and data acquisition is expensive and requires preplanning. These standards are set at a minimum such that the majority of applications and needs are met across the state.

It is important to collect ortho-rectified imagery so that ground features can be measured and other data layers can be created from the data source which has a strong relationship to ground control. The data required for ortho-rectification include orientation parameters for the source image(s) and a digital elevation model (DEM) of the geographic area to be covered by the imagery. Ortho-rectification corrects for tip and tilt of the aircraft and displacement in the photograph caused by changes in the ground elevation.

Generally, the development of ortho-rectified imagery requires the acquisition of overlapping photography of the same geography and some combination of surveyed ground control and airborne (Global Positioning System) GPS collection at the time of photography. A photogrammetrist performs image correlation techniques and aero-triangulation on the resulting block of photographs to establish the orientation parameters of the individual image. Using a most recent DEM source or new LiDAR DEM provides the base for which the new imagery is rectified. These operations make ortho-rectified imagery more expensive than uncorrected aerial photography, but also make it far more accurate and useful.

Ultimately, accurate base maps can be derived from ortho-rectified imagery because the image has been geometrically corrected such that the scale is uniform. Streets and roads, curbs, manholes, water edge, tree inventories, fire hydrants, and numerous other features can be accurately mapped from the imagery. This also allows for accurate measurements of features and relationships between features, directly on the photograph.

The standard provides a consistent structure for data producers and users to ensure compatibility of datasets within the same framework layer and when used between other Nebraska Spatial Data Infrastructure (NESDI) framework layers such as survey and geodetic control and LiDAR.

This standard does not restrict or limit additional buy-ups of imagery data and services. These standards are meant to be a minimum set of standards and are subject to be updated based on technology enhancements, necessary workflow changes, and other data requirements. Other imagery data that is available at specifications that are above the minimum standard will be evaluated on a case-by-case basis.

The standard is not intended to be a substitute for an implementation design. These standards can be used at local, state and federal level to ensure interdisciplinary compatibility and interoperability with other framework layers. These standards integrate with existing standards such as the American Society for Photogrammetry and Remote Sensing (ASPRS) and other NITC related standards.

1.2 Acquisition and Processing

1.2.1 Flight Specifications

Proper planning and pre-flight requirements are necessary steps prior to acquiring imagery. This includes consideration of temporal requirements, proper flight planning, and ensuring that the characteristics of the sensors used in acquisition of imagery meet these requirements.

1.2.1.1 Temporal Requirements

Time of Day: Imagery will need to be acquired during minimal shadow conditions. Image acquisition shall occur when the sun angle is equal to or greater than 30-degrees.

Time of Year: All imagery shall be collected during the late-Winter / early-Spring flying season during leaf-off conditions for deciduous vegetation in Nebraska. Exceptions can be made on a case-by-case basis for certain applications requiring leaf-on imagery.

1.2.1.2 Flight Plans

Flight line orientation for all flight lines shall be in a cardinal direction, either north-south or east-west orientation when feasible. Flight plans must be approved prior to imagery acquisition. Information will need to be provided including project boundary, flight line numbers, flight line locations, and recommended ground control locations. If a frame sensor is used, exposure numbers should be included as well. For quality assurance purposes, the vendor shall submit copies of flight logs as part of the preliminary imagery deliverables.

1.2.1.3 Sensor Characteristics

The entire mission in a given year must be flown with sensors having the same specifications. The system shall use square pixels (ground footprint) at all times during processing. The technique of using aggregated detectors resulting in a rectangular pixel before blending with other channels shall not be used. The aerial camera shall be a precision aerial mapping camera equipped with a low distortion, high resolution lens. Camera characteristics shall be such that the aerial photographs taken can be satisfactorily used with the vendor’s proposed photogrammetric compilation equipment and environment. Calibration certificates for all systems to be used for acquisition will need to be provided.

1.2.1.4 Sun Angle

The images should be acquired only during the portion of the day when the sun angle exceeds the minimum of 30 degrees. To expedite acquisition within the photo periods, different sun angles may be permitted, provided the image does not have excessive shadows that preclude interpretation and data collection.

1.2.2 Ground Control

Ground control needs to be established of sufficient density and accuracy to meet the accuracy requirements of the ortho-rectified imagery.

Ground controls points used for aerial triangulation should be at least three times better than the expected accuracy of aerial triangulation solution. For example, in order to produce an orthophoto with an $RMSE_r$ of 15cm, the aerotriangulation results should have an $RMSE_{xyz}$ of 7.5 cm and the ground control used should have $RMSE_{xyz}$ of 2.5 cm. The control shall be sufficient to supplement the airborne GPS and Inertial Measurement Unit (IMU) in order to meet the required product accuracies.

For all photogrammetric data sets, the accuracy of the aerial triangulation or INS orientation (if used for direct orientation of the camera) should be at least twice the accuracy of derived products, as evaluated at higher accuracy check points using stereo photogrammetric measurements. Ground control and blind quality control points shall be required for softcopy aero- triangulation and ortho-photography generation to meet the accuracies specified.

Both ground control and quality control points will be based on a county or project area size depending on the scope of the project to be flown. The control diagrams, indicating the anticipated vertical and horizontal accuracies, will be reviewed before imagery collection begins.

The availability and/or quality of any existing ground control will need to be determined prior to flight acquisition. Any new control established for a project area will be delivered including sketches, pictures of control locations, and an ISO 19115 compliant metadata file. Those responsible for evaluating ground control should not assume that control exists, but it could be beneficial to use existing control if possible.

1.2.2.1 Global Positioning Systems (GPS)

If additional ground control needs to be established, the ground control shall be established with survey grade instrumentation. The GPS control survey needs to be conducted with a licensed surveyor or engineer representing the quality control process. A plan will need to be provided to recommend and coordinate the placement of ground control target locations of a sufficient quantity and size to control the photogrammetric accuracy specifications. Any new ground control established must be tied to the Nebraska NAD83 horizontal datum. All ground control points must be documented as such so that they are easily located by other surveyors throughout the duration of the project.

The horizontal root-mean-square error (RMSE) of the airborne GPS control data shall not exceed 0.2m. The vertical RMSE of the Airborne GPS control shall not exceed 0.3m.

1.2.2.2 Digital Elevation Model (DEM)

Elevation data is necessary for ortho-rectifying imagery. A digital elevation model (DEM) shall be developed at a density level necessary to support the imagery ortho-rectification process.

The elevation data may come from various sources to build a DEM. Elevation data may be derived from LiDAR, photogrammetry or autocorrelation as long as it provides sufficient accuracy and precision to support imagery horizontal accuracy requirements. Preference is to use LiDAR where it is available in the state. The DEM shall consist of points spaced at regular intervals along a grid, points of significant high or low elevations, and ortho-photography specific breaklines at all significant terrain breaks. In cases, where breaklines are not available suitable breaklines will need to be created to support an elevation dataset. It is not necessary to capture break lines at all curbs, ditches, stream banks, or other similar minor terrain breaks. The DEM shall be free of artifacts and data voids. The vertical accuracy of the DEMs developed to support production of the ortho-rectified imagery shall be sufficient to guarantee the horizontal accuracy specified in these standards.

The U.S. Geological Survey's National Elevation Dataset (NED) has 1/3 arc-second digital elevation model (DEM) data. Unless an area is very flat, the NED should not be used for less than 12 inch resolution data where higher accuracy is required.

There is no guarantee that the available DEM will be adequate to meet the final product accuracy specifications. An updated DEM is necessary in order to support the ortho-rectification production specifications and accuracy standards. This may require the acquisition of LiDAR to complete this task.

Updates to the existing DEM need only support the ortho-rectification process and are not required to support contour modeling or other applications. The DEM data is not to be stored as a record (Z component) for each pixel of the ortho-rectified image.

1.2.3 Ground (Spatial) Resolution

The final imagery output needs to be at a minimum of 12 inch ground sample distance (GSD). GSD is referred to as spatial resolution. This orthoimagery should meet ASPRS Class II horizontal accuracy standards for digital Orthoimagery and 1:2,400 Digital Planimetric Data.

A scale that equivalents higher resolutions (i.e., 6 inch) can be acquired as long as it meets the respective scales and horizontal accuracies associated to its desired spatial resolution found in section 1.2.6.

1.2.4 Spectral Resolution

Imagery will need to be provided in four primary spectral bands at 12 bit including Red (R), Green (G) and Blue (B) and Infrared (IR). All color imagery shall be the equivalent of natural true color, to include 256 levels of value for each color band for RGB. The sensor or camera shall save the bands in the following order: Red, Green, Blue, and infrared.

1.2.5 Radiometric Resolution

The digital aerial images shall be clear and sharp in detail and of high radiometric quality. The sensor shall capture the images in an uncompressed “lossless” image format. The

sensor shall, at minimum, utilize 12 bits per pixel radiometric resolution. Up-sampling from a lower bit depth to a higher bit depth is not allowed (e.g. resampling 8 bit data to 12 bit data). Color balancing shall result in colors which appear natural to a human observer. Image contract and brightness shall be adjusted to minimize perceptible differences within and between adjacent images.

1.2.6 Horizontal Accuracy

Horizontal accuracy assessment will be required for both in absolute and relative conditions. The pixel size of the final digital orthoimagery is being considered for this assessment not the GSD of the raw image that is used to establish the horizontal accuracy class.

- Absolute requires the use of ground control points for testing purposes. These points, found in the image and coordinates from the ortho-rectified image, are compared to the published coordinates.
- Relative horizontal accuracy assessment involves the visual inspection of adjacent images for edge matching, and the comparison of the ortho-rectified image to planimetric data. The relative displacement would be quantified.
- Recommendations for achieving the horizontal accuracy assessment shall be provided prior to acquisition including the number of and the distribution of check points within the project. QC points should be included in flight and control layout prior to acquisition.

The final imagery output needs to meet horizontal accuracy requirements established by ASPRS Class II accuracy for a minimum 12 inch GSD as defined in the following table.

Horizontal Data Accuracy Class	**RMSEx and RMSEy**	**Orthophoto Mosaic Seamline Maximum Mismatch**	**Aerial Triangulation or INS-based RMSEx RMSEy and RMSEz**
I	Pixel size x 1.0	Pixel size x 2.0	Pixel size x 0.5
II	Pixel size x 2.0	Pixel size x 4.0	Pixel size x 1.0
III	Pixel size x 3.0	Pixel size x 6.0	Pixel size x 1.5
…			
N	Pixel size x N	Pixel size x 2N	Pixel size x 0.5N

When producing digital orthoimagery, the GSD as acquired by the sensor (and as computed at mean average terrain) should not be more than 95% of the final orthoimagery pixel size. In extremely steep terrain, additional consideration may need to be given to the variation of the GSD across low lying areas in order to ensure that the variation in GSD across the entire image does not significantly exceed the target pixel size.

The following table serves as a guide for three common ASPRS horizontal accuracy standards for planimetric maps intended for use at common map scales.

Orthophoto Pixel Size	Horizontal Data Accuracy Class	RMSEx or RMSEy (cm)	RMSEr (cm)	Orthophoto Mosaic Seamline Maximum Mismatch (cm)	Horizontal Accuracy at the 95% Confidence Level (cm)
7.5-cm (~3 in)	I	7.5	10.6	15.0	18.4
	II	15.0	21.2	30.0	36.7
	III	22.5	31.8	45.0	55.1
15-cm (~6 in)	I	15.0	21.2	30.0	36.7
	II	30.0	42.4	60.0	73.4
	III	45.0	63.6	90.0	110.1
30-cm (~12 in)	I	30.0	42.4	60.0	73.4
	II	60.0	84.9	120.0	146.9
	III	90.0	127.3	180.0	220.3

1.2.7 Projection and Datum

Imagery for the project will be referenced to the North American Datum of 1983 (NAD83) using the 2007 HARN adjustment, and the North American Vertical Datum of 1988 (NAVD 88) with the latest ellipsoid and Geoid09 adjustments. Imagery shall be oriented to the appropriate Nebraska State Plane using U.S. Feet.

1.2.8 Pixel Clarity

Pixel clarity is defined by pixel size and relation to the ground sample distance (GSD) of the specified pixel size. It is not recommended to resample from a coarser image to obtain a finer image resolution. The image can be resampled from a sharper image for a coarser image (i.e., obtaining an 18-inch pixel resolution from one foot).

1.2.9 Image Quality

Images shall be tonally balanced and image mosaics shall be uniform in contrast without abrupt variations between image tiles. Imagery shall be free of blemishes, and artifacts that obscure ground feature detail. Pixel resolution shall not be degraded by excessive image smear. Imagery shall have a tonal range that prevents the clipping of highlights or shadow detail from the image.

1.3.0 Environmental Conditions and Obstructions

To the extent possible, no clouds, snow, fog, haze, smoke, or other ground obscuring conditions shall be present at the time of the flights. Ground conditions are free of snow, flooding and excessive soil moisture. Streams and rivers should be within their normal banks, unless otherwise negotiated. Spectral reflectance from water must be minimized and should not obscure shoreline features. In no case will the maximum cloud cover exceed 5% per image.

1.3.1 Edge Effects

Sufficient end and side laps need to be taken into consideration to prevent any gaps in coverage and to provide all necessary coverage for accurate ortho-rectification and visual

interpretation. The crab shall not be in excess of three (3) degrees; and, tilt of the camera from verticality at the instant of exposure shall not exceed three (3) degrees.

1.3.2 Building Lean

Additional supplemental flight lines should be acquired in areas of tall buildings to limit building lean in city blocks. Recommended supplemental flight lines should be provided in preliminary flight layout for prior review and approval.

1.3 Data Format

The data format provided will need to be in uncompressed tiles in a GeoTIFF format that can be interpreted by commercial imagery and GIS software. Tile schemes will need to be provided at 5,000 feet x 5,000 feet. If mosaic imagery is suggested, the area of interest (AOI) or collection area (i.e., county, quadrangle, city, etc) will need to be provided. The mosaic imagery need to be compressed and provided as JPEG2000 with a compression ratio of 20:1.

1.4 Maintenance

Entities responsible for data acquisition and deliverables will need to assure data meets standards and are updated and maintained in a timely manner. After spatial and attribute updates and/or modifications are performed to the data it shall be submitted to the appropriate entity(s) responsible for performing quality control and maintenance of the data acquisition.

Maintenance of elevation data determines the suitability to support the greatest range of applications. Many projects require up-to-date, accurate and consistent elevation data and maintenance of this data is necessary to provide the maximum return on investment.

1.4.1 Reporting Errors and Handling Updates

The reporting of errors need to be directed to the appropriate entity in a timely manner. Updated spatial and attribute information in the data will also need to be redistributed. The date field in the metadata when the last record was modified will also need to be updated to ensure proper records management and communication with others in the workflow.

1.5 Quality Control

A quality control process is required by a third-party to ensure the delivery of an image product that satisfies the requirements as defined by these standards. The quality of imagery acquisition is evaluated based on the overall functional correctness and completeness of the technical requirements that also include a horizontal accuracy test. In the event that data does not meet specific requirements of these standards, the imagery will be rejected and the vendor will be required to either reacquire or re-process data appropriately to meet these standards.

1.5.1 Horizontal Accuracy Test

A number of check points will need to be collected within each area of interest to verify the horizontal accuracy of the ortho-rectified production process. The check points must be completely independent of ground control used during aero-triangulation and data

production. The recommended number of check points based on the size of area will follow ASPRS guidelines.

1.5.2 Re-Flights

A plan for re-flights of areas will need to be provided in the event of image rejection during the quality control process, or where original imagery could not be collected because weather or ground cover conditions, or other factors outside the control of the vendor precluded collection at the scheduled time of the flyover. Mechanical or technical problems shall not be considered a legitimate reason for non-collection.

1.6 Integration with other Standards

1.6.1 Street Centerline Standards (NITC 3-205)

These minimum standards for imagery acquisition are designed to ensure the acquisition of imagery sufficient to meet the requirements for digitizing street centerlines as required in the Street Centerline Standards NITC 3-205.

1.6.2 Address Standards (NITC 3-206)

These minimum standards for imagery acquisition are designed to ensure the acquisition of imagery sufficient to meet the requirements for digitizing street centerlines as required in the Address Standards NITC 3-206.

1.7 Metadata

Complete and comprehensive metadata is required for the acquired imagery. The metadata will require detailing the characteristics and quality of submitted imagery files. Information needs to be provided to allow the user sufficient information so they can determine the data's intended purpose as well as how to access the data. The metadata requires a process description summarizing collection parameters such as: contact information, data source, scale, accuracy, projection, use restrictions, and imagery acquisition dates. The process description will also need to be included to describe methodology towards the deliverable products.

1.7.1 Federal Metadata

The ISO 19115:2003(E) North American Profile (NAP) Metadata Standards should be used when feasible and in every effort possible to assure high quality rigorous standards. Metadata will need to be supplied for each tile and be provided in an XML format. All imagery datasets, and their associated attribute databases should be documented with ISO 19115 compliant metadata. Supplemental metadata information includes the following: (1) tested horizontal accuracy statement, (2) lineage, including, but not limited to: flight height, photo acquisition dates (and re-flights if any), overlap, sidelap, number of flight lines, number of exposures, direction of flight lines, control, resolution, tiling scheme, file sizes, description of the process used to create digital orthophotos, source of DEM, and (3) spatial reference information: projection, ellipsoid, horizontal and vertical datum, and horizontal and vertical units.

1.7.2 State Metadata

These standards need to apply to Nebraska's metadata standards located within NITC 3-201 Geospatial Metadata Standard. All metadata from imagery files will need to be registered through the metadata portal at NebraskaMAP (http://NebraskaMAP.gov). All developers of Nebraska-related geospatial data are encouraged to use the site to either

upload existing metadata and/or use the online tools available on the site to create the metadata for imagery.

2.0 Purpose and Objectives

2.1 Purpose

The purpose of this standard is to provide the necessary requirements for the creation, development, delivery, and maintenance of aerial imagery data and services to support the Nebraska Spatial Data Infrastructure (NESDI). These standards will help ensure that imagery acquisition is consistent, accurate, publicly accessible, and cost-effective.

2.2 Objectives

These standards will guide the statewide imagery program having the following objectives:

2.2.1 Provide guidance and necessary workflows to state and local officials as they work, either in-house or with private vendors, to create, develop and maintain aerial imagery data and services. This can increase the likelihood that the data created will be suitable for the range of intended applications and likely future applications. The maintenance of aerial imagery data is necessary for the data to be current and accurate.

2.2.2 Enhance coordination and program management across jurisdictional boundaries by insuring that aerial imagery data can be horizontally integrated across jurisdictional and/or project boundaries, and other framework data layers for regional or statewide applications.

2.2.3 Save public resources by facilitating the sharing of aerial imagery data among public agencies or sub-divisions of agencies by incorporating data standards and following guidelines. Data that is developed by one entity can be done in a way that is suitable to serve the multiple needs of other entities. This avoids the costly duplication of developing and maintaining similar data in the state.

2.2.4 Make aerial imagery data current and readily accessible to the wide range of potential users through NebraskaMAP and other necessary resources.

2.2.5 Facilitate harmonious, trans-agency and public policy decision-making and implementation by enabling multiple agencies and levels of government to access and appropriately use current aerial imagery data. This can make it more likely that intersecting public policy decisions, across levels of government, will be based on the same information.

2.2.6 Lay the foundation for facilitating intergovernmental partnerships for the acquisition and development of high-quality aerial imagery data by defining standards that increase the likelihood that this data will meet the needs of multiple users.

2.2.7 Establish and promote the integration and interrelationships of aerial imagery data with related NESDI framework layers through geometric placement and attributes.

3.0 Definitions

Accuracy

Absolute - A measure of the location of features on a map compared to their true position on the face of the earth.

Relative - A measure of the accuracy of individual features on a map when compared to other features on the same map.

Band - A range of wavelengths of electromagnetic radiation.

Check Point – One of the surveyed points in the sample used to estimate the positional accuracy of the data set against an independent source of higher accuracy.

Confidence Level – The percentage of points within a data set that are estimated to meet the stated accuracy; i.e., accuracy reported at the 95% confidence level means that 95% of the positions in the data set will have an error with respect to true ground position that are equal to or smaller than the reported accuracy value.

Datum – A set of values used to define a specific geodetic system.

Digital Elevation Model - A digital cartographic representation of the elevation of the land at regularly spaced intervals in x and y directions, using z-values referenced to a common vertical datum. A DEM also assumes bare-earth terrain, void of vegetation and manmade features. The USGS DEMs archived in the National Elevation Dataset (NED) have different formats based on 1-arc-second, 1/3-arc-second, and 1/9-arc-second grid spacing.

Forward Lap or End Lap - The extent to which sequential exposures in a flight line overlap

Ground Sample Distance (GSD) – The linear dimension of a sample pixel's footprint on the ground. Within these standards GSD is used when referring to the collection GSD of the raw image, assuming near-vertical imagery. The actual GSD of each pixel is not uniform throughout the raw image and varies significantly with terrain height and other factors. The GSD is assumed to be the value computed using the camera focal length and camera height above average mean terrain.

Ground (spatial) resolution or pixel size – As used within these standards, pixel size is the ground size of a pixel in a digital ortho-rectified imagery product, after all rectifications and resampling procedures.

Horizontal Accuracy - The horizontal component of the positional accuracy of a data set with respect to a horizontal datum, defined at the 95% confidence level.

Image Correlation – Directly comparing hardcopy or softcopy images, or patches of pixels on conjugate digital images, or indirectly comparing information derived from the stereo images, to determine that points on stereo images (viewed from different perspectives) represent the same points on the imaged surface. Automated image correlation is a computerized technique to match the similarities of pixels in one digital image with comparable pixels in its digital stereo image in order to automate or semi-automate photogrammetric compilation. Automated image correlation provides an efficient method for generating DEMs photogrammetrically, but automated correlation normally results in Digital Surface Models (DSMs) instead of DEMs because such correlation generates elevations of rooftops, treetops and other surface features as imaged on the stereo photographs.

Inertial Measurement Unit (IMU) - An electronic device that measures and reports velocity, orientation, and gravitational forces, using a combination of accelerometers and gyroscopes, sometimes also magnetometers. IMUs work to detect changes in pitch, roll, and yaw of an aircraft. IMUs are typically used to maneuver aircraft, including unmanned aerial vehicles (UAVs), among many others, and spacecraft, including satellites and landers.

Leaf-Off / Leaf-On - Leaf-off and leaf-on refer to the presence or lack of the foliage of woody species. Leaf-off means that there is no foliage or a reduced amount of foliage on the tree or shrub species. Leaf-on imagery means that there is foliage on the tree or shrub species (or the species of interest). Sometimes it is beneficial to have leaf-off imagery so that you can see ground features more distinctly. This is helpful for mapping features such as buildings and roads, which may be obscured by tree foliage during the growing season. Leaf-off imagery is also used in forestry applications because the lack of leaves on some trees facilitates the classification of tree types. There are times when you might want leaf-on imagery, especially if the tree or shrub species has a distinctive spectral reflectance that can be distinguished from other vegetation. Leaf-on imagery is also used in agricultural applications to measure the quantity and health of crops. Many woody species may have similar spectral reflectance or structure that may benefit from either a leaf-off or leaf-on flyover.

Map or Cartographic Scale - The relationship between a given distance on the ground and the corresponding distance on a photograph or image. Scale is expressed in at least two different ways. Both are ratios. In the first, commonly used measuring systems are compared; for example 1" = 200' (one inch on the map equals 200 feet on the earth). In the second, the map unit is arbitrary; for example, 1:200 means that one of anything (an inch, a foot, a centimeter, etc.) on the map equals 200 of that same unit on the earth. (1"=200' is the same scale as 1:2400). Scale is presented in several ways: as a bar at the bottom of the map, as a ratio (1:200), or as an equation (1"=200').

Nebraska Spatial Data Infrastructure (NESDI) - A framework of geospatial data layers that have multiple applications, used by a vast majority of stakeholders, meet quality standards and have data stewards to maintain and improve the data on an ongoing basis. These layers are also consistent with the Federal National Spatial Data Infrastructure (NSDI).

Ortho-rectification - The process by which a photograph is prepared from a perspective photograph by removing displacements of points caused by tilt, relief and perspective.

Planimetric - Data about non topographic features on the earth surface that are represented only by their horizontal position.

Projection – A map projection flattens the earth, allowing for locations to be systematically assigned new positions so that a curved surface can be represented on a flat map.

Resolution – The smallest unit a sensor can detect or the smallest unit an ortho-rectified image depicts. The degree of fineness to which a measurement can be made.

Root Mean Square Error (RMSE) – The square root of the average of the set of squared differences between data set coordinate values and coordinate values from an independent source of higher accuracy for identical points.

RMSEr – The horizontal linear RMSE in the radial direction that includes both x- and y-coordinate errors.

RMSEx – The horizontal linear RMSE in the X direction (easting).

RMSEy - The horizontal linear RMSE in the Y direction (northing).

RMSEz - The vertical linear RMSE in the Z direction (elevation).

Side Lap **-** The extent to which the exposures of adjacent flight lines overlap, typical side lap for a block of aerial photography is 30%.

State Plane Coordinate System - The State Plane Coordinate System is a set of 124 geographic zones or coordinate systems designed for specific regions of the United States. It uses a simple Cartesian coordinate system to specify locations rather than a more complex spherical coordinate system (the geographic coordinate system of latitude and longitude). By thus ignoring the curvature of the Earth, "plane surveying" methods can be used, speeding up and simplifying calculations. The system is highly accurate within each zone (error less than 1:10,000). Outside a specific state plane zone, accuracy rapidly declines, thus the system is not useful for regional or national mapping.

4.0 Applicability

4.1 State Government Agencies

State agencies that have the primary responsibility for developing and maintaining aerial imagery data for a particular jurisdiction(s) or geographic area (e.g. for counties for which it has assumed the primary role) are required to comply with the standards as described in Section 1. Those state agencies with oversight responsibilities in this area are required to ensure that their oversight guidelines, rules, and regulations are consistent with these standards. The Nebraska Department of Roads has other imagery acquisition requirements for wetland and reconnaissance projects. They will continue to adhere to their independent photogrammetry requirements as suggested in the NDOR On-Call Digital Aerial Photography, Photogrammetric and Airborne LiDAR Services.

4.2 State Funded Entities

Entities that are not State agencies but receive State funding, directly or indirectly, for aerial imagery development and maintenance for a particular jurisdiction or geographic area are required to comply with the standards as described in Section 1.

4.3 Other

Other entities, such as city and local government agencies (e.g. County Engineer, assessors, and municipalities) that receive state funds have the primary responsibility for developing and maintaining aerial imagery data are required to comply with the standards as described in Section 1.

5.0 Responsibility

5.1 NITC

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. Neb. Rev. Stat. § 86-516(6)

5.2 State Agencies

The State of Nebraska, Office of the CIO (OCIO) GIS Shared Services will be responsible for assuring that metadata is completed and the data is registered and available for distribution through NebraskaMAP.

5.3 Granting Agencies and Entities

State granting or fund disbursement entities or agencies will be responsible for ensuring that these standards are included in requirements related to fund disbursements as they relate to aerial imagery.

5.4 Other

Local government agencies that have the primary responsibility and authority for aerial imagery acquisition will be responsible for ensuring that those sub-sections defined in Section 1 will be incorporated in the overall imagery data development efforts and contracts.

6.0 Authority

6.1 NITC GIS Council

According to Neb. Rev. Stat. § 86-572(2), the GIS Council shall: Establish guidelines and policies for statewide Geographic Information Systems operations and management (a) The acquisition, development, maintenance, quality assurance such as standards, access, ownership, cost recovery, and priorities of data bases; (b) The compatibility, acquisition, and communications of hardware and software; (c) The assessment of needs, identification of scope, setting of standards, and determination of an appropriate enforcement mechanism; (d) The fostering of training programs and promoting education and information about the Geographic Information Systems; and (e) The promoting of the Geographic Information Systems development in the State of Nebraska and providing or coordinating additional support to address Geographic Information Systems issues as such issues arise.

7.0 Related Documents

7.1 American Society for Photogrammetry and Remote Sensing (ASPRS), ASPRS Accuracy Standards for Digital Geospatial Data (2014).

7.2 FGDC Content Standard for Digital Geospatial Data Version 2 (FGDC-STD-001-1998).

7.3 ISO 19115:2003(E) North American Profile (NAP) Metadata Standards. National Oceanic and Atmospheric Administration (NOAA). January 2012.

Addendum 1: License/Subscription Imagery Standards

A1.0 Description. NITC imagery standard to address any imagery licensing or commercial off-the-shelf (COTS) imagery subscription funded with state funds. Since the imagery is not a custom collection, it needs to be best available. The imagery needs to be high enough quality to be able to derive accurate street centerlines and address points (for example, to be able to digitize centerlines and address points on 12" imagery).

A2.0 Standards. For any imagery solution that is subscription based or licensed model, the vendor must meet the following specifications.

- A2.1 Image resolution. Minimum standard of 12" or 30 cm.
- A2.2 Horizontal accuracy. Provide the horizontal accuracy expressed as RMSEr or CE90 and CE95. Must document if the imagery meets NENA standards (draft or published). Must provide documentation on how the horizontal accuracy was determined.
- A2.3 Environmental. Environmental specifications such as cloud cover and snow/ice, bit depth and sun angle, need to meet NITC imagery standard sections 1.2.1.1, 1.2.1.4, and 1.2.1.5 and be documented.
- A2.4 Metadata. Provide metadata on the imagery collection. Metadata needs to follow the NITC metadata standards or at a minimum FGDC compliant metadata. Metadata should accompany individual tile sets.
- A2.5 Projections. Define what the data project is. The most common for Nebraska is Web Mercator WGS84, Nebraska State Plane NAD 83 Feet or UTM NAD 83. Nebraska is covered by UTM Zones 13, 14 and 15. Most of the state is UTM 14. NITC imagery standard is reference in section 1.2.7.
- A2.6 Datum. Define the datum used. The datum should meet the NITC imagery standard referenced in section 1.2.7.

A3.0 Guidelines. The following are items to be considered for any contract or Request for Proposal (RFP) regarding subscription or licensed imagery.

- A3.1 Accessing the imagery.
  - A3.1.1 Is the imagery available to be downloaded or streamed?
  - A3.1.2 If downloaded, what is the timeframe that the imagery can be downloaded or provided on hard drives and the format?
  - A3.1.3 If the imagery is streamed, what format will the REST service be? (For example, WMS, WTMS or other format.) Is the REST service tiled?
  - A3.1.4 Is a viewer also provided? If so, are there associated costs?
  - A3.1.5 Can the imagery be downloaded through the REST service?
- A3.2 Cost, terms and restrictions of the license or subscription.
  - A3.2.1 Is there an option for a 4th band to achieve Color IR? If so, at what cost?
  - A3.2.2 Are there options for higher resolutions, such as 3", 6", 15cm, or other resolutions? If so, at what cost?
  - A3.2.3 What are licensing restrictions with the subscription? (For example, is the imagery available to state agencies, political subdivisions, and viewable to the public?) Can the imagery be used in mobile collection applications?
  - A3.2.4 What happens to the imagery and access to the imagery after the contract expires or is terminated?
  - A3.2.5 What happens to prior versions of imagery? (For example, may prior versions be made available to the public for free?)
  - A3.2.6 Can the vendor provide an evaluations sample of the imagery of Nebraska to review during an evaluation period?

3-205. Street centerlines.

(1) The commission adopts by reference the most recent version of sections 2, 3, and 3.1 of the NENA Standard for NG9-1-1 GIS Data Model released by the National Emergency Number Association [https://www.nena.org/page/ng911gisdatamodel] for GIS data that consists of street centerlines.

(2) The following are optional additional attributes for street centerlines:

From Road Level	FromLevel	O	P	1
To Road Level	ToLevel	O	P	1

FromLevel: Specifies the 'elevation' of a segment FROM node (start point). This field does not require actual elevation in terms of real-world measurements. The value is only used to determine whether a turn is allowed from one street to a street that intersects it in a 2-dimensional space, similar to floors in a building. Nodes at the lowest level would be assigned 0, with overlapping nodes representing additional level(s)/overpass(es) will be assigned the next sequential integer value accordingly.

ToLevel: Specifies the 'elevation' of a segment TO node (end point). This field does not require actual elevation in terms of real-world measurements. The value is only used to determine whether a turn is allowed from one street to a street that intersects it in a 2-dimensional space, similar to floors in a building. Nodes at the lowest level would be assigned 0, with overlapping nodes representing additional level(s)/overpass(es) will be assigned the next sequential integer value accordingly.

--

History: Adopted on March 27, 2015. Amended on July 25, 2019 and November 10, 2022.
URL: https://nitc.nebraska.gov/standards/3-205.pdf

3-206. Address points.

The commission adopts by reference the most recent version of sections 2, 3, and 3.2 of the NENA Standard for NG9-1-1 GIS Data Model released by the National Emergency Number Association [https://www.nena.org/page/ng911gisdatamodel] for GIS data that consists of address points.

--

History: Adopted on March 27, 2015. Amended on July 25, 2019 and November 10, 2022.
URL: https://nitc.nebraska.gov/standards/3-206.pdf

CHAPTER 4

E-GOVERNMENT

Article.

--

ARTICLE 1

GENERAL PROVISIONS

Section.

4-101. Social media guidelines.

The purpose of this section is to provide guidelines for the use of social media by state agencies, boards, and commissions. Agencies may also utilize these guidelines as a component of agency-specific policies. State employees or staff using social media for state business, both on and off the Nebraska.gov domain, should be made aware of these guidelines or, if applicable, agency-specific policies.

(1) Definition. "Social media" is a general term that encompass various online activities that facilitate social interaction and collaborative content creation. Social media includes Twitter, Facebook, YouTube, Flickr, blogs, wikis, photo and video sharing, podcasts, social networking, and multiuser virtual environments.

(2) Business Decision. The decision to utilize social media is a business decision, not a technology-based decision. It must be made at the appropriate management level for each agency, considering the agency's mission, objectives, capabilities, and the potential benefits.

(3) State Portal Link. Agencies should notify the network manager of the state portal to have their social media pages linked on the state website (http://www.nebraska.gov/social/).

(4) Profile Information. Agency social media accounts should include the following information in the profile or information section: (a) "Official Nebraska Government Page," (b) the agency's name, and (c) a link to the agency's website.

(5) Records Retention. Agencies should follow applicable records retention policies for social media accounts. (See Schedule 124, Item 124-125, http://www.sos.ne.gov/records-management/pdf/general-records-for-state-agencies-124.pdf.)

(6) Agency Access. Agencies should ensure that more than one staff member has access to the agency's social media sites.

(7) Alternative Contact Information. If the social media site it intended for pushing information only, the agency should provide alternative ways to contact the agency.

(8) Disclaimer. This subsection contains recommended items to address on a social media disclaimer or disclosure page. The page should include a general statement of purpose and notice of the following:

(a) The social media site is not hosted by the state and is subject to policies within the control of the third-party host of the site;

(b) Communication of a personal or private nature in relation to agency business, as well as official state business interactions, should be made via the traditional agency communications channels and not via the public comment areas of the social media site;

(c) The agency is not responsible for any web page author's personal content outside the work place;

(d) The agency is not responsible for any third-party content of any kind;

(e) All communications are subject to the state's public records laws;

(f) If comments are allowed on a social media site, it is a limited forum and comments must be related to the subject matter of the social media posting. Comments may be monitored. If content is removed, a copy will be maintained in accordance with applicable records retention requirements. The following forms of content will not be allowed: (i) comments not related to the subject matter of the particular social media article being commented upon; (ii) comments campaigning for or against the nomination or election of a candidate or the qualification, passage, or defeat of a ballot question; (iii) profane language or content; (iv) content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, national origin, physical or mental disability, or sexual orientation; (v) sexual content or links to sexual content; (vi) solicitations of commerce; (vii) conduct or encouragement of illegal activity; (viii) information that may tend to compromise the safety or security of the public or public systems; or (ix) content that violates a legal ownership interest of any other party.

(9) Best Practices. The following are suggestions on how best to use and maintain social media sites:

(a) Ensure that your agency sanctions official participation and representation on social media sites. Stick to your area of expertise and provide unique, individual perspectives on what is going on at the state and in other larger contexts. All statements must be true and not misleading, and all claims must be substantiated and approved;

(b) Post meaningful, respectful comments, no spam, and no remarks that are off-topic or offensive. When disagreeing with others' opinions, keep it appropriate and polite;

(c) Pause and think before posting. Reply to comments in a timely manner when a response is appropriate unless you have posted a disclaimer that this is not official two-way communication;

(d) Be smart about protecting yourself, your privacy, your agency, and any restricted, confidential, or sensitive information. What is published is widely accessible, not easily retractable, and will be around for a long time (even if you remove it), so consider the content carefully. Respect proprietary information, content, and confidentiality;

(e) If you are under a generic name, consider using some form of tagging to identify the person posting content; and

(f) Email or login names should lead the user back to a "state id," such as an official state email address, or make a user name that indicates you are a state employee.

--

History: Adopted on November 9, 2010. Amended on June 30, 2011 and July 12, 2018.
URL: https://nitc.nebraska.gov/standards/4-101.pdf

ARTICLE 2

STATE GOVERNMENT WEBSITE

Section.

4-201. State government web pages; footer guidelines.

The footer of each Nebraska state government web page should include the following: (1) a link to the Nebraska state government home page, http://www.nebraska.gov; and (2) a link to the Nebraska.gov website policies page, http://www.nebraska.gov/policies/; or a link to the agency's website policies page; or both.

--

History: Adopted on June 14, 2005. Amended on July 12, 2010; December 10, 2013; and November 9, 2017.
URL: https://nitc.nebraska.gov/standards/4-201.pdf

4-202. Web cookie standard.

The purpose of this standard is to establish guidance for the use of web cookies on websites, web pages, and web applications created by state agencies, boards and commissions.

(1) Nebraska.gov and state agencies may use cookies to store user information subject to the requirements of this section.

(a) Permanent Cookies. Permanent cookies: (1) must not contain personal identifying information (e.g. names, date of birth, social security number, hint answers); (2) may be used to save personalized web site settings (e.g. font size, color, text type); and (3) may include an expiration date if appropriate.

(b) Session Cookies. Session cookies: (1) must be erased when a user's web browser session ends or the user logs out of the application; and (2) must only be accessible to the specific application(s) in use.

(2) Any use of cookies can be made known to the user through the use of appropriate browser settings.

--

History: Adopted on August 4, 2006. Amended on July 12, 2018.
URL: https://nitc.nebraska.gov/standards/4-202.pdf

4-203. Security statement.

The following security statement will be posted on a website policies page linked directly from the Nebraska state government home page:

> "The State of Nebraska is committed to ensuring the integrity and security of the information and systems it maintains. The State has taken steps designed to safeguard its telecommunications and computing infrastructure to prevent unauthorized access to internal systems and confidential information. If you have any knowledge of a security breach or potential security breach, please contact us at 402-471-4636 or cio.help@nebraska.gov."

--

History: Adopted on June 14, 2005. Amended on July 12, 2018.
URL: https://nitc.nebraska.gov/standards/4-203.pdf

4-204. Emergency information web page.

This section establishes the recommended location for an emergency information web page where information for the general public would be posted in the event of a disaster.

The emergency information web page should be named “disaster.html” and should be placed in the top level directory of the agency website (e.g., http://agency.nebraska.gov/disaster.html).

--

History: Adopted on February 22, 2007. Amended on July 12, 2018.
URL: https://nitc.nebraska.gov/standards/4-204.pdf

CHAPTER 5

STATE GOVERNMENT ENTERPRISE SYSTEMS

Article.

1. [Reserved.]
2. Email System.
3. Internet Fax System.
4. Active Directory.

--

URL: https://nitc.nebraska.gov/standards/5-Chapter.pdf

ARTICLE 1

[RESERVED]

Section.

5-101. [Repealed.]

--

History: Adopted on April 11, 2012. Amended on July 12, 2018. Repealed on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/5-101.pdf

5-102. [Repealed.]

--

History: Adopted on November 15, 2011. Repealed on November 8, 2018.
URL: https://nitc.nebraska.gov/standards/5-102.pdf

ARTICLE 2

EMAIL SYSTEM

Section.

5-201. Email standard for state agencies.

All state government agencies, except higher education entities, shall use the email service provided by the Office of the CIO for their workers.

--

History: Adopted on November 17, 1997 (by the Information Resources Cabinet). Amended on June 3, 2004; June 14, 2005; September 18, 2007; March 4, 2008; and July 12, 2018.

URL: https://nitc.nebraska.gov/standards/5-201.pdf

5-202. [Repealed.]

--

History: Adopted on November 13, 2003. Repealed on April 19, 2013.
URL: https://nitc.nebraska.gov/standards/5-202.pdf

5-203. [Repealed.]

--

History: Adopted on November 13, 2003. Repealed on April 19, 2013.
URL: https://nitc.nebraska.gov/standards/5-203.pdf

5-204. [Repealed.]

--

History: Adopted on March 1, 2011. Amended on June 30, 2011; February 14, 2012 (Technical Panel); December 10, 2013; February 11, 2014 (Technical Panel); and July 12, 2017. Repealed on July 14, 2023.

URL: https://nitc.nebraska.gov/standards/5-204.pdf

ARTICLE 3

INTERNET FAX SYSTEM

Section.

5-301. Internet fax standard for state agencies.

All state government agencies, except higher education entities, shall use the OCIO Internet Fax System provided by the Office of the CIO for computer-based fax services, including desktop and application-based faxing.

This standard does not apply to the use of stand-alone fax machines connected directly to a telephone line.

--

History: Adopted on September 30, 2003. Amended on November 30, 2009, and July 12, 2018.
URL: https://nitc.nebraska.gov/standards/5-301.pdf

ARTICLE 4

ACTIVE DIRECTORY

Section.

5-401. Active Directory; user photographs.

(1) Purpose. Microsoft Active Directory has an attribute ("thumbnailPhoto") to store a thumbnail photograph of each user. Other applications, including Microsoft Outlook and the Exchange Global Address List, will display these photographs automatically in the context of providing information about the user. This policy provides guidance on the use of this feature in the state's shared Active Directory forest.

(2) Optional Use. Each agency has the option to use, or not use, the thumbnail photograph functionality in the state's shared Active Directory forest.

(3) Requirements. If an agency chooses to use the thumbnail photograph functionality, the following requirements will apply:

(a) Image file type: JPEG;

(b) Image file size: 10 KB or smaller;

(c) Image file name: Same as the user login ID plus the .jpg extension (for example, john.doe.jpg);

(d) Image size: 96x96 pixels is recommended;

(e) Image content: A recent head-and-shoulders photograph of the user (not an avatar, icon, drawing, etc.);

(f) The agency is responsible for obtaining photographs of their users;

(g) The agency must use the mechanism provided by the Office of the CIO for uploading agency image files; and

(h) The agency must not modify the Active Directory “thumbnailPhoto” attribute directly.

--

History: Adopted on December 10, 2013. Amended on July 12, 2018.
URL: https://nitc.nebraska.gov/standards/5-401.pdf

CHAPTER 6

[RESERVED]

CHAPTER 7

NETWORKS

Article.

1. State Network.
2. Network Nebraska.

RD. Resource Documents.

--

URL: https://nitc.nebraska.gov/standards/7-Chapter.pdf

ARTICLE 1

STATE NETWORK

Section.

7-101. State communications system; acceptable use policy.

(1) Purpose. This policy applies to all users of the state communications system. It is intended to provide minimum standards for acceptable use of the system; agencies may adopt policies or standards more stringent than those contained herein. All use of the system is subject to applicable state and federal laws. Users should not have any expectation of privacy regarding personal business conducted on the system unless otherwise protected by state or federal law.

(2) Acceptable Use. The state communications system may be used for the following:

(a) The conduct of state business;

(b) State government sponsored activities;

(c) By state employees and officials for emails, text messaging, local calls, and long-distance calls to children at home, teachers, doctors, daycare centers, baby-sitters, family members, or others to inform them of unexpected schedule changes, and for other essential personal business. Any such use for essential personal business shall be kept to a minimum and shall not interfere with the conduct of state business. A state employee or official shall be responsible for payment or reimbursement of charges, if any, that directly result from any such communication. [Neb. Rev. Stat. § 81-1120.27(1)] Essential personal business shall not include use of the state communications system for personal financial gain or campaigning for or against the nomination or election of a candidate or the qualification, passage, or defeat of a ballot question; these uses are prohibited. [Neb. Rev. Stat. § 49-14,101.01(2) and § 49-14,101.02(2)]; and

(d) Such other uses allowed by law.

(3) Remedial Action. Each agency is responsible for taking immediate remedial action to address any violation of this policy within the agency.

(4) Exception. This section does not apply to wireless access points available for general use by the public.

--

History: Adopted on March 9, 2004. Amended on November 30, 2009, and July 12, 2018.
URL: https://nitc.nebraska.gov/standards/7-101.pdf

7-102. DNS forwarding standard.

All outbound internet DNS traffic must be forwarded through the state's internal DNS servers.

--

History: Adopted on June 27, 2007. Amended on March 4, 2008, and July 12, 2018.
URL: https://nitc.nebraska.gov/standards/7-102.pdf

7-103. SMTP routing standard.

All inbound and outbound SMTP traffic must be routed through the anti-spam and anti-virus appliance managed by the Office of the CIO.

--

History: Adopted on June 27, 2007. Amended on March 4, 2008, and July 12, 2018.
URL: https://nitc.nebraska.gov/standards/7-103.pdf

7-104. Web domain name standard.

(1) The approved domain names for Nebraska state government websites are “nebraska.gov” and “ne.gov.” The Chief Information Officer may approve other domain names using the .gov top level domain.

(2) The domain “state.ne.us” is a supported legacy domain that may serve content but should not be publicly promoted.

(3) Domain names using top level domains other than those listed in subsections (1) and (2) may be registered and serve content but must not be publicly promoted.

(4) All state government websites using the .gov domain must comply with federal .gov domain requirements (https://home.dotgov.gov/registration/requirements/).

(5) All domain name registrations, purchases, and renewals must be made by the Office of the CIO.

--

History: Adopted on April 19, 2013. Amended on October 28, 2014; July 12, 2018; and March 10, 2022.
URL: https://nitc.nebraska.gov/standards/7-104.pdf

7-105. Wireless local area network standard.

(1) Purpose. The purpose of this standard is to ensure that only properly secured and managed wireless local area networks are deployed by state agencies.

(2) Registration Requirement. All wireless local area networks that connect to the state network must be registered with the Office of the CIO.

(3) Registration Process. The registration process will identify: contact information; device information, including the manufacturer, model, and physical location; the security/firewall technologies being deployed; where logging information is to be stored; and, if the use of the wireless access is only for internet, a description showing how traffic will be separated. Registration information must be submitted to the Office of the CIO Service Desk. Registration must occur prior to deployment. The Office of the CIO will contact the registering agency after reviewing the registration information. Final device names are assigned by the Office of the CIO during the registration process to avoid conflicts and confusion, and to aid in incident response and in identifying and locating wireless devices. If technology allows for the broadcast of a device name, standardized names should appear in the broadcast description, along with any unique identifiers assigned to the unit.

(4) Unregistered and Unsecured Devices. Only approved wireless local area networks and access points will be deployed within state agencies. Unregistered devices will be removed from service. Network managers for the Office of the CIO will incorporate procedures for scanning for unregistered wireless devices and access points. The Office of the CIO may disable network access for a device, server or network if inadequate security is found or improper procedures are discovered.

(5) Management and Security of Access Points.

(a) Physical Security. Access points must be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices must not be placed in easily accessible public locations.

(b) Configuration Management. All wireless access points must be secured using a strong password. Passwords must be changed at least every six months. Administrators must ensure all vendor default user names and passwords are removed from the device.

(6) Security of the Wireless Network.

(a) Logging. All access to the wireless network must be logged with records kept for a minimum of one year. Records must include the time of access, the IP and MAC addresses of the device, and the username.

(b) Access to the State Network. Accessing the state network requires a username and password combination that is unique to each user. The SSID must use a minimum of WPA2 with the use of a FIPS 140-2 validated AES encryption module.

(c) Wireless Intrusion Detection Systems. All wireless networks must use a wireless intrusion detection systems (WIDS) capable of location detection of both authorized and unauthorized wireless devices. All systems must provide continuous scanning and monitoring. WIDS logs and documented actions must be maintained for a minimum of one year

(7) Management of Airspace. All conflicts regarding wireless connectivity are resolved by the Office of the CIO.

--

History: Adopted on September 30, 2013. Renumbered on July 12, 2018 (previously was § 7-301). Amended on August 4, 2006; April 11, 2012; and July 12, 2018.
URL: https://nitc.nebraska.gov/standards/7-105.pdf

7-106. Internet of Things (IoT) standard.

This policy provides standards for Internet of Things (IoT) devices within the state network. IoT devices include but are not limited to door controls, cameras, and wireless sensors. While the benefits of IoT devices are numerous and compelling, it is important to remember that these devices have the potential to introduce significant threats and risks to the state network. IoT devices do not follow an international compatibility standard leaving them more exposed to vulnerabilities. The State of Nebraska must properly govern and manage deployment IoT devices.

The following are the minimum standards for IoT devices on the state network:

(1) IoT devices must be approved by the Office of the CIO prior to being put on the state network;

(2) IoT devices must be isolated from business operations on the state network;

(3) IoT devices must support either username/password or certificate-based authentication;

(4) IoT devices must support a minimum of TLS 1.2;

(5) IoT devices must have the ability to be managed at the enterprise level;

(6) IoT devices must allow for NTP and DNS to be set by administrators;

(7) IoT device access must be limited to only what is necessary;

(8) Network traffic for IoT devices should not be prioritized over normal business operations unless the IoT device impacts emergency services or public safety; and

(9) Wired connections for IoT devices are preferred over wireless connections when possible.

--

History: Adopted on March 10, 2022.
URL: https://nitc.nebraska.gov/standards/7-106.pdf

ARTICLE 2

NETWORK NEBRASKA

Section.

7-201. Network Nebraska; network edge device standard.

(1) Purpose. The purpose of this standard is to set minimum standards and specifications for network edge devices that would perform the routing and switching functions of voice, video, and data across the network and assure that packets would get to their correct destination while maintaining the appropriate quality of service (QoS).

(2) Technical Standards. Agencies and other entities electing to connect to Network Nebraska for purposes of transmitting data across the state shall comply with this standard.

(a) Network edge device specifications for new purchases: (1) QoS capabilities; (2) sufficient ports for desired network design; (3) security and/or firewall features; (4) routing and/or routing protocol; (5) traffic shaping and rate limiting; (6) VLAN (802.1q) support; (7) secure remote management (SSH); (8) hardware based encryption acceleration; (9) performance to meet anticipated usage demand; (10) compatibility with central site router features; and (11) IPv6 capable. Option include: a Layer 3 router for basic site deployment; an enhanced Layer 3 router for larger site deployment or higher performance; or a Layer 3 switch/firewall combination.

(b) Network edge device specifications for existing equipment: (1) QoS capabilities; (2) sufficient ports for desired network design; (3) security and/or firewall features; (4) routing and/or routing protocol; (5) traffic shaping and rate limiting; (6) VLAN (802.1q) support; (7) secure remote management (SSH); (8) hardware based encryption acceleration; (9) performance to meet anticipated usage demand; (10) compatibility with central site router features; and (11) IPv6 capable.

(3) Responsibilities.

(a) Network Nebraska Operational Entities. The Collaborative Aggregation Partnership, composed of the University of Nebraska Computer Services Network, the Office of the CIO, and Nebraska Educational Telecommunications, will be responsible for sharing the responsibilities of the network operations portion of Network Nebraska. The responsibility for identification and mitigation of non-compliant entities with respect to this standard resides with the Collaborative Aggregation Partnership.

(b) Education-Related Political Subdivisions. An education-related political subdivision shall provide notice in writing, as required by guidelines established by the University of Nebraska and the Chief Information Officer for participation in Network Nebraska, to the distance education director of the Educational Service Unit Coordinating Council, the University of Nebraska, and the Chief Information Officer prior to the use of any new or additional equipment

that will impact the use of Network Nebraska by such education-related political subdivision or other education-related political subdivisions. [Neb. Rev. Stat. § 86-520.01]

--

History: Adopted on July 12, 2006. Amended on March 4, 2008; November 15, 2011; and July 12, 2018.
URL: https://nitc.nebraska.gov/standards/7-201.pdf

7-202. Contracting guideline for upgrade of distance learning services.

(1) Purpose. The purpose of this guideline is to make the contracted services portion of distance learning contracts more flexible for the end-user and the provider and better able to accommodate future technology applications.

(2) Objective. The objective of this guideline is to permit users to access all the bandwidth on the negotiated circuit. It will allow providers to continue service and to expand networks as required by updating the systems they use to NEBS (Network Equipment Building System) standard compatible equipment. It will allow interoperability between users among multiple consortia. It will permit new telecommunications services on the DS-3 connections in use and permit increased speeds on current services such as access to the internet.

(3) Guidelines. Entities that receive state funding for telecommunications and public entities that are approaching contract expiration for existing distance learning services are advised to make every attempt to take advantage of the efforts to aggregate services and contracts. As new contracts are contemplated for distance learning, it is recommended that discussions minimally include consideration of the following:

(a) Contracting Options. (1) Negotiate one contract for connective terminal hardware and transport as long as the end-user has full access to and flexible use of all bandwidth on the network and has the ability to upgrade video encoding equipment as desired, or (2) negotiate two contracts at the local level; one contract for procurement (including maintenance) of connective terminal hardware (CODEC) and a second contract for transport (preferably the use of Network Nebraska).

(b) Contract Expiration Dates. To the extent possible, the local entity should make transport contract expiration dates co-terminus with the Network Nebraska core transport contracts (contact the Office of the CIO for more information).

--

History: Adopted on November 13, 2003. Amended on July 12, 2018.
URL: https://nitc.nebraska.gov/standards/7-202.pdf

7-203. IP communication protocol standard for synchronous distance learning and videoconferencing over Network Nebraska.

(1) Purpose. The purpose of this standard is to implement a consistent communication protocol to be used by all entities wishing to pass synchronous, interactive teleconference video over Network Nebraska.

(2) Standard. All state agencies, entities that receive state funding for telecommunications, and entities that wish to pass synchronous video over Network Nebraska must use IP as their communication protocol for synchronous video.

--

History: Adopted on November 13, 2003. Renumbered on July 12, 2018 (previously was § 7-401). Amended on July 12, 2018.
URL: https://nitc.nebraska.gov/standards/7-203.pdf

7-204. Video and audio compression standard for synchronous distance learning and videoconferencing.

(1) Purpose. The purpose of this section is to establish video and audio protocol standards that will enable all existing and future synchronous distance learning and videoconferencing facilities in Nebraska to achieve interoperability and maintain an acceptable quality of service.

(2) Standards.

(a) Video protocol standards for synchronous distance learning and videoconferencing: (i) for data rates above 384 Kbps, H.263; and (ii) for data rates at or below 384 Kbps, H.264 (MPEG-4 Part 10). The CODECs selected for purchase or use should be capable of accommodating both standards and be capable of manual rate selection and/or automatic rate selection. The interconnecting CODECs should be allowed to automatically negotiate the best data rate.

(b) Audio protocol standards for synchronous distance learning and videoconferencing: (i) for data rates above 128 Kbps, G.722; and (ii) for data rates at or below 128 Kbps, G.722 or G.722.1 or G.728. The CODECs selected for purchase or use should have the ability to use G.722 at all speeds and one or both of the other two standards listed for lower speeds. If any two CODECs do not have a common protocol at or below 128Kbps then they should continue to use G.722. The CODECs selected for purchase or use should be capable of accommodating audio standard G.722 and be capable of manual rate selection and/or automatic rate selection. The interconnecting CODECs should be allowed to automatically negotiate the best data rate.

(3) Applicability. This section applies to synchronous distance learning and videoconferencing facilities as follows:

(a) If utilizing state-owned or state-leased communications networks: (i) any synchronous distance learning facility or videoconferencing application which utilizes state-owned or state-leased communications networks must comply with the compression standards listed in this section; or (ii) the entity must provide, or arrange for, the necessary gateway technology to transcode to the adopted standards.

(b) If using state funding: (i) all new facilities or applications receiving state funding must comply with the compression standards listed in this section; and (ii) all existing facilities or applications receiving state funding for ongoing operations must convert to the standards listed in this section as soon as fiscally prudent or upon renewal of any existing communications service contract, whichever comes first.

--

History: Adopted on September 9, 2004. Renumbered on July 12, 2018 (previously was § 7-402). Amended on July 12, 2018.

URL: https://nitc.nebraska.gov/standards/7-204.pdf

7-205. Scheduling standard for synchronous distance learning and videoconferencing.

(1) Purpose. The purpose of this standard is to establish and define the needs for scheduling to be addressed when purchasing and maintaining scheduling coordination systems. The objective of this standard is to enable all existing and future synchronous distance learning and videoconferencing facilities in Nebraska to achieve interoperability and maintain an acceptable scheduling of services through recurring and ad hoc event coordination.

(2) Standards. This subsection consists of a list of five components and accompanying features that must be available in any software system that is developed for use in scheduling of synchronous events using videoconferencing technology. It is the intent that any and all such scheduling systems defined by the specifications below be accessible either through the internet or within a defined intranet as decided upon by the system administrators. The following sections describe the various levels and types of scheduling or coordination that must be accommodated.

(a) Hardware Control Component. When attempting to link two or more sites electronically, a system must have the capability to coordinate the connectivity between/among the sites. This includes controlling the network and endpoint hardware and bandwidth necessary to cause a successful connection. A hardware control system must be able to control hardware in a network and be capable of linking into other systems listed in this standard to enable the following: (i) browser-based access; (ii) locate devices by IP address [both static and DHCP]; (iii) locate devices by MAC address; (iv) facilitate far-end control in endpoint devices with the capability; (v) display a call list that is understood by non-technical staff using plain English site descriptions; (vi) hardware and software systems must work such that the scheduling system is available for use at least 99.9% of the time; (vii) automatically accumulate log data that may be searched by system administrators using multiple search variables; (viii) maintain security in ways that can be defined by system administrators including providing an identity management system that allows for multiple levels of user access as defined by system administrators; and (ix) facilitate various types of events, such as broadcast to all, broadcast to some, 2-way point-to-point, and 2-way multipoint.

(b) Event Logging Component. A system coordinator must have the ability to track information about events. This may include knowing the number of people at a site, the minutes an event runs at any given site, or the number of events a specific organization schedules. An event logging system must be able to automatically store data and permit reporting and be capable of linking into other systems listed in this standard to include the following: (i) browser-based access; (ii) store data in an ODBC compliant relational database; (iii) provide fields for logging various pieces of information; (iv) permit system administrator defined fields [no fewer than 64]; and (v) local contact and facility arrangement information.

(c) Facilities Coordination Component. If an event will include locations for which more than one person/organization has responsibility, then some mechanism must exist for coordinating use of facilities. There may be technical or administrative limits as to the number or types of sites that can participate in any given event. This could be as simple as users coordinating times over the telephone or through email, but for some applications there may be a greater need for pre-scheduling and coordination among multiple administrators. A facilities coordination system shall enable access to facilities based on defined permissions, resolve conflicts based on pre-determined policies and be capable of linking into other systems listed in this standard to include the following: (i) browser-based access; (ii) system editable user access, including: (A) building level admin such that the facilities at a specific location can set policies for that site and permit use by others; (B) regional admin such that a group of facilities can set policies for all related sites and permit use by others; (C) sector admin such that groups of groups of facilities can set policies for all related sites and permit use by others; and (D) user account directory service with definable permissions for each account; (iii) facilities information to be posted, including: (A) identify technology available by site; (B) physical site location; and (C) local contact and facility arrangement information; and (iv) permit system administrator defined fields [no less than 64] that would provide for event information to be posted.

(d) People Coordination Component. If a specific location is to be used, this implies that operational support will be available to support the success of events. Since there will be a variety of site designs and equipment configurations, then there may be a variety of demands on staff time. Finally, there may be limitations as to the total number of participants allowed. A people coordination system must enable interaction of people based on policies set by system administrators and be capable of linking into other systems listed in this standard to include the following: (i) browser-based access; (ii) allow for multiple permission levels including: (A) view schedules, (B) request systems/facilities, and (C) approve systems/facilities use; (iii) provide information about instructor/facilitator and their availability; (iv) allow for predetermined maximum number of attendees; (v) track and display count of committed and remaining attendees; (vi) allow for predetermined maximum number of sites; and (vii) track and display count of committed and remaining sites.

(e) Event Clearinghouse Component. As system users see a need for pre-scheduled events coordinated among a large number of facilities and administrators, the concept of a virtual location for brokering of events becomes attractive. Such a clearinghouse should serve as a way that event coordinators might let others know the specifics of events they are planning [e.g., a certain class with a specific sort of content will be offered on a certain schedule for a certain period of time or a specific event will happen one time on a specific day at a specific time]. Such an event clearinghouse should also serve as a way for interested parties to find events that meet their specific needs [e.g., a school administrator has a certain number of students who need a specific class that is not offered locally]. Availability might also include information about participant or site number limitations [e.g., the total seats/sites in the class/event, the number

requested/registered so far and the number remaining of the total]. An event clearinghouse system must enable online interaction for publishing of event information and be capable of linking into other systems listed in this standard to include the following: (i) browser-based access; (ii) posting of one-time single events; (iii) posting of sequenced or cyclical events; (iv) posting of costs to participate in an event; (v) permit system administrator defined fields [no less than 256]; (vi) provide for automated multiple time zone accommodation; (vii) use an ODBC compliant relational database; (viii) user defined search/reporting capability; and (ix) provide for automated email notification of site requests/confirmations.

(3) Applicability. This section applies to the purchase and maintenance of synchronous distance learning and videoconferencing software systems used by educational institutions. The governing board or chief administrative officer of each organization is responsible for selecting and using a synchronous distance learning and videoconferencing software system that is in compliance with these standards. It is the intent of the Technical Panel and Commission that the guidelines and policies for usage of such scheduling and clearinghouse systems be determined by the administrative entities that oversee such distance learning and videoconferencing.

--

History: Adopted on September 9, 2004. Renumbered on July 12, 2018 (previously was § 7-403). Amended on July 12, 2018.
URL: https://nitc.nebraska.gov/standards/7-205.pdf

RESOURCE DOCUMENTS

Section.

7-RD-01. Telecommunications facilities and services.

(1) Purpose. This resource document is intended to provide guidance to agencies on telecommunications facilities and services needed in an ordinary office setting and to provide a suggested allocation of responsibilities between a lessor, lessee, and tenant agency. Any such work in a state owned building should meet these minimum requirements.

(2) Responsibilities.

(a) Tenant Agency. The tenant agency will obtain all telecommunication services except local cable-television or satellite-television services from the Office of the CIO. The tenant agency will pay the monthly charges for said telecommunication services. The tenant agency will pay any charges for local cable-television or satellite-television services. This includes costs to install satellite-television receiving equipment and cabling. The tenant agency will contact the Office of the CIO should any of the items in this document not meet the needs of the agency.

(b) Lessor. The lessor should ensure adequate entrance facilities are provided for the telecommunication services required by the tenant agency. This includes all necessary tie cables between the service provider's terminal and/or demarc blocks and all remote wiring-closets/consolidation-points used to attach services to the station cabling serving the telecommunication information outlets. Costs associated with the installation and/or upgrading of existing entrance facilities and/or tie cables should be incurred by the lessor. The lessor should provide, at a minimum, a telecommunications information outlet at each desk and/or workstation. Each telecommunications information outlet should consist of two modular jack connectors: one telephone (voice) jack and one computer (data) jack.

(3) Telecommunications Facilities and Services; Recommended Requirements.

(a) Telecommunications Information Outlet Cabling Requirements.

(i) Each telephone cable shall be a solid copper, 24 AWG, 100 Ω balanced twisted-pair (UTP), at a minimum Category 3 cable with four individually twisted-pairs, which meet or exceed the mechanical and transmission performance specifications as outlined in the most current ANSI TIA-568 Commercial Building Telecommunications Cabling Standard, as of the signing date of the lease agreement.

(ii) Each data cable shall be a solid copper, 23 or 24 AWG, 100 Ω balanced twisted-pair (UTP), at a minimum Category 6 cable with four individually twisted-pairs, which meet or exceed the mechanical and transmission performance specifications as outlined in the most current ANSI TIA-568 Commercial Building Telecommunications Cabling Standard, as of the signing date of the lease agreement.

(b) Telecommunications Information Outlet Connector Requirements.

(i) Each voice outlet shall be an 8-pin modular, at a minimum Category 3, unkeyed jack, using the USOC pin/pair assignment.

(ii) Each data outlet shall be an 8-pin modular, at a minimum Category 6, unkeyed jack, using the T568B pin/pair assignment.

(c) Telecommunications Cabling Installation Requirements.

(i) The lessor shall provide a complete and working telecommunication distribution system. This system shall include, but is not limited to: all station, riser, aerial, and intra-campus cables as required; conduits, raceways, and all associated cable support hardware; telephone and data outlet connectors, face plates, and identification labels; termination blocks and brackets, patch panels and mounting brackets, distribution rings; all cable terminations and testing; and all associated appurtenances as required by the distribution system.

(ii) Each telephone and computer jack shall be terminated on separate cables, which shall be terminated on separate connecting blocks/panels at a common central location.

(iii) Installation, termination, and testing of telecommunications information outlet components shall be performed by qualified personnel, employed by a company whose primary business is providing telecommunication services. This does not include work normally performed by an electrical contractor.

(iv) All work shall be performed in accordance with the equipment manufacturer's requirements.

(v) All cable terminations shall be performed at the respective terminal boards, equipment cabinets, and station outlets.

(vi) All station cabling shall be "home run" to appropriate distribution frame, block, or equipment cabinet. No splices will be allowed in these lines.

(vii) Distribution panels are not to be located in a plenum area or above accessible ceilings.

(viii) All cables installed above accessible ceilings shall be neatly bundled utilizing commercially available products and attached to appropriate supports. Cables installed randomly and disorderly will not be allowed.

(ix) All cables shall be installed in a fashion not to interfere with the general maintenance of other electrical/mechanical devices, as well as in a manner that other electrical/mechanical devices will not interfere with the operation of the cables intended application.

(x) All installations shall conform to the most current ANSI TIA-568 Commercial Building Telecommunications Cabling Standard, as well as any associated technical systems bulletin, as of the signing date of the lease agreement.

(d) Telecommunications Information Outlet Testing Requirements.

(i) Each Voice and data cable link shall be tested and conform to the most current ANSI TIA-568 Commercial Building Telecommunications Cabling Standard, as of the signing date of the lease agreement. Testing shall be accomplished using level III or higher field testers.

(e) Telecommunications Information Outlet Documentation Requirements.

(i) Each information outlet faceplate and closet termination point shall be labeled.

(ii) The lessor shall provide a floor plan (paper copy and editable electronic copy) of the occupied space to the tenant agency. This floor plan shall indicate the following: outlet locations and labeling scheme; wiring closets and/or station-cabling concentration points; telephone rooms; data server rooms; and, if more than one wiring closet serves the occupied space(s), a visual representation shall indicate the floor area(s) being served by each closet.

(iii) The tenant agency shall maintain a current copy of the lessor-provided floor plan, indicating any moves, adds, or changes to the information outlets which occurred during the period of the lease. At the end of the lease term, the tenant agency shall provide the lessor a copy of this updated and current floor plan.

(f) Regulatory and Other Requirements.

(i) Wiring methods, conductor applications, and insulation materials shall meet all applicable provisions of the National Electrical Code and Federal Communications Commission Rules and Regulations as well as applicable State and Local Codes.

(ii) All new cables and wires installed shall be listed by Underwriters Laboratories, Inc.

(iii) All cables installed shall meet appropriate fire ratings.

(4) Definitions.

Demarc, or demarcation point, means the physical point at which separation is made between the telecommunications service provider's cable facilities and those owned by the end user/building owner. The point in which the provider's service is handed off to the user's cable facilities and/or equipment. Multiple demarc locations in one physical structure are common. Tie cables which provide connectivity between entrance facilities and demarc locations are owned by the local service provider.

Entrance facilities means an entrance to a building for both public and private network service cables (including antennas) including the entrance point at the building wall and continuing to the entrance room or space. Entrance facilities are often used to house electrical protection equipment and connecting hardware for the transition between outdoor and indoor cable. The entrance facility includes overvoltage protection (often referred to as a terminal) and connecting hardware for the transition between outdoor and indoor cable.

Home run means an individual cable run installed from a central distribution point to termination point. Each cable run is a continuous length without a splice or intermediate point. Each cable run is a continuous length without a splice or intermediate termination point. Typically referred to as a "star" topology.

Telecommunications information outlet means a user connection facility provided in a work area as part of a structured cabling system.

Tie cable means cabling facilities used to connect two physical points together. (Example: multi-conductor cable used to extend services from an entrance room or space to a remote wiring closet or station-cabling cross-connect field.) Riser cables, used to extend services between floors of a structure, are also considered tie cables. Tie cables can be copper or optical fiber in construction.

--

History: Approved by the Technical Panel on December 11, 2012.
URL: https://nitc.nebraska.gov/standards/7-RD-01.pdf

CHAPTER 8

INFORMATION SECURITY POLICY

Article.

1. Purpose; Scope; Roles and Responsibilities; Policy Exception Process.
2. General Provisions.
3. Access Control.
4. Network Security.
5. System Security.
6. Application Security.
7. Auditing and Compliance.
8. Vulnerability and Incident Management.
9. Data Security.

--

ARTICLE 1

PURPOSE; SCOPE; ROLES AND RESPONSIBILITIES; POLICY EXCEPTION PROCESS

Section.

8-101. Purpose.

The purpose of this Information Security Policy is to provide a uniform set of reasonable and appropriate security safeguards for protection of the confidentiality, integrity, and availability of State of Nebraska information collected, stored, and used to serve the citizens of the state. This Information Security Policy contains the safeguards, responsibilities and acceptable behaviors required to establish and maintain a secure environment.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-101.pdf

8-102. Scope.

(1) This policy applies to all information technology systems for which the state has administrative responsibility, including systems managed or hosted by third parties on behalf of an agency. In the event an agency has developed policies or additional requirements for information security, the more restrictive policy will apply.

(2) Portions of this policy are based on the standards, guidelines, and best practices developed by the National Institute of Standards and Technology (NIST), including the NIST Cybersecurity Framework (https://www.nist.gov/cyberframework) and related publications (https://csrc.nist.gov/publications). Additional items contained in these NIST publications—that are not included in this policy—should be treated as guidance and best practices to be followed by agencies as appropriate.

--

History: Adopted on July 12, 2017. Amended on March 12, 2020.
URL: https://nitc.nebraska.gov/standards/8-102.pdf

8-103. Roles and responsibilities.

(1) State Agencies. Agencies that create, use, or maintain information systems for the state must establish and manage an information security program consistent with this policy to ensure the confidentiality, availability, and integrity of the state's information assets. Agencies may work with the Office of the Chief Information Officer for assistance with implementing an information security program.

(2) Office of the Chief Information Officer. The Office of the Chief Information Officer is responsible for recommending policies and guidelines for acceptable and cost-effective use of information technology in noneducation state government.

(3) State Information Security Officer. The state information security officer serves as a security consultant to agencies and agency information security officers to assist the agencies in meeting the requirements of this policy and other policies. The state information security officer may also perform assessments of agency security for risk and compliance with this policy and other security related policies and frameworks as applicable.

(4) Agency Information Security Officer. An agency information security officer may be designated at the discretion of the agency. The agency information security officer has the responsibility for ensuring implementation, enhancement, monitoring, and enforcement of information security policies and standards for their agency. The agency information security officer may collaborate with the Office of the CIO on information security initiatives within the agency.

(5) Nebraska Information Technology Commission. The Nebraska Information Technology Commission is the owner of this policy with statutory responsibility to adopt minimum technical standards, guidelines, and architectures.

(6) Technical Panel. The Technical Panel is responsible for recommending technical standards and guidelines to be considered for adoption by the Nebraska Information Technology Commission.

(7) State Government Council. The State Government Council is an advisory group chartered by the Nebraska Information Technology Commission to provide recommendations relating to state government agencies.

(8) Security Architecture Workgroup. The Security Architecture Workgroup is chartered by the State Government Council to make recommendations to the State Government Council and Technical Panel on matters relating to security within state government; provide information to state agencies, policy makers, and citizens about real or potential security threats or

vulnerabilities that could impact state business; document and communicate existing problems, potential points of vulnerability, and related risks; and determine security requirements of state agencies stemming from state and federal laws, regulations, and other applicable standards.

--

History: Adopted on July 12, 2017. Amended on March 12, 2020 and July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-103.pdf

8-104. Policy exception process.

This policy establishes the controls and activities necessary to appropriately protect information and information technology resources. While every exception to a policy or standard weakens the protection for state IT resources and underlying data, it is recognized that at times business requirements dictate a need for temporary policy exceptions. In the event an agency believes it needs an exception to this policy, the agency may request an exemption by following the procedure outlined in section 1-103.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-104.pdf

ARTICLE 2

GENERAL PROVISIONS

Section.

8-201. Acceptable use.

Subject to additional requirements contained in state law, the following are the policies and provisions governing the acceptable use of information technology resources in state government: (1) section 7-101 is the acceptable use policy for the state network; (2) Neb. Rev. Stat. § 49-14,101.01 establishes certain statutorily prohibited uses of public resources; and (3) the following additional requirements established by this section: (a) all state electronic business must be conducted on approved IT devices; (b) accessing or attempting to access HIGH IMPACT or MODERATE IMPACT information for other than a required business "need to know" is prohibited; and (c) misrepresenting yourself as another individual or organization is prohibited.

Use of state information technology resources may be monitored to verify compliance with this policy.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-201.pdf

8-202. Change control management.

To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained.

The change management process may differ between changes to IT infrastructure (which includes all hardware, system software, and network assets) and application software (which includes commercial off the shelf data applications and in-house developed data application software). However, underlying requirements for managing change are the same. All IT infrastructure and application development changes are required to follow a change management process to ensure the change is approved for release and does not unknowingly add security risks to the state's environment. All changes to network perimeter protection devices should be included in the scope of change management.

(1) IT Infrastructure. The following change management standards are required to be followed for all IT infrastructure:

(a) The Office of the CIO requires a change management process with assigned responsibilities to ensure all changes to hardware, system software, and network infrastructure are authorized. This process will include representation from the Office of the CIO, agency, state information security officer, and application development (when application changes impact or are impacted). This process must occur on a periodic basis with sufficient frequency to meet demands for changes to the environment;

(b) All records, meetings, decisions, and rationale of the change control group must be documented and securely stored for audit purposes. The agenda for this meeting is flexible but should generally address a review of at least the following: (1) change summary, justification and timeline; (2) functionality, regression, integrity, and security test plans and results; (3) security review and impact analysis; (4) documentation and baseline updates; and (5) implementation timeline and recovery plans;

(c) The agency is required to maintain baseline configuration documentation in use throughout the infrastructure. These baseline configuration documents shall be categorized as MODERATE IMPACT information, and secured appropriately. The baseline documents must be reviewed and updated on an annual basis or after any significant changes to the baseline have been installed; and

(d) All changes to the production infrastructure are required to be made by authorized personnel only, using access credentials assigned to that individual. Actions performed by these user credentials will be logged.

(2) Application Development. The following change management standards are required to be followed for application software systems that create, process, or store HIGH IMPACT or MODERATE IMPACT data:

(a) Application change management processes must be performed with assigned responsibilities to ensure all changes to application software are approved and documented. Change management teams will include appropriate application development staff and appropriate staff to represent state information security requirements;

(b) The change management processes may vary depending on the data application size and configuration, however all processes must include formal procedures with tools to support the documentation, review and approval for each change request;

(c) The change management processes will retain a documented history of the change process as it passes through the software development life cycle with documentation securely stored for audit purposes. Documentation should address a review of the following: (1) change summary, justification, and timeline; (2) functionality, regression, customer acceptance, and security test plans; (3) security review and impact analysis; (4) documentation and baseline updates; and (5) implementation timeline and recovery plans;

(d) Changes to software applications must be controlled and production installations must be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code must be implemented;

(e) Changes to production libraries should not be the same personnel who made the application changes unless documented procedures are in place that ensure the confidentiality, integrity, and availability of the data maintained in the production library; and

(f) Application development changes that impact IT infrastructure must be submitted to the infrastructure change management process for review, approval, and implementation coordination.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-202.pdf

8-203. Multi-function devices.

All multi-function devices used to process, store, or transmit data must be approved by the state information security officer or agency information security officer. The device must be configured and managed to adequately protect sensitive information.

Configuration and management of multi-function devices must include minimum necessary access to the processing, storing, or transmitting functions. All unnecessary network protocols and services must be disabled. Access controls must be in place, and administrator privileges must be controlled and monitored. Auditing and logging must be enabled. Access to the internal storage must be physically controlled. The devices must be securely disposed or cleansed when no longer needed. Software and firmware must be updated to the latest version supported by the vendor. All HIGH IMPACT or MODERATE IMPACT information must be encrypted in transit when moving across a WAN as well as when stored on the internal storage unit of the device. If the device stores information and is not capable of encrypting internal storage, then it must be physically secured or not used for HIGH IMPACT or MODERATE IMPACT information. Encryption technology must be approved by the state information security officer or agency information security officer.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-203.pdf

8-204. Email.

(1) Users of the state email system must not set up rules, or use any other methodology, to automatically forward emails to a personal or other account outside of the state network unless approved by the state information security officer and, if applicable, the agency information security officer.

(2) HIGH IMPACT or MODERATE IMPACT data must not be sent by email, or stored in the email system, unless it has been encrypted using technology approved by the state information security officer and, if applicable, the agency information security officer.

--

History: Adopted on July 12, 2017. Amended on March 12, 2020 and July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-204.pdf

8-205. Portable storage devices.

(1) HIGH IMPACT or MODERATE IMPACT data must not be stored on portable storage devices unless it has been encrypted using OCIO-approved technology.

(2) Portable storage devices must not be left in a vehicle unattended.

--

History: Adopted on July 12, 2017. Amended on November 10, 2022 and July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-205.pdf

8-206. Facilities; physical security requirements.

Agencies must perform a periodic threat and risk assessment to determine the security risks to facilities that contain state information, and implement reasonable and appropriate physical security measures to prevent and detect unauthorized access, theft, damage or interference.

Based on the threat and risk assessment, a multi-layered physical security perimeter must be established in agency environments where information or information assets are stored or where operational data centers, network wiring closets, or telephony connection equipment exists, or where printers that print HIGH IMPACT or MODERATE IMPACT information are used, and any other location where information may be in use or stored, such as file cabinets, microfiche storage areas, etc. The security layers create a perimeter that would require multiple methods of access control to gain entry. These layers could be in the form of an entry point with card key access, a staffed reception area, a locked cabinet or office, or another physical barrier. HIGH IMPACT or MODERATE IMPACT information must maintain at least two barriers to access at all times.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-206.pdf

8-207. Facilities; identification badges; visitors.

Only authorized individuals are allowed to enter secure areas of state facilities that contain information technology infrastructure. Those individuals will be issued an electronic ID badge. All authorized individuals are required to scan their ID badge before entry into these secure areas. ID badges must be visible, and staff are encouraged to question anyone they do not recognize who is not wearing a badge. Staff who forget their badges will be issued a temporary badge after management approval. Temporary badges must be returned at the end of the day.

All visitors are required to sign a visitor's log, including the following information: name, organization, signature, purpose of visit, date, time in, time out, and person to see. Visitors will be assigned a temporary badge that must be visible at all times. Visitors are not allowed into secure areas such as data centers. If it is necessary for a visitor to enter a secure area, they must be escorted at all times. When exiting the facility, the visitor must sign out and return the badge while under staff supervision.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-207.pdf

8-208. External service providers.

All external service providers with access to HIGH IMPACT or MODERATE IMPACT information must have a written agreement that includes the minimum security requirements necessary for the protection of this information. The state information security officer may inspect these external service provider arrangements to ensure compliance with state policies and requirements.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-208.pdf

8-209. Agency security planning and reporting.

Pursuant to the terms of certain federal data exchange agreements, state agencies may be required to maintain the following documentation:

(1) Information security strategic plan (section 8-210);

(2) System security plan (section 8-211); and

(3) Other information security documentation not covered by this section.

For agencies not subject to federal data exchange agreements, these planning documents are considered guidelines and recommended as best practice.

--

History: Adopted on July 12, 2017. Amended on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-209.pdf

8-210. Information security strategic plan.

Proper risk-based planning is critical to ensure the most appropriate projects are prioritized and funded by the state and its agencies. Information security planning is no exception. Planning for information protection should be given the same level of executive scrutiny at the state as planning for information technology changes. This plan should be updated and published on a biennial basis, and should include a two-year projection of key security business drivers and planned security infrastructure implementation. This plan is necessary to ensure that information security is viewed as a strategic priority, and is included as part of the overall planning process.

Contents of the information security strategic plan:

(1) Summary of the information security, mission, scope, and guiding principles;

(2) Analysis of the current and planned technology and infrastructure design, and the corresponding changes required for information security to stay aligned with these plans;

(3) Summary of the overall information risks assessments and current risk levels;

(4) Assessment of the current information security posture related to the future targeted posture, identified gaps, and high-level timeline necessary to close or mitigate those gaps;

(5) Summary of the policies, standards, and procedures for information security, and projected changes necessary to stay current and relevant;

(6) Summary of the information security education and awareness program, progress, and timeline of events;

(7) Summary of disaster recovery and business continuity activity and plans if the agency is required to maintain these documents by other requirement or policy;

(8) Analysis of the regulatory and contractual compliance environment, including potential new regulations or pending contractual requirements that will affect information security; and

(9) Proposed two-year timeline of events and key deliverables or milestones.

--

History: Adopted on July 12, 2017. Amended on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-210.pdf

8-211. System security plan.

The system security plan (SSP) provides an overview of the security requirements of the information system including all in-house or commercially developed and maintained systems and installations and to all external business partner systems and installations operated by, or on behalf of the state. The SSP describes the controls in place or planned for meeting those requirements and delineates responsibilities and expected behavior of all individuals who access the system. The SSP will describe the current controls in place to protect information at a level commensurate with the sensitivity level of the system.

The agency information security officer should develop or update the SSP in response to each of the following events: new system; significant system modification; increase in security risks/exposure; increase of overall system security level; serious security violation(s); or every three years (minimum) for an operational system.

Contents of the system security plan:

(1) System name and title, description and scope of system including each all in-house or commercially developed system and installations included in the SSP;

(2) Responsible organization: Name and contact information for business area responsible for the systems defined in the SSP. Decision authority for business functionality and business risks;

(3) Key contacts: Name and contact information for personnel who can address system characteristics and operation. IT maintenance personnel for the system, applications, and infrastructure;

(4) System operation status and description of the business process, including a description of the function and purpose of the systems included in the SSP;

(5) System information and inventory, including a description or diagram of system inputs, processing, and outputs. Include the information classification for all information processed, accessed, or exposed. Include a system network and workflow diagram;

(6) A detailed diagram showing the flow of information. Describe details where this data is stored, accessed, or processed and include details of the security mechanisms applicable to this type of data;

(7) Applicable laws, regulations, or compliance requirements: List any laws, regulations, or specific standards, guidelines that specify requirements for the confidentiality, integrity, or availability of information in the system;

(8) Review of security controls and assessment results that have been conducted within the past three years; and

(9) Information security risk assessment which includes identification of potential threat/vulnerabilities in the information system, analysis of planned or actual security controls, and potential impacts on operations, assets, or individuals.

--

History: Adopted on July 12, 2017. Amended on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-211.pdf

8-212. [Repealed.]

--

History: Adopted on July 12, 2017. Repealed on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-212.pdf

ARTICLE 3

ACCESS CONTROL

Section.

8-301. Remote access.

It is the responsibility of all agencies to strictly control remote access from any device that connects from outside of the state network to a desktop, server or network device inside the state network and ensure that employees, contractors, vendors, and any other agent granted remote access privileges to any state network utilize only approved secure remote access tools and procedures.

The following are the requirements for remote access:

(1) Requests for remote access must be reviewed and approved by the agency and the Office of the CIO;

(2) All remote sessions must use access control credentials and an OCIO-approved form of multi-factor authentication;

(3) All remote sessions must utilize OCIO-approved cryptographic mechanisms as defined by NIST 800-140 to protect the confidentiality and integrity of remote access sessions;

(4) All remote sessions over open public networks must use a VPN when connecting to the state network;

(5) All devices connecting to the network must have up-to-date anti-virus protection, active firewalls, and appropriate security patch levels equivalent to those provided for state equipment;

(6) All remote state owned or managed devices must be password protected and full-disk encrypted using OCIO-approved technology;

(7) All remote access sessions must be logged. The Office of the CIO or the agency will perform periodic monitoring of remote access sessions with random inspections of the user security settings and protocols to ensure compliance with this policy;

(8) Remote access logon failures must be logged. Credentials must be disabled after three (3) consecutive failed login attempts;

(9) Remote sessions must be locked after no more than 15 minutes of inactivity until the user re-establishes access with the appropriate credentials and authentication procedures;

(10) Mechanisms must be employed to ensure personally identifiable information, or other sensitive information (e.g., SSA, FTI, PII, PHI) cannot be downloaded or remotely stored; and

(11) Restricted data types cannot be accessed by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies, or military installations.

--

History: Adopted on July 12, 2017. Amended on November 4, 2021.
URL: https://nitc.nebraska.gov/standards/8-301.pdf

8-302. Passwords.

(1) Minimum Password Requirements. The following are the minimum password requirements for state government passwords:

(a) Must contain a minimum of eight characters;

(b) Must contain at least three of the following four: at least one uppercase character; at least one lowercase character; at least one numeric character; or, at least one symbol (!@#$%^&); and

(c) Cannot repeat any of the passwords used during the previous 365 days.

In addition to the minimum password complexity outlined above, additional password requirements are necessary for differing levels of data classification when authenticating users to networks or applications. The highest data classification level that a user has access to during an authenticated session will determine the additional password requirements. All employees and contractors of the state shall use a password that follows at least a confidential level of authentication when logging into a state network or application.

(2) Additional Access Requirements for HIGH IMPACT Information. Information that is classified as HIGH IMPACT requires the highest level of security. This includes root/admin level system information accessed by privileged accounts. A password used to access HIGH IMPACT information must follow the password complexity rules outlined in subsection (1), and must contain the following additional requirements:

(a) Multi-factor authentication;

(b) Expire after 60 days;

(c) Minimum password age set to 15 days; and

(d) Accounts will automatically be disabled after three unsuccessful password attempts.

(3) Additional Access Requirements for MODERATE IMPACT Information. Information that is classified as MODERATE IMPACT requires a high level of security. A password used to access MODERATE IMPACT information must follow the password complexity rules outlined in subsection (1), and must contain the following additional requirements:

(a) Expire after 90 days; and

(b) Accounts will automatically lock after three consecutive unsuccessful password attempts.

(4) Password Requirements for LOW IMPACT Information. Information that is classified as LOW IMPACT requires minimal level of security and need not comply with subsection (1).

Typically, this data would not include personal information but may carry special regulations related to its use or dissemination. LOW IMPACT data may also be data that is sold as a product or service to users that have subscribed to a service.

(5) Password Requirements for Accessing NO IMPACT Information. Information that is classified as NO IMPACT requires no additional password security and need not comply with subsection (1).

(6) Non-Expiring Passwords. Non-expiring passwords require a unique high level of security. Typically this information is confidential in nature and must follow the requirements in subsection (1). The additional requirements for access to HIGH IMPACT or MODERATE IMPACT data with a non-expiring password are:

(a) Extended password length to 10 characters;

(b) Independent remote identity proofing may be required;

(c) Personal security question may be asked;

(d) Multi-factor authentication; and

(e) Any feature not included on this list may also be utilized upon approval of the state information security officer.

(7) Automated System Accounts. Examples of automated system accounts include those that act as an intermediary between the public user and state systems, internal system to system interfaces, perform backups or run batch jobs. System account passwords shall expire after 365 days, unless mechanisms to restrict the use of those credentials to just the authorized service can be implemented and approval is granted by the state information security officer.

(8) Multi-User Computers. Multi-user computers include those computers in kiosks or training labs, where users have limited or restricted access to state resources. Agencies may use non-expiring passwords on multi-user computers. In these cases, mechanisms to ensure the user account with non-expiring passwords is unable to access HIGH IMPACT or MODERATE IMPACT information.

(9) System Equipment/Devices. Agencies may use non-expiring passwords for system equipment/devices. It is common for many devices (e.g., IP cameras, HVAC controls) in today's IT environment to utilize login capabilities to protect the device from unauthorized access. While many of these devices make use of a user ID and password in a manner like those found while authenticating a user, the distinction to be made is that the user ID is used to authenticate the device itself to the system and not a person.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-302.pdf

8-302.1. Public accounts; passwords.

This section sets forth the format, minimum requirements, and review procedures for public accounts accessing state resources. This section applies to all public accounts created for use within the State of Nebraska domain namespaces. Public accounts are accounts on state managed systems that are to be used by the general public and are not to be used by state employees or contractors to conduct state business.

(1) Information Access. A public account may only be used by the user to access their own information.

(2) Passwords. The following are the minimum requirements for public account passwords:

(a) Must contain a minimum of 12 characters;

(b) Must contain at least three of the following four complexity requirements: at least one uppercase letter; at least one lowercase letter; at least one numeric value; or, at least one special character; and

(c) Accounts must be locked temporarily after five failed password attempts.

(3) Review Process. Accounts with no successful login activity for a period of 24 months will be disabled. Accounts with no successful login activity for 26 months will be deleted.

(4) Misuse or Abuse. Any misuse or abuse of a public accounts will cause the account in question to be terminated.

--

History: Adopted on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-302.1.pdf

8-303. Identification and authorization.

(1) All employees and other persons performing work on behalf of the state, authorized to access any state information or IT resources, that have the potential to process, store, or access non-public information, must be assigned a unique identifier which resides in a State of Nebraska identity management system with the minimum necessary access required to perform their duties to align with the least privilege methodology.

(2) Staff are required to secure their user IDs from unauthorized use.

(3) Sharing user IDs is prohibited.

(4) To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical. Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, increased auditing and management supervision must be implemented. At a minimum, the audit of security must remain independent and segregated from the security function.

--

History: Adopted on July 12, 2017. Amended on March 10, 2022 and November 10, 2022.
URL: https://nitc.nebraska.gov/standards/8-303.pdf

8-304. Privileged access accounts.

Privileged access accounts include administrator accounts, embedded accounts used by one system to connect to another, and accounts used to run service programs. These accounts are used by systems and personnel to access sensitive files, execute software, load and configure policies and configuration settings, and set up or maintain accounts.

Due to the elevated access levels these accounts typically have, the following standards and procedures must be followed to minimize the risk of incidents caused by these accounts:

(1) All privileged access accounts must be assigned to an individual with an approved business need for the privileged access. These accounts must not be shared;

(2) All privileged access accounts must use OCIO-approved multi-factor authentication where technically possible;

(3) Service accounts must not be used to interactively log in to a system or resource;

(4) Default administrator accounts must be renamed, removed or disabled. Default passwords for renamed or disabled default administrator accounts must be changed;

(5) Default system account credentials for hardware and software must be either disabled, or the password must be changed. Use of anonymous accounts is prohibited, and unassigned accounts must be assigned to an individual prior to use. When no longer needed, the account must be disabled. At all times, the state requires individual accountability for use of privileged access accounts;

(6) Privileged access accounts must have enhanced activity logging enabled and reviewed at least quarterly;

(7) Privileged access through remote channels will be allowed for authorized purposes only and must include multi-factor authentication;

(8) Passwords for these accounts must be changed every 60 days;

(9) The password change process must support recovery of managed systems from backup media. Historical passwords should remain accessible in a history table in the event that they are needed to activate a backup copy of a system; and

(10) Privileged access accounts must be approved, provisioned, and maintained by the Office of the CIO.

Exceptions to this policy may be granted by the state information security officer.

--

History: Adopted on July 12, 2017. Amended on March 10, 2022 and November 10, 2022.
URL: https://nitc.nebraska.gov/standards/8-304.pdf

ARTICLE 4

NETWORK SECURITY

Section.

8-401. Network documentation.

The State of Nebraska encourages the use of its electronic communications infrastructure in support of its mission. However, this infrastructure must be well-managed and protected to ensure the security of Agency information. Therefore, all network devices that access the state internal network are required to adhere to these standards.

The Office of the CIO and agencies will implement a range of network controls to ensure the confidentiality, integrity, and availability of the data flowing across its trusted, internal network, and ensure the protection of connected services and networks. The Office of the CIO ensures that measures are in place to mitigate security risks created by connecting the state network to a third party network. All direct connections to the state network and direct connections between agencies must be authorized by the Office of the CIO.

Where an agency has outsourced a server or application to an external service provider (such as a web application), the agency must perform or have performed a security review of the outsourced environment to ensure the confidentiality, integrity, and availability of the state's information and application is maintained. For applications hosted by Nebraska.gov, the Nebraska State Records Board will perform the security review on behalf of all agencies.

All publicly accessible devices attached to the state network must be registered and documented in the IT inventory system. Additions or changes to network configurations, including through the use of external service providers, must be reviewed and approved through the Office of the CIO's change management process. Publicly accessible devices must reside in the Office of the CIO's DMZ unless approved by the Office of the CIO for legitimate business purposes.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-401.pdf

8-402. Network transmission security.

The following are network transmission security requirements:

(1) All encryption must be approved by the state information security officer. Any transmissions over unsecured networks (such as the Internet) that contain HIGH IMPACT or MODERATE IMPACT information must be encrypted using technology that is FIPS 140-2 compliant;

(2) Network scanning and monitoring is prohibited, unless prior approval is obtained from the Office of the CIO. If approved, scanning must be restricted to authorized and registered IP addresses only, and conducted by authorized personnel only;

(3) The Office of the CIO shall ensure that all networks and systems are monitored 24x7 with authorized tools (such as network based intrusion detection and prevention systems) and personnel to detect system anomalies or security events; and

(4) Passwords and SNMP community names may not be sent in clear text over open networks. All devices must use authorized encryption for access authorization to the state network. Access to the DMZ applications is exempt from this requirement.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-402.pdf

8-403. Network architecture requirements.

The following are network architecture requirements:

(1) All devices that store, access, or process HIGH IMPACT or MODERATE IMPACT information must not reside in the public tier, and must be protected by at least two firewalls. Firewalls must be placed at perimeter locations so that all critical systems are protected by multiple firewalls and monitoring systems;

(2) All publicly accessible devices must be located in an access-controlled environment, and access credentials must be managed by authorized personnel;

(3) All network devices that contain or process HIGH IMPACT or MODERATE IMPACT data must be secured with a password-protected screen saver that automatically locks the session after no more than 15 minutes of inactivity;

(4) Devices that include native host-based firewall software in the operating system must have the firewall activated and properly configured, unless the active firewall software compromises the usability of critical applications, or lessens the posture of other security systems;

(5) The state network will have an annual verification of all open ports, protocols, and services for publicly accessible systems;

(6) Any requests for public IP addresses or for additional open ports must be approved by the state information security officer;

(7) Staff will follow approved change control and configuration management procedures for network devices. Patches and hot-fixes recommended by network hardware or software vendors must be installed as soon as practical after testing; and

(8) Services and applications that will not be used must be disabled or removed if such action will not negatively impact operations. Protocols such as telnet, VNC, RDP, or others that do not actively support approved encryption should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-403.pdf

8-404. External connections.

Direct connections between the state network and external networks must be implemented in accordance with these policies and standards:

(1) Connections will be allowed only when external networks have been reviewed and found to have acceptable security controls and procedures, or appropriate security measures have been implemented to protect state resources. A risk analysis should be performed to ensure that the connection to the external network would not compromise the state network. Additional controls, such as the establishment of firewalls and a DMZ may be implemented between any third party and the state. All external connections will be reviewed on an annual basis;

(2) External network and workstation connections to the state network must have an agency sponsor and a business need for the network connection. The external network equipment must also conform to the state's security policies and standards, and be approved by the Office of the CIO; and

(3) Any connection between agency firewalls over public networks that involves sensitive information must use encryption to ensure the confidentiality and integrity of the data passing over the external network.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-404.pdf

8-405. Wireless networks.

Advances in wireless technology and pervasive devices create opportunities for new and innovative business solutions. However, security risks, if not addressed correctly, could expose state information systems to a loss of service or compromise of sensitive information. Everything transmitted over radio waves (wireless devices) can be intercepted. This represents a potential security issue.

The following are wireless network requirements:

(1) Agencies shall take appropriate steps, including the implementation of encryption, user authentication, and virus protection measures, to mitigate risks to the security of state data and information systems associated with the use of wireless network access technologies;

(2) No wireless network or wireless access point will be installed without the written approval of the Office of the CIO; and

(3) All wireless networks will be inspected annually by the state information security officer and agency information security officer to ensure proper security protocols are in place and operational.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-405.pdf

ARTICLE 5

SYSTEM SECURITY

Section.

8-501. System security; approved hardware and software; documentation.

(1) Only Office of the CIO approved hardware or software is permitted within the state's information technology infrastructure.

(2) All authorized hardware and software shall be inventoried and documented. Results shall be secured in an auditable fashion.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-501.pdf

8-502. Minimum user account configuration.

(1) User accounts must be provisioned with the minimum necessary access required to perform duties. Accounts must not be shared, and users must guard their credentials.

(2) User accounts must be provisioned to use OCIO-approved multi-factor authentication.

(3) Administrator level access is privileged and must be restricted to authorized IT personnel only. All privileged access accounts are subject to additional security, including multi-factor authentication, and enhanced auditing and logging of activity.

(4) Local accounts must be disabled unless required for business purposes, and in those cases, use of these accounts must be approved, tightly controlled, and monitored. All use of local accounts are required to be associated with an individual user.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-502.pdf

8-503. Minimum server configuration.

The state recognizes the National Institute of Standards and Technology (NIST) along with Center for Internet Security (CIS) Controls and Benchmarks as sources for recommended security requirements that provide minimum baselines of security for servers.

NIST and CIS provide instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All state system administrators should examine NIST and CIS Control documents when installing or configuring servers. The documents are not all inclusive, but rather meant as a means of prompting and guiding administrators through the installation process.

Agencies must comply with the following NIST standards, guidelines, and checklists: NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations; NIST SP 800-70, National Checklist Program for IT Products; and NIST SP 800-44, Guidelines on Securing Public Web Servers. Agencies should also strive to implement the highest tier possible for the CIS Controls and Benchmarks.

Server Hardening. All State of Nebraska servers are required to be hardened according to these standards. In addition, these servers must have a published configuration management plan as defined below and approved by the Office of the CIO. The following are server hardening standards:

(1) Servers may not be connected to the state network until approved by the Office of the CIO. This approval will not be granted for servers until these hardening standards have been met or risk levels have been accepted by agency management;

(2) The operating system must be installed by authorized IT personnel only, and all vendor supplied patches must be applied. All software and hardware components must be currently supported by the vendor. All unsupported hardware and software components must be identified and have a management plan for replacement that is approved by the Office of the CIO;

(3) All unnecessary software, system services, system and admin accounts, and drivers must be removed or disabled unless doing so would have a negative impact on the server;

(4) Logging of auditable events, as defined in NIST SP 800-53 control objectives, will be enabled. Audit logs will be secured and only accessible to accounts with privileged access and retained for a minimum of one year or be retained in accordance with federal and state guidance;

(5) Security parameters and file protection settings must be established, reviewed, and approved by the Office of the CIO;

(6) All system software must have security updates and patches applied when made available from the vendor. Priority setting of vulnerabilities will be based on impact to the agency and as referenced in the National Vulnerability Database (https://nvd.nist.gov);

(7) Servers will be scanned monthly for unauthorized software or unauthorized changes to the configuration baselines;

(8) Servers will be monitored with active intrusion detection, intrusion protection, and end-point security monitoring that has been approved by the state information security officer. This monitoring must have the capability to alert IT administrative personnel within 1 hour;

(9) Servers must be loaded from standardized processes and software. These processes and software shall be appropriately configured and protected, with integrity controls to ensure only authorized and documented changes are possible;

(10) All significant changes to servers must go through a formal change management and testing process to ensure the integrity and operability of all security and configuration settings. Significant changes must have a documented security impact assessment included with the change;

(11) Remote management of servers must be performed over secured channels only. Protocols that do not actively support approved encryption, such as telnet, VNC, and RDP, should only be used if they are performed over a secondary encryption channel, such as TLS; and

(12) Agencies must implement prevention techniques to protect against unauthorized data mining of information from public facing systems (e.g. Captcha).

--

History: Adopted on July 12, 2017. Amended on July 8, 2021.
URL: https://nitc.nebraska.gov/standards/8-503.pdf

8-504. Minimum workstation configuration.

Improperly configured workstations are at risk to be compromised. Without proper adherence to these workstation security standards, the state is at increased risk to have data lost, stolen, or destroyed. This standard is necessary to protect the state from unauthorized data or activity residing or occurring on state equipment. It is also necessary to reduce the likelihood of malicious activity propagating throughout the state networks or launching other attacks. All managed workstations that connect to the state's network are required to meet these standards. The Office of the CIO is responsible for maintaining these standards and for configuring and managing the hardware, software, and imaging processes for all managed workstations. Workstation standards should be securely maintained and stored in a centralized documentation library. The degree of protection of the workstation should be commensurate with the data classification of the resources stored, accessed, or processed from this computer. The following are minimum workstation configuration standards:

(1) OCIO-approved endpoint security (anti-virus) software, must be installed and enabled;

(2) The host-based firewall must be enabled;

(3) The operating system must be configured to receive automated updates;

(4) The system must be configured to enforce password complexity standards on accounts;

(5) Application software should only be installed if there is an expectation that it will be used for state business purposes. Application software not in use should be uninstalled;

(6) All application software must have security updates applied as defined by patch management standards and be of a vendor supported version;

(7) Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion;

(8) CIS Level 1 Controls should be maintained on all state managed workstations, where technically feasible;

(9) Shared login accounts are prohibited unless approved in advance and configured by IT. Shared login accounts are only acceptable if approved through the policy exception process and alternate mechanisms or access layers exist to ensure the ability to individually identify personnel accessing non-public information;

(10) Shared login accounts are forbidden on multi-user systems where the manipulation and storage of HIGH IMPACT or MODERATE IMPACT information takes place;

(11) Users need to lock their desktops when not in use. The system must automatically lock a workstation after 5 minutes of inactivity;

(12) Users are required to store all HIGH IMPACT or MODERATE IMPACT information on IT managed servers, and not the local hard drive of the computer. Local storage may only be used for temporary purposes when the data stored is not sensitive, and where loss of the information will not have any detrimental impact on the state;

(13) All workstations must be re-imaged with standard load images prior to reassignment; and

(14) Equipment scheduled for disposal or recycling must be cleansed following agency media disposal guidelines.

--

History: Adopted on July 12, 2017. Amended on November 10, 2022 and July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-504.pdf

8-505. [Repealed.]

--

History: Adopted on July 12, 2017. Repealed on November 10, 2022.
URL: https://nitc.nebraska.gov/standards/8-505.pdf

8-506. Minimum mobile device configuration.

All mobile devices accessing the state network or containing state information must be provisioned to meet these security policies and be approved by the Office of the CIO. All devices that will be connected to the state network must be logged with device type and approval date. The following are minimum mobile device configuration standards:

(1) Mobile devices must be shut down or locked when not in use. These devices must not be left unattended in a public access area. They must be locked in a secure cabinet or room, or kept on the person. Devices should not be shared;

(2) Mobile devices must not be left in a vehicle unattended;

(3) Storing HIGH IMPACT or MODERATE IMPACT information on any mobile device is prohibited unless arrangements and mechanisms for securing the data has been explicitly approved by the state information security officer. In those cases, the device must be encrypted using OCIO-approved technology;

(4) Personally owned mobile devices (e.g., smartphones and tablets) may be used for approved state purposes, including email, when configured to access the state information through a managed interface or sandbox only. Devices that are not configured to use the authorized interface are prohibited from accessing any state information, including email;

(5) The device must have security settings that block users from changing mandatory settings;

(6) Strong passwords are required, and passwords must change regularly per state policy regarding passwords;

(7) The device must lock after no more than 5 minutes of inactivity and must require the re-entry of a password or PIN code to unlock;

(8) After 10 unsuccessful password attempts, the device or the state container will be erased. In the event that the device becomes lost or stolen, the Office of the CIO must have the capability to remotely locate, lock, and erase the device;

(9) The device should have all data backed up at the state data center;

(10) Devices need to be cleared of all information from the prior user before being issued to a new user;

(11) The device OS must be up to date and patched. New versions of the OS must be vetted for security posture and supportability;

(12) Devices must be properly disposed of using mechanisms approved by the state information security officer. State data must be cleared and devices properly disposed of or recycled. The disposition process is required to be documented and periodically audited; and

(13) New devices are required to be configured and operate within established security guidelines and help desk support must be established before these devices can be operational. New devices need to be validated before being made available for users to request.

--

History: Adopted on July 12, 2017. Amended on November 10, 2022 and July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-506.pdf

8-507. System maintenance.

The following are system maintenance standards:

(1) All systems involved in the processing, storage, or access to any state information must be maintained per manufacturer specifications. Maintenance personnel must be approved for this activity by the state information security officer and must be briefed on the requirements for protecting sensitive information;

(2) Maintenance activity must be logged to include the date/time of the maintenance, activity performed, the person or organization who performed the maintenance, the name and department of the escort (if applicable), and a detailed list of any equipment removed or replaced during the maintenance. This list should include serial numbers, if applicable;

(3) Prior to removing any equipment from the secured environment to which it is assigned, the equipment must be approved for release and validated by the state information security officer that all non-public information has been encrypted, secured, or permanently deleted from the equipment. When equipment is returned, it must be inspected for unauthorized systems, settings, or services to ensure the integrity of the security systems before reloading data or placing back into the environment;

(4) All tools used for maintenance must be tested. The Office of the CIO must maintain a list of approved maintenance tools that is reviewed and updated at least annually;

(5) Nonlocal or remote maintenance must be approved in advance by the state information security officer or the Office of the CIO, and must also comply with all agency and Office of the CIO requirements for remote access;

(6) All remote maintenance activity must be logged and reviewed;

(7) Maintenance of agency-developed software must follow the state's change management process to ensure changes are authorized, tested and accepted by agency management. All known security patches must be reviewed, evaluated and appropriately prioritized;

(8) Vendor patches must be applied in an order based on organizational risk and must be applied within thirty days of receipt; and

(9) All vendor supplied software deployed and operational must be currently supported by the vendor.

--

History: Adopted on July 12, 2017. November 10, 2022.
URL: https://nitc.nebraska.gov/standards/8-507.pdf

ARTICLE 6

APPLICATION SECURITY

Section.

8-601. Application documentation.

To ensure that security is built into applications, security requirements, including the need for rollback arrangements, must be identified during the requirements phase of a project and justified, agreed to, and documented as part of the overall business case for the system. To ensure this activity is performed, the agency information security officer must be involved in all phases of the application development life cycle from the requirements definition phase, through implementation and eventual application retirement.

Controls in applications may be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level, and included in the agency's security standards documents. The security measures that are implemented must be based on the threat, vulnerability, and risk assessments of the information being processed and cost-benefit analysis.

Significant changes involving applications that store, access, or process HIGH IMPACT or MODERATE IMPACT information must go through a formal change management process. For recurring maintenance of these applications, an abbreviated change management process may suffice if that abbreviated process has been approved by the state information security officer.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-601.pdf

8-602. Application code.

Access to source code libraries for both agency business applications and operating systems must be tightly controlled to ensure that only authorized individuals have access to these libraries and that access is logged to ensure all activity can be monitored.

All application source code must be backed up and access restricted to authorized personnel only. Application changes are required to go through a software development life cycle process that ensures the confidentiality of information, and integrity and availability of source and executable code. Application changes must follow the change management process as defined in section 8-202.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-602.pdf

8-603. Separation of test and production environments.

Development software and testing tools can cause serious problems to the production environment if separation of these environments does not exist. Separation of the development, test and production environments is required, either on physically separate machines or separated by access controlled domains or directories. Processes must be documented and implemented to govern the transfer of software from the development environment to the production platform. Each agency must consider the use of a quality assurance environment where user acceptance testing can be conducted. The following controls must be considered:

(1) Access to compilers, editors and other system utilities must be removed from production systems when not required;

(2) Logon procedures and environmental identification must be sufficiently unique for production testing and development;

(3) Access to systems and business applications must be restricted to those individuals who have a business need to access those resources in the performance of their job responsibilities; and

(4) It is recognized that at times, business or technical requirements dictate the need to test with live data. In those cases, it is mandatory to have approval from the state information security officer, and to implement production-class controls in the applicable test environment to protect that information.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-603.pdf

8-604. Application development.

The following standards are required to be followed for agency developed application software that create, process, or store HIGH IMPACT or MODERATE IMPACT data:

(1) The agency must establish an application change management processes with assigned responsibilities to ensure all changes to applicable application software are approved and documented. Change management teams will include appropriate application development staff and appropriate staff to represent state information security requirements;

(2) The change management processes may vary depending on the data application size and configuration, however all processes must include formal procedures with tools to support the documentation, review and approval for each change request;

(3) The change management processes must retain a documented history of the change process as it passes through the application development life cycle with documentation securely stored for audit purposes. Documentation should address a review of the following: change summary, justification, and timeline; functionality, regression, integrity, and security test plans and results; security review and impact analysis; documentation and baseline updates; and implementation timeline and recovery plans;

(4) Changes to software applications must be controlled and production installations must be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code must be implemented;

(5) Changes to production libraries should not be the same personnel who made the application changes unless documented procedures are in place which ensure the confidentiality, integrity, and availability of the data maintained in the production library;

(6) Application development changes that impact agency IT infrastructure must be submitted to the Infrastructure Change Control Team for review, approval, and implementation;

(7) The security requirements of new applications must be established, documented and tested prior to their acceptance and use. The agency information security officer must ensure that acceptance criteria are utilized for new applications and upgrades. Acceptance testing must be performed to ensure security requirements are met prior to the application being migrated to the production environment;

(8) All applications are required to maintain up-to-date documentation that includes an assessment of security threats and impacts, and a detailed description of the data handling with its accurate classification;

(9) Applications that provide user interfaces must have an appropriate warning banner displayed, applicable to the data being accessed (e.g., PHI, FTI, PII);

(10) Application credentials, where possible, should be inherited from the state managed authentication source. If that is not possible, credentials should have the same level of management and approval as other agency access credentials; and

(11) Applications must be configured such that HIGH IMPACT or MODERATE IMPACT data will be encrypted when transmitted outside the agency internal network.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-604.pdf

8-605. Web applications and services.

Internet-facing systems are diverse to meet a multitude of different needs. Therefore, information exposures by these systems differ, as do threats. Security controls should be implemented to mitigate meaningful risks to an application. Because every system is different, the web application developer is the most knowledgeable about the system and the risks it faces.

This standard establishes a baseline of security requirements for all state websites, web services, and all vendor supported or hosted web applications. All applications that are Internet-facing are required to securely maintain documentation and evidence of compliance levels with this standard.

This standard is based on the research and recommendations from the SysAdmin, Audit, Network, and Security (SANS) Institute and the Open Web Application Security Project (OWASP). The following are the security standards for web applications and services:

(1) Consider the threats, vulnerabilities, and risks to your application. If you are unsure, follow the threat risk methodology published by OWASP (http://www.owasp.org/index.php/Threat_Risk_Modeling);

(2) Consider and implement additional security controls to ensure the confidentiality, integrity, availability of the information based on the unique threats and exposures that face your application;

(3) Implement error-handling in a manner that denies processing on any failure or exception;

(4) All input fields must be validated before accepting. Input should be checked to prevent the program from executing malicious code. Input length must be validated to determine if it is within the predetermined minimum and maximum ranges. Input values should be screened for valid data types (e.g., number or character only, no special characters);

(5) Output fields must be sanitized to ensure the output does not reveal too much information that could be used by malicious intent (e.g., default system-generated messages should be translated by the application). If invalid user input is encountered, the error message should not reveal the specific component which caused the error. Messages should be general in nature, and not reveal anything more than what is necessary;

(6) The identity of the user must be authenticated if the application has access to non-public information. All user credentials and passwords must meet the security policy requirements for strength, change, and history. User access and capability must be limited to the functions required for the authorized access level only;

(7) The requesting and granting of user accounts must include an approval process that validates the user and the minimum necessary access levels;

(8) Establish security settings commensurate with the type of access;

(9) All external systems (including web services), which require access to the application, must be authenticated and permissions checked before the external system becomes trusted;

(10) All password entry fields should not "echo" the password in readable text when it is entered. Auto-complete of password fields should be disabled;

(11) All sessions should be terminated when the user logs out of the system;

(12) If a web application needs to store temporary or session-related information that is HIGH IMPACT or MODERATE IMPACT outside of the secured agency internal network, that information must be encrypted in all cases – whether stored or in transit. Encryption technology must be approved by Office of the CIO;

(13) All web applications are required to have a security scan and test of the application on a recurring basis as determined by the state information security officer. Higher risk or impact applications should be tested annually. This test shall be coordinated and supervised by the state information security officer, agency information security officer, and IT management. Some packaged web applications where the package's architecture inherently protects the application from security risks, may have reduced testing requirements versus other web applications; and

(14) The anonymous public facing environment shall contain publicly approved content only. All non-public data and applications shall be segregated by additional firewalls and network monitoring.

[Other application security recommendations and development guides can be reviewed at the OWASP (https://www.owasp.org/index.php/Category:OWASP_Guide_Project) and SANS (http://www.sans.org/top25-software-errors/) websites.]

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-605.pdf

8-606. Staff use of cloud storage websites.

Accessing online cloud storage websites (such as Dropbox, Google Drive, etc.) is a security risk that will be restricted based on an employee's job functions. Use of these systems for any state purposes is prohibited unless approved by the employee's supervisor or manager. Even if approved, it is prohibited to process or store any HIGH IMPACT or MODERATE IMPACT information with these services, unless the storage is encrypted with approved technology, and has been approved in advance by the state information security officer.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-606.pdf

8-607. Cloud computing.

(1) Cloud computing, defined.

This standard incorporates the following definition from the National Institute of Standards and Technology (NIST SP 800-145, September 2011 [footnotes omitted]):

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprised of multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound

together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Other Deployment Models [not part of the NIST definition]:

Government community cloud. A community cloud infrastructure provisioned solely for use by federal, state, and/or local government.

State cloud. The private cloud infrastructure provided by the Office of the CIO.

(2) Standard.

(a) The following table contains the acceptable uses of cloud computing by state agencies. The classification of the data to be processed or stored using cloud computing determines the acceptable options. If there is a mix of data classifications, the most restrictive data classification must be used.

Data Classification	Cloud Deployment Models					
	State Cloud	Private Cloud	Government Community Cloud	Community Cloud	Public Cloud	Hybrid Cloud
HIGH IMPACT	✓	△	△	△	⊘	△
MODERATE IMPACT	✓	△	✓	△	⊘	△
LOW IMPACT	✓	✓	✓	✓	✓	✓
NO IMPACT	✓	✓	✓	✓	✓	✓

(✓) means an approved deployment model for cloud computing;
(⊘) means an unapproved deployment model for cloud computing; and
(△) means prior approval by the Office of the CIO is required.

(b) Prior approval process. An agency requesting prior approval of a cloud computing service must submit a service request to the Office of the CIO Service Desk. The request should provide detailed information about the cloud deployment model and data to be processed or stored using cloud computing. The Office of the CIO will respond to the request within four business days. The Office of the CIO may approve the request, approve the request with conditions, deny the request, or request additional information.

(c) Exemption for existing services. Cloud computing services in use on December 31, 2017, are exempt from the requirements of this section. The exemption for an existing service ends when either: (1) the current term of the agreement for such service expires; or (2) there are significant changes to the service.

(d) FedRAMP compliance. If the cloud service provider (CSP) does not have an official FedRAMP certification by an accredited third-party assessor organization (3PAO) and the CSP may store or process any HIGH IMPACT or MODERATE IMPACT data, the following conditions must be met or addressed in an agreement with the CSP:

(i) The cloud service provider or third-party host (CSP/3PH) must provide evidence of secure storage of access credentials that are at least equal to that of state's internal systems;

(ii) Access to the cloud service must require multi-factor authentication based on data classification levels;

(iii) De-provisioning of credentials must occur within two (2) hours of de-provisioning of the internal system credentials;

(iv) Information must be encrypted using IT approved technology for information in transit as well as information stored or at rest;

(v) Encryption key management will be controlled and managed by the state unless explicit approval for key management is provided to CSP/3PH by the agency;

(vi) All equipment removed from service, information storage areas, or electronic media that contained state information must have the information purged using appropriate means. Data destruction must be verified by the state before allowing that equipment, information storage space, or media to be destroyed or assigned for reuse. A certificate of destruction must be provided for equipment that has been destroyed;

(vii) CSP/3PH must provide vulnerability scanning and testing on a schedule approved by the state information security officer. Results will be provided to agency;

(viii) Patch management of hardware and software at the CSP/3PH are required to meet the same standards that are required at state;

(ix) CSP/3PH must meet all state requirements for chain of custody and information breach notification. CSP/3PH will maintain an incident management program that notifies the state within one (1) hour of a breach;

(x) CSP/3PH will provide evidence of audit and assessment of the security of the service environment, and will agree to reasonable inspection of such security by gency-authorized parties;

(xi) CSP/3PH is required to advise the state on all geographic locations of stored state information. CSP/3PH will not allow state information to be stored or accessed outside the United States. This includes both primary and alternate sites;

(xii) Privileged access roles at the CSP/3PH are required to meet the same vetting standards of privileged access personnel at the state, such as background checks, etc.;

(xiii) CSP/3PH's must have SLAs in place that clearly define security and performance standards;

(xiv) CSP/3PH will provide adequate security and privacy training to its associates, and provide the state information security officer with evidence of this training;

(xv) CSP/3PH will provide the state with the functionality to conduct a search of the data to meet public records requests; and

(xvi) Before contracting with a CSP/3PH, the state shall have proactive records planning in place to ensure the ability to have timely and actual destruction of records in accordance with Department record retention policies.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-607.pdf

8-608. Low-code/no-code and containerization development.

Low-code/no-code and containerization development platforms are types of visual software development environments that allow enterprise developers to drag and drop application components, connect them together and create mobile or web apps and microservices. These types of environments allow for the dynamic allocation of resources. While these types of environments allow for swift and agile development without the necessity to write fully coded applications, the platforms also present architectural, security and governance challenges. The following are low-code/no-code and containerization development standards:

(1) All projects involving low-code/no-code in the cloud must be reviewed and approved by the OCIO Cloud Review Board;

(2) Low-code/no-code projects must maintain compliance with all applicable standards; and

(3) All vendor supplied software deployed and operational must be supported by the vendor.

--

History: Adopted on November 10, 2022.
URL: https://nitc.nebraska.gov/standards/8-608.pdf

ARTICLE 7

AUDITING AND COMPLIANCE

Section.

8-701. Auditing and compliance; responsibilities; review.

It is the responsibility of the state information security officer to ensure an appropriate level of security oversight is occurring at all potential exposure points of state and agency systems and operations so that the state has reasonable assurance that the overall security posture continuously remains intact. The state information security officer and agency information security officer have the responsibility to ensure the overall security program meets state and federal legal requirements.

The state information security officer will establish and manage an entity-wide oversight and compliance function. This will include, at a minimum, appropriate information security oversight at key points within the technology acquisition process, hardware and software change management process, and the contract management process when changes involve access to or potential exposure of HIGH IMPACT or MODERATE IMPACT information.

Compliance with this policy is mandatory. Any compromise or suspected compromise of this policy must be reported as soon as reasonably possible to appropriate agency management and the state information security officer.

An agency review to ensure compliance with this policy and applicable NIST SP 800-53 security guidelines must be conducted at least annually.

The state information security officer may periodically review agency compliance with this policy and the related NIST control framework. Such reviews may include: (1) reviews of the technical and business analyses required to be developed pursuant to this policy; and (2) project documentation, technologies or systems which are the subject of the published policy or standard.

These additional reviews may occur due to significant changes in technical infrastructure, or to validate corrective actions after a security incident. All identified gaps or deficiencies must be documented in an agency security corrective action plan that shall be made available to the state information security officer as necessary. This plan is classified as a HIGH IMPACT information document, and should contain detailed descriptions of the security deficiencies, recommended remediation or mitigation activity, key milestones and target dates, and responsible parties. This plan should be a regular item for review by senior agency and Office of the CIO management to ensure acceptable progress is being made on mitigating or remediating security gaps.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-701.pdf

8-702. Awareness and training.

(1) The state provides information technology resources to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations subject to state government policies and applicable state and federal laws. It is the responsibility of all staff to protect information resources and ensure that such resources are not misused.

An information security awareness program must be developed, implemented, documented, and maintained that addresses the security education needs of the state. To ensure staff is knowledgeable of security procedures, their role and responsibilities regarding the protection of agency information and the proper use of information processing to minimize security risks, all staff with access to agency information must receive security awareness training, which must be reinforced at least annually. Technical staff must be trained to a level of competence in information security that matches their duties and responsibilities.

(2) New Hire and Refresher Training. All new hires must complete security training, including information about this policy, as part of their orientation. On an annual basis, all staff must complete a security and privacy training session. The state will maintain records of all attendance for new hire and refresher training.

(3) Simulated Phishing. Phishing is a significant threat vector for the state's technology environment. To aid in mitigating this threat and raise awareness of the tactics and techniques used by malicious actors to compromise credentials, simulated phishing campaigns will be conducted at least annually by the Office of the CIO. Anonymized reports may be provided on a per agency basis upon request.

(4) Security Briefings. Management should periodically incorporate information security topics into their meetings with staff. Additionally, the state information security officer may require periodic security briefings to selected audiences when circumstances require, such as responding to a gap in security policy or addressing recurrence of security incidents.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-702.pdf

8-703. Security reviews; risk management.

(1) This policy is based on the NIST SP 800-53 security controls framework. Pursuant to that framework, the state must conduct an annual review of the information technology environment to ensure compliance with these standards. The security controls that are to be inspected are organized into control families within three classes (management, operational, and technical).

The state information security officer will facilitate and oversee an annual security control assessment. This assessment will cover at least 1/3 of the control areas defined in the NIST SP 800-53 security controls, such that over a three-year timeframe all control areas will have been assessed. This review must be conducted for each major system used within the state, and must include all infrastructure and peripheral processes that are used to support state business processes.

(2) Unscheduled Risk Assessments. Unscheduled risk assessments may be performed at the discretion of the state information security officer or agency information security officer, typically when circumstances require additional oversight, such as after a security incident, increased security threat, or significant changes to the IT infrastructure. These assessments are flexible in nature, and are intended to review specific elements that have been identified as exception-based or high priority. These reviews can also be performed to validate the appropriate remediation or mitigation of a previous finding.

The security officer shall document the business area, reason for the review, scope of inspection, and dates of the review in the corrective action planning documentation. All findings and results will also be documented in the security corrective action plan.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-703.pdf

8-704. Logging.

All systems that handle HIGH IMPACT or MODERATE IMPACT information, allow interconnectivity with other systems, or make access control (authentication and authorization) decisions, must record and retain audit-logging information sufficient to answer the following questions:

(1) What activity was performed?

(2) Who or what performed the activity, including on what system the activity was performed?

(3) What the activity was performed on (object)?

(4) When was the activity performed?

(5) What tool(s) was the activity performed with?

(6) What was the status (such as success vs. failure), outcome, or result of the activity?

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-704.pdf

8-705. Logging; format, storage, and retention.

The state is required to ensure the availability of audit log information that is subject to federal audit by allocating sufficient audit record storage capacity to meet policy requirements. Office of the CIO and the agency IT teams shall perform annual capacity planning and trend analysis to reduce the likelihood of such capacity being exceeded. The capacity and utilization of log files must be regularly monitored and reported, and action will be taken to keep an approved level of free space available for use. Automated notification of agency or Office of the CIO personnel must occur if the capacity of log files reaches defined threshold levels, or the audit logging system fails for any reason.

The audit logging process is required to provide system alerts to appropriate agency or Office of the CIO personnel in the event of an audit processing failure (e.g., shut down information system, unintended overwriting of the oldest audit records, stop generating audit records). All system logs must be sent to a central log review system that is protected from unauthorized access and is backed up for availability and integrity purposes. All log files subject to federal audit requirements must be retained for seven years.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-705.pdf

8-706. Logging; auditable events.

Security safeguard regulations require logging and reviewing events that are determined to have a moderate or above level of risk. Auditable events may be incorporated into system auto logs and change management documents. The following events should be logged and reviewed on a weekly basis:

(1) Log on and off the system;

(2) Change of password;

(3) All system administrator commands, while logged on as system administrator;

(4) Switching accounts or running privileged actions from another account (e.g., Linux/Unix SU or Windows RUNAS);

(5) Creation or modification of super-user groups;

(6) Subset of security administrator commands, while logged on in the security administrator role;

(7) Subset of system administrator commands, while logged on in the user role;

(8) Clearing of the audit log file;

(9) Startup and shutdown of audit functions;

(10) Use of identification and authentication mechanisms (e.g., user ID and password);

(11) Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);

(12) Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system;

(13) Changes made to an application or database by a batch file;

(14) Application-critical record changes;

(15) Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);

(16) All system and data interactions concerning FTI;

(17) Additional platform-specific events, as defined by agency needs or requirements;

(18) Detection of suspicious or malicious activity such as from an intrusion detection or prevention system (IDS/IPS), anti-virus system, or anti-spyware system; and

(19) Physical entrance or access to secured and restricted areas or facilities where system and network infrastructure reside.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-706.pdf

8-707. Logging; audit log contents.

Audit logs must contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The logs must identify or contain at least the following elements, or enough information in which to infer the following elements with reasonable assurance:

(1) Type of action (e.g., authorize, create, read, update, delete, and accept network connection);

(2) Subsystem performing the action (e.g., process or transaction name, process or transaction identifier);

(3) Identifiers (as many as available) for the subject requesting the action (e.g., user name, computer name, IP address, and MAC address). Note that such identifiers should be standardized to facilitate log correlation;

(4) Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time;

(5) Whether the action was allowed or denied by access-control mechanisms;

(6) Description or reason-codes of why the action was denied by the access-control mechanism, if applicable; and

(7) Depending on the nature of the event that is logged, there may be other information necessary to collect.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-707.pdf

8-708. Logging; audit review, monitoring, findings and remediation.

(1) Security safeguard regulations require regular inspections of system audit logs for indications of inappropriate or unusual activity. Additionally, these logs must be reviewed by authorized personnel to facilitate investigations of suspicious activity or suspected violations. All reports of findings must be reported to appropriate officials who will prescribe the appropriate and necessary actions. Logs must be reviewed as follows:

(a) Logs of suspicious activity must be reviewed as soon as possible;

(b) Logs of system capacity and log integrity must be reviewed on a weekly basis;

(c) Logs of privilege access account creation or modification must be reviewed on a weekly basis; and

(d) All other logs must be reviewed at least monthly.

(2) When possible, the agency or Office of the CIO will employ automated mechanisms to alert the Office of the CIO, state information security officer, or agency information security officer when inappropriate or unusual activities with security implications are discovered. Any automation used for log analysis must not change the underlying log structure. It is acceptable for log analysis tools to extract data for analytical review, if the original audit logs remain unchanged and secured.

(3) All relevant findings discovered because of an audit log review must be listed in the appropriate problem tracking system or the corrective action planning process to ensure prompt resolution or appropriate mitigating controls. All results and findings generated by the audit or review process must be provided to appropriate agency management within one week of completion. This report should be considered MODERATE IMPACT information.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-708.pdf

8-709. Logging; application logging review and monitoring.

All state applications must provide logging for security events. Application logs are invaluable data for identifying security incidents, monitoring policy violations, establishing baselines, providing information about problems and unusual conditions, contributing additional application-specific data for incident investigation which is lacking in other log sources, and helping defend against vulnerability identification and exploitation through attack detection.

Application logging content must be part of the overall system analysis and design activity, and should consider:

(1) Application process startup, shutdown, or restart;

(2) Application process abort, failure, or abnormal end;

(3) Significant input and output validation failures;

(4) Business process monitoring (e.g., activity abandonment, transactions, connections, information requests);

(5) Audit trails (e.g., data addition, modification and deletion, data exports);

(6) Performance monitoring (e.g., data load time, page timeouts);

(7) Compliance monitoring and regulatory, legal, or court ordered actions;

(8) Authentication and authorization successes and failures;

(9) Session management failures;

(10) Use of higher-risk functionality (e.g., addition or deletion of application credentials, changes to privileges, assigning users to tokens, adding or deleting tokens, submission of user-generated content - especially file uploads); and

(11) Suspicious, unacceptable or unexpected behavior.

Application logs must be reviewed at least monthly. Corrective actions to address application deficiencies must be managed through the application development process or the applicable corrective action planning process.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-709.pdf

ARTICLE 8

VULNERABILITY AND INCIDENT MANAGEMENT

Section.

8-801. Incident response.

Computer systems are subject to a wide range of mishaps from corrupted data files, to viruses, to natural disasters. These incidents can occur at any time of the day or night. Many mishaps are fixed through day-to-day operating procedures, while more severe mishaps are addressed in other ways (e.g., disaster recovery plans). Responses to an incident can range from recovering compromised systems to the collection of evidence for a variety of forensic requirements. Preparation and planning for incidents, and ensuring the right resources are available, are critical to the state's ability to adequately detect, respond and recover from security incidents.

The security policy requires the establishment and maintenance of a computer security incident response capability that is in effect 24x7. This document identifies key steps for reporting security incidents and establishes formal reporting requirements for all such instances to the state's senior management and agency officials responsible for reporting to federal offices.

These procedures also describe the way Office of the CIO or agency technical staff will aid the in the eradication, recovery, and permanent remediation of the root cause of the incident. This is important to preserve as much evidence as practical while keeping in mind that prevention of damage is of the highest priority.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-801.pdf

8-802. Incident response plan.

All agencies that process, store, or access HIGH IMPACT or MODERATE IMPACT information are required to maintain an incident response plan. This plan must include operational and technical components, which provide the necessary functions to support all the fundamental steps within the incident management life cycle, including the following:

(1) Preparation.

(a) A security incident is any adverse event whereby some aspect of the state infrastructure is threatened (e.g., personal violation, loss of data confidentiality, disruption of data integrity, denial of service, security breach). It is important to note that even if there is no evidence of information being accessed by unauthorized personnel, exposing sensitive information in an unsecure manner is considered a security incident. For example, any unencrypted email containing HIGH IMPACT or MODERATE IMPACT information (e.g. Federal Tax Information, Personally Identifiable Information) sent outside the secured state network is a security incident and should be reported as such.

(b) All security incidents must be reported to the state information security officer, agency management, and the Office of the CIO Service Desk immediately. Security incidents will be tracked by the state information security officer. Any state staff who observe, experience, or are notified of a security incident, should immediately report the situation to the agency information security officer, state information security officer or the Office of the CIO Service Desk, but at the very least to their supervisor. All state management are responsible to ensure that their staff understand that awareness of the incident are to be reported immediately.

(c) State Information Security Officer and Agency Information Security Officer.

The security officers are responsible for assembling, engaging, and overseeing the incident response team. They will coordinate the management of security incidents and any identified follow-up activity, remediation, or countermeasures. They are also responsible for taking lead with information technology personnel to perform analysis and triage of incident impact and reportable conditions.

The security officers will finalize and sign off on any security incident reports, and determine follow-up activity, root cause analysis, long term mitigation, and updates to the security awareness training.

Agency information security officers are also responsible for ensuring that all technical areas within the agency have an understanding and ability to meet this standard. They are required to

perform education and training of this standard to all applicable agency personnel, and then test the incident response process annually.

(d) Incident Response Team.

The state information security officer will identify key personnel who will serve as members of the state incident response team. This team will be made up of knowledgeable staff that can rapidly respond to, manage, and support any suspected incident to minimize damage to state information systems, networks and data by identifying and controlling the incident, properly preserving evidence, and reporting to appropriate entities. This team may change from time to time, depending on the nature of the incident and the skills necessary to recover from it. Agencies may also identify additional incident response teams for their specific environment. The state information security officer or agency information security officer will maintain a contact list which includes the names, telephone numbers, pager numbers, mobile telephone numbers, email addresses, organization names, titles, and roles and responsibilities for all potential key incident response resources. Key responsibilities for the incident response team include:

(i) The state's priority is "prevention over forensics." In other words, do not allow a damaging incident to continue so that additional evidence may be collected;

(ii) Conduct the initial triage. Perform a damage and impact assessment and document the findings;

(iii) Report to agency management on a regular schedule with status and action plans;

(iv) Maintain confidentiality of the circumstances around the incident;

(v) Follow procedures to maintain a chain of trust and to preserve evidence;

(vi) Initiate the root cause analysis; bring in other resources as necessary; and

(vii) Initiate return to normal operations; bring in other resources as necessary.

(e) Incident Management Procedures.

Incident management procedures require, first and foremost, prevention of damage from the incident over forensics. This means that the priority is to shut off or terminate any potential damaging threat. It is strongly desired to perform this action in a manner that allows for detailed forensics or preservation of evidence, but if there is ANY doubt, all state personnel, whether employees or contractors, are required to disable the threat immediately. Following the assessment and termination of the threat, the next priority is containment, followed by recovery actions, damage determination, report documentation, lessons learned, and implementation of corrective actions.

All communication related to the incident should be carefully managed and controlled by the Office of the CIO and agency senior management. All personnel involved in an incident management support activity will communicate only with the parties necessary for incident analysis or recovery activity, and to the state information security officer, Office of the CIO, or the agency information technology team. No other communication, unless explicitly authorized, is allowed.

A security incident report is classified as HIGH IMPACT information.

(f) Incident Management Training and Testing.

Annually, the state information security officer and agency information security officers shall provide training for appropriate identification, management, and remediation of an incident and shall facilitate a simulated incident response and recovery test for the state or agency security incident response team. This test will simulate a variety of security related incidents.

(2) Incident Triage and Identification.

As soon as an incident is suspected, personnel qualified and designated to respond shall be notified to take immediate action, determine incident impact, file a ticket, or prepare a report.

Initial triage will be conducted by the state information security officer/agency information security officer, Office of the CIO Service Desk, or the information technology team to understand the scope and impact of the incident and initiate appropriate action. Once an incident has been identified and reported, the state information security officer/agency information security officer will assume oversight of the incident response and will continually assess the incident conditions and determine if escalation of response actions is appropriate. Prevention of damage is given priority over forensics of incident source. Therefore, the state information security officer/agency information security officer and IT management may quarantine any potentially threatening system and terminate any threatening activity. The state information security officer will ensure that a security incident report is completed for all incidents.

For more complicated incidents that may require further analysis, the incident response team will be assembled via direction from the state information security officer, Office of the CIO, agency information security officer, or agency IT management. This team will take over the triage and impact assessment process.

A damage analysis of security incidents is to be initiated immediately after assessment by the state information security officer or the incident response team. They will determine if the incident impacts organizations outside of the agency's internal network. They will also determine if any reportable conditions, such as unauthorized disclosure of HIGH IMPACT or MODERATE IMPACT information exists. If the incident appears to have any citizen information compromised, immediate notification to the agency management, state information security officer, and agency information security officer is required. Agency management will oversee and coordinate all communication actions.

All forms of unauthorized disclosure of HIGH IMPACT or MODERATE IMPACT information, including the potential for unauthorized disclosure (such as information spillage), will be considered incidents. Information spillage refers to instances where either HIGH IMPACT or MODERATE IMPACT information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, an incident has occurred and corrective action is required.

(3) Incident Containment.

Any IT resources that are engaged in active attacks against other IT resources must be isolated and taken off the state network immediately. Incidents involving the exposure, or potential exposure, of HIGH IMPACT or MODERATE IMPACT information to unauthorized parties must also be contained immediately. Other compromises must be contained as soon as practical, considering impacts of service interruptions, recovery of equipment, and potential impacts of the incident itself.

Containment can be achieved by immediately disconnecting the resource from the network, revoking user access, or other means as appropriate. The state information security officer has the authority to coordinate with the Office of the CIO to block compromised services and hosts that present a threat to the rest of the state network. Notifications of outages or service interruptions will follow normal Office of the CIO or agency procedures if possible, but will not delay the outage or interruption if an attack or breach is underway or if the threat of an attack or breach is imminent.

(4) Incident Communication.

Reportable conditions, such as the breach of PHI, PII or FTI, require notification within specific timeframes as defined in state and federal law. It is the responsibility of the state information security officer and agency information security officers to understand these requirements and ensure the state and agency remain compliant in the event of a reportable incident.

Additionally, communication during a security incident must be carefully controlled to ensure that information that is disclosed is accurate, timely, and provided only to appropriate audiences.

It is the responsibility of the state information security officer, agency information security officer, Office of the CIO, and agency management to ensure that all communication regarding any security incident is managed and controlled.

(5) Preservation of Evidence.

In the event of a discovery of a breach of system security protections, an internal security investigation must be properly performed to preserve evidence. If the incident involves any type of law enforcement, the incident response team will work with law enforcement to secure the potential evidence without reviewing additional content. Network hardware, software or data may be considered potential evidence.

The chain of custody steps that should be taken to preserve all potential evidence in the event of a security breach are as follows:

(a) If possible, isolate the system from the network, either physically (unplug the network cable), or logically. Do NOT power the system off. Evidence in system memory may be lost;

(b) If the system cannot be taken off the network, take pictures and screenshots;

(c) Notify the agency information security officer immediately after initial steps, but no later than one hour after becoming aware of the possible incident;

(d) Make a bit copy of the drive before investigating (e.g., opening files, deleting, rebooting);

(e) Dump memory contents to a file;

(f) Label all evidence; and

(g) Log all steps.

(6) Incident Documentation and Root Cause Analysis.

An incident report is required for all incidents except those classified as having a low impact to the state network. The incident report should include entry of the root cause, actions taken and any remediation or mitigation strategy to reduce the risk of recurrence. Depending on the nature of the security incident, a post-mortem meeting may be conducted.

Documentation of information is critical in situations that may eventually involve authorities as well as provides documentation of the actions taken to resolve the event. Incident reports are HIGH IMPACT information.

A formal root cause analysis must be performed within two weeks of the occurrence of the incident. This analysis should identify the core issues of the incident in the affected environment and actions that can be taken to address these issues. This can include physical, logical, or environmental changes, operational or administrative control changes, or enhanced training, education, or awareness programs.

(7) Incident Recovery and Permanent Remediation.

The incident response team, working with technology, application and data owners, shall evaluate and determine when to return compromised systems to normal operations. Access to compromised systems will be limited to authorized personnel until the security incident has been

contained and root cause mitigated. Analysis and mitigation procedures must be completed as soon as possible, recognizing state systems are vulnerable to other occurrences of the same type.

The Office of the CIO, state information security officer, and agency information security officer shall define and prioritize the requirements to be met before returning an affected or compromised system to normal operations.

Recovery procedures:

(a) Reinstalling compromised systems from trusted backup-ups, if required;

(b) Reinstalling system user files, startup routines, or settings from trusted versions or sources, if required;

(c) Validating restored systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons; and

(d) Increasing security monitoring and heighten awareness for a recurrence of the incident.

--

History: Adopted on July 12, 2017. Amended on March 12, 2020 and July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-802.pdf

8-803. Penetration testing.

Systems that provide information through a public network, either directly or through another service that provide information externally (such as the World Wide Web), will be subjected to state penetration testing and intrusion testing. Penetration and intrusion testing will be conducted at the request of the agency or data owner(s) to determine if unauthorized access and or changes to an application can be made.

The results of the penetration and intrusion testing will be reviewed in a timely manner by the state information security officer. Any vulnerability detected will be evaluated for risk by the agency and a mitigation plan will be created and forwarded to the state information security officer. The tools used to perform these tasks will be updated periodically to ensure that recently discovered vulnerabilities are included.

Where an agency has outsourced a server, application or network services to another entity, responsibility for penetration and intrusion testing must be coordinated by both entities.

Any penetration or intrusion testing must be performed by individuals who are authorized by the state information security officer and who have requested and received written consent from the Office of the CIO at least 24 hours prior to any testing or scanning. Agencies authorized to perform penetration and intrusion testing or vulnerability scanning must have a process defined, tested and followed to minimize the possibility of disruption. Any other attempts to perform tests or scans will be deemed an unauthorized access attempt.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-803.pdf

8-804. Vulnerability scanning.

Systems that provide information through a public network, either directly or through another service that provide information externally (such as the World Wide Web), will be subjected to vulnerability scanning.

All servers will be scanned for vulnerabilities and weaknesses by the Office of the CIO before being installed on the state network. For both internal and external systems, scans will be performed at least monthly or after any major software or configuration changes have been made, to ensure that no major vulnerabilities have been introduced. Priority setting of vulnerabilities will be based on impact to the state and as referenced in the National Vulnerability Database (http://nvd.nist.gov).

All web-based applications will be scanned for vulnerabilities and weaknesses before being promoted to a production environment or after any major upgrades or changes have occurred. Results of the vulnerability scan will be reviewed in a timely manner by the state information security officer. Any vulnerability detected will be evaluated for risk by the Office of the CIO or agency and a mitigation plan will be created as required and forwarded to the state information security officer. The tools used to perform these tasks will be updated periodically to ensure that recently discovered vulnerabilities are included.

Where an agency has outsourced a server, application or network services to another entity, responsibility for vulnerability scanning must be coordinated by both entities.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-804.pdf

8-805. Malicious software protection.

Software and associated controls must be implemented across agency systems, and logs monitored, to detect and prevent the introduction of malicious code into the state environment. The introduction of malicious code such as a computer virus, worm or Trojan horse can cause serious damage to networks, workstations and state data. Users must be made aware of the dangers of malicious code. The types of controls and frequency of updating signature files, is dependent on the value and sensitivity of the information that could be potentially at risk.

For workstations, virus signature files must be updated at least weekly. On host systems or servers, the signature files must be updated daily or when the virus software vendor's signature files are updated and published. Security patches for software will be applied as defined by the change management process, but all software must have security patches applied as soon as possible.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-805.pdf

8-806. Security deficiencies.

All security deficiencies reported or identified in any security review, scan, assessment, or analysis must be documented in the state or agency plan of action and milestones report. These gaps must be managed to mitigation, remediation, or approved risk acceptance.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-806.pdf

8-807. Third party cyber risk management.

The State of Nebraska provides a wide range of services utilizing information technology. These numerous and complex services can only be accomplished with the support of third-party vendors, contractors, and service providers. Risks associated with these third parties must be managed by agencies.

The following are the requirements for monitoring and evaluating third-party cyber risk:

(1) Agencies must maintain a list of third-party vendors, the services those third parties provide to the agency, and define the business processes in which they are involved;

(2) A documented cyber risk analysis should be performed prior to the initiation of information technology projects involving third-party participants, except where the third party is already engaged in activities with the agency, in which case the additional services may be added to an existing assessment;

(3) The agency should design and implement additional oversight of third-party relationships involving critical business processes; and

(4) Written contracts must outline the roles and responsibilities of all parties.

--

History: Adopted on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-807.pdf

ARTICLE 9

DATA SECURITY

Section.

8-901. State data.

Data is a critical asset of the State of Nebraska. All staff have a responsibility to protect the confidentiality, integrity, availability of data generated, accessed, modified, transmitted, stored or used by the state, irrespective of the medium on which the data resides and regardless of format.

Agencies are responsible for establishing and implementing appropriate managerial, operational, physical, and technical controls for access to, use of, handling of, transmission of, and disposal of state data in compliance with this policy, federal requirements, and any applicable records retention schedule. The agency data owner should carefully evaluate and determine the appropriate data sensitivity or classification category for their information. Assigning classifications determines day-to-day practices with information: how it is handled, who handles it, how it is transported, how it is stored, and who has access.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-901.pdf

8-902. Data classification categories.

Data owned, used, created or maintained by the state is classified into the following four categories:

HIGH IMPACT

This classification level is for data that may only be accessed by a limited number of authorized staff on a strict "need to know" basis. This data includes, but is not limited to federal tax information, Social Security Administration data, protected health information, criminal justice information, and payment card information. This data shall have the strictest controls in place.

MODERATE IMPACT

This classification level is for data relating to the nature, location, or function of cybersecurity infrastructure, network architecture, system controls, and personally identifiable information. This data shall be tightly controlled, ensuring proper safeguards are in place.

LOW IMPACT

This classification level is for data that is public in nature but may require authorization to share. This data requires a minimal level of security and would not have a significant impact in the event of data disclosure.

NO IMPACT

This classification level is for public information and requires minimal level of protection and can be handled in the public domain.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-902.pdf

8-903. Data inventory.

Each agency shall identify and classify all information according to this policy. Each agency shall maintain an inventory of where HIGH IMPACT and MODERATE IMPACT information reside, so those environments can be assessed for security adequacy.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-903.pdf

8-904. Data security control assessment.

Each agency shall perform a security control assessment that assesses the adequacy of security controls for compliance with this policy and any applicable security frameworks (e.g., NIST, PCI, CMS, and IRS). The assessment may be performed internally by the agency information security officer or with the assistance of the state information security officer. Each agency is required to have an assessment at least once every year, covering at least one-third of the applicable controls such that all control areas have been assessed over a three-year period. Agencies are also required to perform an assessment anytime significant changes to the technical environment occur.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-904.pdf

8-905. Data sharing.

It is critical that agencies that share information and systems learn as much as possible about the risks associated with the planned or current interconnection and the security controls that they can implement to mitigate those risks. It also is critical that they establish formally documented agreements regarding the management, operation and use of interconnections, as required. The agreement should be reviewed and approved by appropriate senior staff from each organization.

All agencies that share connectivity and information between the agency and the Office of the CIO are required to have a security program that meets this policy. The agency information security officer shall develop a system security plan that must be approved by the state information security officer. All agencies shall perform a security control assessment that identifies the adequacy of security controls and precautions for protecting state information. If the agency performs this assessment independent of the state information security officer, an approved and signed interconnection system agreement that describes the security controls and plans will be in place to protect state information.

--

History: Adopted on July 12, 2017.
URL: https://nitc.nebraska.gov/standards/8-905.pdf

8-906. Data destruction.

Agency data must be disposed of in accordance with the Records Management Act and any related records retention schedule. Disclosure of sensitive information through careless disposal or re-use of equipment presents a risk to the state. Formal procedures must be established to minimize this risk. Storage devices such as hard disk drives, paper or other storage media (e.g., tape, diskette, CDs, DVDs, USB drives, cell phones, and memory sticks) regardless of physical form or format containing HIGH IMPACT or MODERATE IMPACT information must be physically destroyed or securely overwritten when the data contained on the device is to be disposed. These events should include certificates of destruction. State and agency asset management records must be updated to reflect the current location and status of physical assets (e.g., in service, returned to inventory, removed from inventory, destroyed) when any significant change occurs.

--

History: Adopted on July 12, 2017. Amended on July 14, 2023.
URL: https://nitc.nebraska.gov/standards/8-906.pdf