AGENDA
STATE GOVERNMENT COUNCIL
Executive Building - Lower Level Conference Room
521 S 14th Street
Lincoln, Nebraska
Thursday, June 8, 2017
1:30 p.m.

1:30 p.m.	1. Roll Call, Meeting Notice & Open Meetings Act Information 2. Public Comment 3. **Approval of Minutes* – February 9, 2017 and April 13, 2017** *(Attachment 3)*	Chair
	4. Standards and Guidelines **a. Proposal 17-02*** Definitions *(Attachment 4-a)* **b. Proposal 17-01*** Information Security Policy i. Amendment 1 to Proposal 17-01 *(Attachment 4-b-i)* ii. Strikethrough version of Amendment 1 *(Attachment 4-b-ii)*	Chris Hobbs
	5. Agency Reports and Other Business	Members
3:30 p.m.	6. Adjourn	Chair

*** Indicates an action item**

The Council will attempt to adhere to the sequence of the published agenda, but reserves the right to adjust the order and timing of items and may elect to take action on any of the items listed.

Meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on June 1, 2017. The agenda was posted to the NITC website on June 1, 2017.

Nebraska Open Meetings Act

STATE GOVERNMENT COUNCIL
1526 Building - 4th Floor - Hearing Room 4D
Lincoln, Nebraska
Thursday, February 9, 2017, 1:30 p.m.
MEETING MINUTES

MEMBERS PRESENT:
Ed Toner, Chief Information Officer, Chair
Terri Slone, Department of Labor
Byron Diamond, Administrative Services
Kim Menke, Department of Natural Resources
Chris Hill, Department of Health and Human Services
Dorest Harvey, Private Sector
Keith Dey, Department of Motor Vehicles
Aaron Anderson, Workers' Compensation Court
Jim Ohmberger, OCIO-Enterprise Computing Services
Kelly Lammers, Department of Banking
Pam Kunzman, Nebraska State Patrol
Jayne Scofield, OCIO-Network Services
Chris Ayotte, Department of Revenue
Ron TeBrink, Department of Correctional Services
Jennifer Rasmussen, State Court Administrator's Office
Rod Wagner, Library Commission
Bill Wehling, Department of Roads

MEMBERS ABSENT: Colleen Byelick, Secretary of State; Dennis Burling, Department of Environmental Quality; Mike Calvert, Legislative Fiscal Office; Brent Gaswick, Department of Education; Gerry Oligmueller, Budget; Darrell Fisher, Crime Commission

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

The Chair, Ed Toner, called the meeting to order at 1:30 p.m. There were 17 voting members present at the time of roll call. A quorum existed to conduct official business. The meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on January 10, 2017. The agenda was posted to the NITC website on February 6, 2017. A copy of the Nebraska Open Meetings Act was available in the meeting room.

PUBLIC COMMENT

Chris Henkenius, CEO of H4 Technology, wrote a letter to the council with concerns regarding the state's procurement process and in-state vendors. Mr. Toner and Mr. Diamond informed Mr. Henkenius that the state is aware of this concern and Administrative Services has begun and will continue discussing this issue. Mr. Henkenius was thanked for his time. A copy of the letter was left with Mr. Toner.

APPROVAL OF JUNE 9, 2016 AND AUGUST 11, 2016 MINUTES*

Mr. Harvey moved to approve the June 9th and August 11th meeting minutes as presented. Ms. Kunzman seconded. Roll call vote: Slone-Yes, Diamond-Abstain, Menke-Abstain, Hill-Abstain, Harvey-Yes, Dey-Yes, Anderson-Yes, Ohmberger-Yes, Lammers-Abstain, Kunzman-Yes, Scofield-Yes, Ayotte-Abstain, TeBrink-Abstain, Rasmussen-Abstain, Toner-Yes, Wagner-Abstain, and Wehling-Yes. Results: Yes-9, No-0, and 8-Abstained. Motion carried.

STANDARDS AND GUIDELINES
Security Architecture
Chris Hobbs, State Information Security Officer

Mr. Hobbs discussed the draft standards. The Security Architecture Workgroup is seeking input on the draft documents. This will be an agenda item for approval at a future meeting.

PRESENTATION: GIS OVERVIEW
Nathan Watermeier, State GIS Coordinator

The GIS Council has been collaborating with state agencies and other stakeholders to address GIS issues and needs on a statewide basis. In addition to the Office of the CIO, other state agencies involved in this effort include: Nebraska Game and Parks Commission, Department of Roads, Department of Natural Resources, Nebraska State Patrol and Department of Environmental Quality. The goal is to create the data (boundaries, elevation, imagery, addresses, parcels, roads and water) once, to be shared by many. Expenses currently shared by the core agencies is approximately $1,230,000..

The OCIO is promoting an Enterprise approach to GIS which would accomplish the following:

- Leverage data for decision making across state government.
- Provide centralized location for data and services. Reduce duplication and costs.
- Free up staffing that could be used otherwise to leverage data.
- Create redundancy and reduce risk. Increase system and workflow resilience.
- Create governance and coordination to support policies, security, data sharing, and adoption of standards.
- Develop a concerted line of defense for sustainable customer service and support.
- Provide focused training for different level of users to maximize output for core business functions.

The geospatial/GIS Enterprise Platform would include 30+ TB, redundant NAS and backup, secure FTP/Dropbox, and tiered storage options.

Next Steps include:

- Formalize the Geographic Information Office within the Office of the Chief Information Officer
- Move forward with a consolidation effort to centralize map based server systems and existing support through the Geospatial/GIS Enterprise

Mr. Toner have kudos to Mr. Watermeier and Mr. Wehling for their contributions to this effort. Mr. Harvey, NITC Commissioner, also gave kudos to GIS Council for their contribution.

CIO UPDATE
Ed Toner, Chief Information Officer

The OCIO has started Phase 3 of the IT Consolidation initiative. It was initially scheduled to start mid-year, but the date was moved up. The OCIO will be having discovery meetings with the agencies to understand work being performed relevant to this phase. The goal is to have the discovery meetings completed by the end of March. One goal will be to have site support centers across the state to provide faster and more efficient service to our customers at local locations. Members of the Phase 3 team include staff from the OCIO, DHHS and NDOR. Council members were encouraged to go to the FAQ page on the OCIO website for additional information.

AGENCY REPORTS AND OTHER BUSINESS

There were no agency reports.

ADJOURNMENT

Mr. TeBrink moved to adjourn the meeting. Ms. Slone seconded. All were in favor. Motion carried.

The meeting was adjourned at 2:35 p.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Jayne Scofield of the Office of the CIO/NITC.

STATE GOVERNMENT COUNCIL
Executive Building - Lower Level Conference Room
521 S 14th Street
Lincoln, Nebraska
Thursday, April 13, 2017, 1:30 p.m.

WORKING SESSION

MEETING MINUTES

MEMBERS PRESENT:
Chris Hill, Department of Health and Human Services
Colleen Byelick, Secretary of State
Keith Dey, Department of Motor Vehicles
Aaron Anderson, Workers' Compensation Court
Jim Ohmberger, OCIO-Enterprise Computing Services
Mike Fargen, Crime Commission
Pam Kunzman, Nebraska State Patrol
Chris Ayotte, Department of Revenue
Ron TeBrink, Department of Correctional Services
Jennifer Rasmussen, State Court Administrator's Office
Rod Wagner, Library Commission

MEMBERS ABSENT: Ed Toner, Chief Information Officer; John Albin, Department of Labor; Byron Diamond, Administrative Services; Rex Gittins, Department of Natural Resources; Dorest Harvey, Private Sector; Kelly Lammers, Department of Banking; Jayne Scofield, OCIO-Network Services; Bill Wehling, Department of Roads; Dennis Burling, Department of Environmental Quality; Mike Calvert, Legislative Fiscal Office; Brent Gaswick, Department of Education; Gerry Oligmueller, Budget

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

Mr. Ohmberger called the meeting to order at 1:30 p.m. Without objection, Mr. Ohmberger served as the temporary chair for this meeting. There were 11 voting members present at the time of roll call. A quorum was not present. The meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on March 27, 2017. The agenda was posted to the NITC website on April 10, 2017. A copy of the Nebraska Open Meetings Act was available at the front of the meeting room.

DISCUSSION OF PROPOSAL 17-01 INFORMATION SECURITY POLICY

Chris Hobbs, State Information Security Officer

Mr. Hobbs led a discussion of the draft Information Security Policy. This new policy was drafted by the Security Architecture Workgroup and replaces the existing security related standards and guidelines. The Technical Panel has posted this proposal for the 30-day comment period, which ends on May 12. Suggested changes received during the comment period and from the State Government Council will be addressed at the June meetings of the State Government Council and Technical Panel.

Members discussed the following issues: defined terms; consistent use of terms; training requirements; length of time for training of new hires; process for terminating accounts; segregation of duties; baseline configuration documentation for change management; identification badges; monitoring system access; non-state issued email accounts; remote access requirements; and password requirements.

At the end of the time allotted for this working session, members had discussed articles 1 through 3. Members were ask to send Mr. Hobbs any additional comments on the draft policy by the end of the

month. Mr. Ohmberger indicated an additional meeting may be necessary to review the remaining articles.

ADJOURNMENT

Mr. Dey moved to adjourn the meeting. All were in favor. Motion carried.

The meeting was adjourned at 2:40 p.m.

Meeting minutes were taken by Rick Becker, Office of the CIO/NITC.

Attachment 4-a

State of Nebraska
Nebraska Information Technology Commission
Technical Standards and Guidelines

Proposal 17-02

A PROPOSAL TO REVISE NITC 1-101 relating to definitions; to modify the basic format of the definitions; to amend various definitions; to add new definitions; and to repeal the original section.

Section 1. The following provisions constitute a revised section 1-101:

~~1. General Provisions~~1-101 General definitions.

~~For purposes of the NITC Standards and Guidelines documents, the definitions found in this document apply. Some NITC Standards and Guidelines documents may contain additional definitions which will only apply to the document in which they appear.~~ Subject to additional definitions contained in subsequent articles which are applicable to specific articles or parts thereof, and unless the context otherwise requires, in the NITC Technical Standards and Guidelines:

~~2. Definitions~~

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

2. "Agency"~~: Any~~ means any agency, department, office, commission, board, panel, or division of ~~the state~~state government.

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

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

4. “AISO” is an abbreviation for agency information security officer.

5. “Authentication”~~: The~~ means the process to establish and prove the validity of a claimed identity.

6. “Authenticity”~~: This is~~ means the exchange of security information to verify the claimed identity of a communications partner.

7. “Authorization”~~: The~~ means the granting of rights, which includes the granting of access based on an authenticated identity.

8. “Availability”~~: The~~ means the assurance that information and services are delivered when needed.

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

10. “Breach”~~: Any~~ means any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

11. “Business ~~Risk~~risk”~~: This is~~ means the combination of sensitivity, threat and vulnerability.

12. “Chain of ~~Custody~~custody”~~: Protection~~ means the protection of evidence by each responsible party to ensure against loss, breakage, alteration, or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence.

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

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

15. “CIO” is an abbreviation for Chief Information Officer.

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

17. "Commission" means the Nebraska Information Technology Commission.

18. "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. Neb. Rev. Stat. § 81-1120.02(4).

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

20. "Compromise"~~: The~~ 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.

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

22. "Confidentiality"~~: The~~ means the assurance that information is disclosed only to those systems or persons that are intended to received that information.

23. "Continuity of ~~Operations~~ operations ~~Plans~~ plan"~~(COOP): Provides~~ means a plan that provides for the continuation of government services in the event of a disaster.

24. "Controls"~~: Countermeasures~~ means countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

25. "COOP" is an abbreviation for continuity of operations plan.

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

27. "Cyber ~~Security~~ security ~~Incident~~incident"~~: Any~~ means any electronic, physical, natural, or social activity that threatens the confidentiality, integrity, or availability of ~~State of Nebraska~~state information systems, or any action that is in violation of the Information Security

Policy.

For example:

- Any potential violation of ~~Federal~~ federal or ~~State~~ state law, or NITC policies involving ~~State of Nebraska~~state information systems.

- A breach, attempted breach, or other unauthorized access to any ~~State of Nebraska~~state information system originating from either inside the ~~State~~ 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 of Nebraska~~state in a manner inconsistent with ~~State~~ state policies.

- False identity to gain information or passwords.

28. "Data"~~: Any~~ 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.

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

30. "Data ~~Owner~~owner"~~: An~~ means an individual or a group of individuals with responsibility for making classification and control decisions regarding use of information.

31. "Denial of ~~Service~~service"~~: An~~ 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.

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

33. "DMZ"~~: Demilitarized~~ is an abbreviation for demilitarized zone~~;~~, and means a semi-secured buffer or region between two networks such as between the public Internet and the trusted private ~~State~~ state network.

34. "Encryption"~~: The~~ means the cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

35. "Enterprise"~~: 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. Neb. Rev. Stat. § 86-505.

36. "Enterprise ~~Project~~project"~~: 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. Neb. Rev. Stat. § 86-506.

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

38. "External ~~Network~~network"~~: The~~ 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.

39. "External service provider" means a non-agency consultant, contractor, or vendor.

40. “Family Educational Rights and Privacy Act (FERPA)”: Federal means the federal law regarding the privacy of educational information. For additional information visit the U.S. Department of Education

41. “FERPA” is an abbreviation for the federal Family Educational Rights and Privacy Act.

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

43. “Geographic Information information System system”(GIS): A 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 GIS geographic information system must also include a focus on people, organizations, and standards.

44. “Geospatial Datadata”: A term used to describe 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.

45. “GIS” is an abbreviation for geographic information system.

46. “GLBA” is an abbreviation for the federal Gramm-Leach-Bliley Act.

47. “Gramm-Leach-Bliley Act (GLB)”: Federal regulation means the federal act requiring privacy standards and controls on personal information for financial institutions. For additional information visit the Bureau of Consumer Protection

48. “Guideline”: An means an NITC document that aims to streamline a particular process. Compliance is voluntary.

49. “Health Insurance Portability and Accountability Act (HIPAA)”: A Congressional means the federal act that addresses the security and privacy of health data. For additional information visit Health & Human Services

50. "HIPAA" is an abbreviation for the federal Health Insurance Portability and Accountability Act.

51. "Host"~~: A~~ means a system or computer that contains business and/or operational software and/or data.

52. "Incident"~~: Any~~ means any adverse event that threatens the confidentiality, integrity or accessibility of information resources.

53. "Incident ~~Response~~response"~~: An~~ means an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident).

54. "Incident ~~Response~~ response ~~Team~~team"~~: A~~ means a group of professionals within an agency trained and chartered to respond to identified information technology incidents.

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

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

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

58. "Information ~~System~~system"~~: A~~ 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.

59. "Information ~~Technology~~technology"~~: Information technology~~ means computing and telecommunications systems and their supporting infrastructure and interconnectivity used to

acquire, transport, process, analyze, store, and disseminate information electronically. Neb. Rev. Stat. § 86-507.

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

61. "Information ~~Technology~~ technology ~~Resources~~resources"~~: Hardware~~ 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.

62. "Integrity"~~: The~~ means the assurance that information is not changed by accident or through a malicious or otherwise criminal act.

63. "Internet"~~: A~~ 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.

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

65. "Internet Protocol ~~(IP)~~"~~: A~~ means a packet-based protocol for delivering data across networks.

66. "IP" is an abbreviation for Internet Protocol.

67. "IT" is an abbreviation for information technology.

68. "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.

69. "LAN" is an abbreviation for local area network.

70. "Local ~~Area~~ area ~~Network~~ network"~~(LAN): A~~ 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~~ state agencies, ~~LANs~~ local area networks are defined as restricted to rooms or buildings.~~ An interconnection of LANs over a citywide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas is commonly called a wide area network (WAN).~~

71. "Malicious ~~Code~~code"~~: Malicious Code refers to~~ 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.

72. "MAC address" is an abbreviation for media access control address.

73. "MAN" is an abbreviation for metropolitan area network.

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

75. "May" means that an item is truly optional.

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

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

78. “Must” means an absolute requirement of the specification.

79. “Must not” means an absolute prohibition of the specification.

80. “Nebraska Information Technology Commission (NITC)”: The means the information technology governing body created in Neb. Rev. Stat. § 86-515.

81. “Network Interface interface Card card”(NIC): A 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.

82. “Network Nebraska”: The means the network created pursuant to Neb. Rev. Stat. § 86-5,100.

83. “NIC” is an abbreviation for network interface card.

84. “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.

85. “NITC” is an abbreviation for Nebraska Information Technology Commission.

86. “Not recommended” has the same meaning as should not.

87. “OCIO” is an abbreviation for Office of the Chief Information Officer.

88. “Office of the Chief Information Officer (OCIO)”: A 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 are part of the OCIOOffice of the Chief Information Officer.

89. “Office of the CIO” is an abbreviation for Office of the Chief Information Officer.

90. “Optional” has the same meaning as may.

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

92. “Physical ~~Security~~security”~~: The~~ 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.

93. “Policy”~~: An~~ 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 of Nebraska~~state.

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

95. “Privacy”~~: The~~ means the right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

96. “Private ~~Information~~information”~~: Private Information~~ means personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired: (a) social security number; ~~or~~(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.

97. “Privileged ~~Account~~access account”~~: The~~ means the User ID or account of an individual whose job responsibilities require special system authorization, such as a network

administrator~~,~~ or security administrator~~, etc~~. Special authorizations are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator~~, etc~~.

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

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

100. "Recommended" has the same meaning as should.

101. "Records Management Act"~~: The~~ means the Nebraska records management statutes codified at Neb. Rev. Stat. §§ 84-1201 to 84-1228.

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

103. "Recovery"~~: A~~ means a defined step or process within an incident response plan with the goal of returning the affected or compromised systems to normal operations.

104. "Required" has the same meaning as must.

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

106. "Risk"~~: The~~ 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.

107. "Risk ~~Assessment~~assessment"~~: The~~ 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.

108. "Risk ~~Management~~management"~~: The~~ means the process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

109. "Router"~~: A~~ 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.

110. "Security ~~Management~~management"~~: The~~ means the responsibility and actions required to manage the security environment including the security policies and mechanisms.

111. "Security ~~Policy~~policy"~~: The~~ 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.

112. "Sensitive ~~Information~~information"~~: Disclosure or modification of this~~ 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.

113. "Sensitivity"~~: The~~ means the measurable, harmful impact resulting from disclosure, modification, or destruction of information.

114. "Separation of ~~Duties~~duties"~~: A~~ means the concept that no individual should have control over two or more phases of an operation or areas of conflicting responsibility.

115. "Shall" has the same meaning as must.

116. "Shall not" has the same meaning as must not.

117. "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.

118. "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.

119. “SISO” is an abbreviation for state information security officer.

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

121. “Staff”: Any means State of Nebraska full time and temporary state employees, third party contractors and consultants who operate as employees, volunteers and other agency workers and other persons performing work on behalf of the state.

122. “Standard”: Sets 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.

123. “Standards and Guidelinesguidelines”: Refers to 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

124. “State”: The means the State of Nebraska.

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

125. “State Information information Security security Officerofficer”: The Information Security Officer appointed by the Chief Information Officer to lead the NITC Security Architecture Workgroup. Responsibilities include creating and maintaining polices for the State of Nebraska, conducting vulnerability / penetration tests at an enterprise level, and to assist Agency Information Security Officer's means the individual employed by the state with such title.

126. “State Networknetwork”: The has the same meaning as communications system State of Nebraska's internal, private network, e.g. the State's 10.x.x.x address space.

127. “Switch”: A 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.

128. "System"~~(s): An~~ 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.

129. "System ~~Development~~ development ~~Life~~ life ~~Cycle~~cycle"~~: A~~ means a software development process that includes defining the system requirements, the design specifications, the software development, installation and training, maintenance, and disposal.

130. "TCP/IP"~~: An~~ 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.

131. "Technical Panel"~~: The~~ means the panel created in Neb. Rev. St. § 86-521.

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

132. "Threat"~~: A~~ 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.

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

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

135. "UID" is an abbreviation for user ID.

136. "Unauthorized ~~Access~~ access ~~Or~~ or ~~Privileges~~privileges"~~: Insider or outsider who gains~~ means access to network or computer resources without permission.

137. "User": ~~Any agency (ies), federal government entity (ies), political subdivision(s), their employees or third party contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a System for a legitimate government purpose~~ means a person who is authorized to use an information technology resource.

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

139. “Virtual ~~Local~~ local ~~Area~~ area ~~Network~~ network”~~(VLAN): A VLAN is~~ 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.

140. “Virtual ~~Private~~ private ~~Network~~ network”~~(VPN): A~~ 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.

141. “Virus”~~: A~~ 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).

142. “VLAN” is an abbreviation from virtual local area network.

143. “VPN” is an abbreviation for virtual private network.

144. “Vulnerability”~~: A~~ 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.

145. “Vulnerability ~~Scanning~~scanning”~~: The~~ 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.

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

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

148. “Web ~~Site~~ site or ~~Website~~website”~~: A~~ means a set of interconnected ~~Web~~ web ~~Pages~~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.

149. “Wide ~~Area~~ area ~~Network~~ network”~~(WAN): A~~ 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 ~~(LAN)~~ and is usually spread over a larger geographic area~~ than that of a LAN~~.

150. “Wireless ~~Local~~ local ~~Area~~ area ~~Network~~ network”~~(WLAN): A wireless local area network (or wireless LAN, or WLAN) is~~ means the linking of two or more computers without using wires. ~~WLAN~~ 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.

151. “WAN” is an abbreviation for wide area network.

152. “WLAN” is an abbreviation for wireless local area network.

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

Sec.2. Original section 1-101 is repealed.

Sec.3. Subsections 21, 74, 99 and 105 of section 1 of this proposal become operative on December 1, 2017. The other provisions of this proposal take effect when approved by the Commission.

Attachment 4-b-i

State of Nebraska
Nebraska Information Technology Commission
Technical Standards and Guidelines

Amendments to Proposal 17-01
Amendment 1

1. Strike the original sections and insert the following new sections:

Section 1. The following provisions constitute a new CHAPTER 8 of the Technical Standards and Guidelines:

CHAPTER 8

INFORMATION SECURITY POLICY

Article.

1. Purpose; Scope; Roles and Responsibilities; Enforcement and 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; ENFORCEMENT AND POLICY EXCEPTION PROCESS

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.

8-102. Scope

This policy is applicable to state agencies, boards, and commissions, excluding higher education entities. 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.

8-103. Roles and Responsibilities

State Agencies

Agencies that create, use, or maintain information systems for the state must create and maintain an information security program consistent with this policy to ensure the confidentiality, availability, and integrity of the state's information assets.

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.

State Information Security Officer

The state information security officer performs as a security consultant to agencies and agency information security officers to assist the agencies in meeting the requirements of this policy. The state information security officer may also perform periodic reviews of agency security for compliance with this and other security policies and standards.

Agency Information Security Officer

The agency information security officer has overall responsibility for ensuring the implementation, enhancement, monitoring, and enforcement of the information security policies and standards for

their agency. The agency information security officer is responsible for providing direction and leadership to the agency through the recommendation of security policies, standards, processes and education and awareness programs to ensure that appropriate safeguards are implemented, and to facilitate compliance with those policies, standards and processes. The agency information security officer is responsible for investigating all alleged information security violations. In this role, the agency information security officer will follow agency procedures for referring the investigation to other investigatory entities, including law enforcement. The agency information security officer will coordinate and oversee security program activities and reporting processes in support of this policy and other security initiatives.

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.

Technical Panel

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

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.

Security Architecture Workgroup

The Security Architecture Workgroup is a workgroup 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 security issues; document existing problems, potential points of vulnerability, and related risks; and, determine security requirements of state agencies stemming from state and federal laws or regulations.

8-104. Enforcement and 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.

ARTICLE 2

GENERAL PROVISIONS

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) NITC 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 acceptable use provisions are established by this policy:
   (a) all state electronic business must be conducted on approved IT devices;
   (b) accessing or attempting to access CONFIDENTIAL or RESTRICTED 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.

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.

IT Infrastructure - The following change management standards are required to be followed for all IT infrastructure.

1. 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.

2. All records, meetings, decisions, and rational 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:

   A. Change summary, justification and timeline;

B. Functionality, regression, integrity, and security test plans and results;

C. Security review and impact analysis;

D. Documentation and baseline updates; and

E. Implementation timeline and recovery plans.

3. The agency is required to maintain baseline configuration documentation in use throughout the infrastructure. These baseline configuration documents shall be categorized as CONFIDENTIAL 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.

4. 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.

Application Development – The following change management standards are required to be followed for application software systems that create, process, or store CONFIDENTIAL or RESTRICTED data.

1. 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.

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 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:

    A. Change summary, justification, and timeline;

    B. Functionality, regression, customer acceptance, and security test plans;

    C. Security review and impact analysis;

    D. Documentation and baseline updates; and

    E. 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 that ensure the confidentiality, integrity, and availability of the data maintained in the production library.

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

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 CONFIDENTIAL or RESTRICTED 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 CONFIDENTIAL or RESTRICTED information. Encryption technology must be approved by the state information security officer or agency information security officer.

8-204. Email

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 or the agency information security officer.

CONFIDENTIAL or RESTRICTED data should not be sent by email unless it has been encrypted using technology approved by the state information security officer or the agency information security officer.

8-205. Portable Media

CONFIDENTIAL or RESTRICED data should not be stored on portable media unless it has encrypted using technology approved by the state information security officer or the agency information security officer.

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 CONFIDENTIAL or RESTRICTED 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. CONFIDENTIAL or RESTRICTED information must maintain at least two barriers to access at all times.

8-206. Facilities; Identification Badges and 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.

8-207. State and Agency Security Planning and Reporting

The following standard and recurring reports are required to be produced by the state information security officer and each agency information security officer:

1. Information security strategic plan;
2. System security plan(s); and
3. Plan of actions and milestones (POA&M).

These reports will reflect the current and planned state of information security at the agency.

A. <u>Information Security Strategic Plan</u>

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 must be updated and published on an annual basis, and should include a 5-year projection of key security business drivers, planned security infrastructure implementation, and forecasted costs. It should include an educated view of emerging threats and protections, and an analysis of the potential impacts to state information assets. 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.

<u>Contents of the Information Security Strategic Plan:</u>

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. Detailed descriptions of significant security risks, and plans to mitigate or remediate those risks.

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.
8. Analysis of the regulatory and contractual compliance environment, including potential new regulations or pending contractual requirements that will affect information security.
9. Proposed five-year timeline of events and key deliverables or milestones.
10. Line item cost projections for all information security activity that is itemized by:
    a. Steady state investments: The costs for current care and maintenance of the information security program.
    b. Risk management and mitigation: The line item expenses necessary to mitigate or resolve security risks for the agency in a prioritized order.
    c. Future technology: The line item forecasted expenses and timelines necessary to support emerging or changing technology, and to be ready for new and emerging threats.
    d. Regulatory: The line item expense necessary to meet all regulatory and contractual compliance requirements.

B. <u>System Security Plan</u>

The state and agency 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 address all control areas identified in the NIST 800-53 control framework, and will describe the current controls in place to protect information at a level commensurate with the sensitivity level of the system.

The state information security officer will work with each agency information security officer to maintain an SSP incorporating each identified system managing information or used to process agency business.

The agency information security officer and the state information security officer are required to develop or update the SSP in response to each of the following events:

- New system
- Major system modification

- Increase in security risks / exposure
- Increase of overall system security level
- Serious security violation(s)
- 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. Describe information flow and how information is handled. 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 sensitive information, including CONFIDENTIAL and RESTRICED 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. Detailed information security descriptions, procedures, protocols, and implemented controls for all NIST 800-53 control areas within the scope of the system. Identify compensating controls or compliance gaps within this section of the SSP.
8. System interconnection or information sharing: Describe all interfacing or connections between two or more systems or business partners.
9. 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.
10. Review of security controls and assessment results that have been conducted within the past three years.
11. 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.

C. Plan of Action and Milestones Report (POA&M)

The POA&M is a reporting tool that outlines weaknesses and delineates the tasks necessary to mitigate them. The information security POA&M process will be used to facilitate the remediation of information security and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions
- Defining roles, responsibilities, and accountabilities for weakness resolution
- Assisting in identifying the security funding requirements necessary to mitigate weaknesses
- Tracking and prioritizing resources
- Ensuring appropriate progress and priorities are continually addressed
- Informing decision makers

The POA&M process provides significant benefits to the state. It is a dynamic management tool useful for ongoing efforts to address programmatic and system-specific vulnerabilities. It assists in essential decision-making activities, facilitating and helping to ensure the oversight and mitigation of security weaknesses and the cost-effective use of mitigation resources. To function effectively, a POA&M must be continually monitored and diligently updated. The state information security officer and agency information security officers are responsible for maintaining the POA&M and for providing quarterly updates to the leadership.

Contents of the Information Security Plan of Action with Milestones:

1. Source – Identifies the audit, review, event or procedure which identified this action item
2. ID – Identification tracking number of this action item which can be tied to the source and timeframe of identification
3. Project/Task – Defines the project, task objective and goals of the action item
4. Key content and description – Narrative describing the key elements of the action item
5. Key milestones – Lists each measurable activity required to complete the action item
6. Milestone status – Lists the status of each milestone (Open, Completed, Closed Assigned, In Progress)
7. Target or completion date – Expected date each milestone will be completed. The agency should also accommodate approved changes to target dates in a manner that reflects the new date while keeping record of the original due date.
8. Responsible party – List of individuals or support unit assigned to address the action item

ARTICLE 3

ACCESS CONTROL

8-301. Remote Access Standard

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 standards apply to all staff that connect to the state network through the Internet. This includes all approved work-from-home arrangements requiring access to state systems and agency office locations that use the Internet to access the state network. Each state agency will be responsible for ensuring that remote access to state resources is secured and compliant with this policy.

(1) The following are the general requirements for remote access:
   (a) Requests for remote access must be reviewed and approved by the state information security officer and the agency information security officer prior to access being granted.
   (b) Staff approved for remote connectivity are required to comply with all policies and standards.
   (c) 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.
   (d) 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.
   (e) Remote access logon failures must be logged. Credentials must be disabled after three (3) consecutive failed login attempts.
   (f) 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.
   (g) Staff with remote access privileges must ensure that their computer which is remotely connected to the state network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.

(2) The following are additional requirements for remote access to data classified as CONFIDENTIAL or RESTRICTED:
   (a) Requests for remoted access must indicate if CONFIDENTIAL or RESTICTED data may be accessed.
   (b) Mechanisms must be employed to ensure personally identifiable information, or other sensitive information cannot be downloaded or remotely stored.

(c) All state owned or managed devices must be password protected and full-disk encrypted using approved technology. Encryption technology must be provided or approved by the Office of the CIO.

(d) Remote sessions that store, process, or access CONFIDENTIAL or RESTRICTED information or systems must use access control credentials and an approved form of multi-factor authentication before connecting to the state network. Remote sessions must employ Office of the CIO approved cryptography during the entire session when connected to the state network.

8-302. Minimum Password Configuration

A. Minimum Password Requirements

The following are the minimum password requirements for state government passwords:

- Must contain a minimum Eight (8) characters
- Must contain at least Three (3) of the following Four (4):
- At least One (1) uppercase character
- At least One (1) lowercase character
- At least One (1) numeric character
- At least One (1) symbol (!@#$%^&)
- 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.

B. Additional Access Requirements for RESTRICTED Information

Information that is classified as RESTRICTED requires the highest level of security. This includes root/admin level system information accessed by privileged accounts. A password used to access RESTRICTED information must follow the password complexity rules outlined in subsection A, and must contain the following additional requirements:

- Multi-factor authentication
- Expire after 60 days
- Minimum Password Age set to 15 days
- Accounts will automatically be disabled after three unsuccessful password attempts

C. Additional Access Requirements for CONFIDENTIAL Information

Information that is classified as CONFIDENTIAL requires a high level of security. A password used to access CONFIDENTIAL information must follow the password complexity rules outlined in subsection A, and must contain the following additional requirements:

- Expire after 90 days
- Accounts will automatically lock after three consecutive unsuccessful password attempts

D. Password Requirements for MANAGED ACCESS PUBLIC Information

Information that is classified as MANAGED ACCESS PUBLIC requires minimal level of security and need not comply with subsection A. Typically, this data would not include personal information but may carry special regulations related to its use or dissemination. MANAGED ACCESS PUBLIC data may also be data that is sold as a product or service to users that have subscribed to a service.

E. Password Requirements for Accessing PUBLIC Information

Information that is classified as PUBLIC requires no additional password security and need not comply with subsection A.

F. 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 A. The additional requirements for access to CONFIDENTIAL or RESTICTED data with a non-expiring password are:

- Extended password length to 10 characters
- Independent remote identity proofing may be required
- Personal security question may be asked
- Multi-factor authentication
- Any feature not included on this list may also be utilized upon approval of the state information security officer.

G. 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.

H. 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 CONFIDENTIAL or RESTRICTED information.

I. 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.

8-303. Identification and Authorization

A. All staff 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 user ID with the minimum necessary access required to perform their duties.

B. Staff are required to secure their user IDs from unauthorized use.

C. Sharing user IDs is prohibited.

D. 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.

8-304. Privilege 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:

- 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.
- Default administrator accounts must be renamed, removed or disabled. Default passwords for renamed or disabled default administrator accounts must be changed.
- 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 privilege accounts.
- Privileged access accounts will have enhanced activity logging enabled. The Office of the CIO and all applicable agencies will perform a quarterly review of privileged access account activity.
- Privileged access through remote channels will be allowed for authorized purposes only and must include multi-factor authentication.
- Passwords for these accounts must be changed every 60 days.
- 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.

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

ARTICLE 4

NETWORK SECURITY

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.

8-402. Network Transmission Security

1 All encryption must be approved by the state information security officer. Any transmissions over unsecured networks (such as the Internet) that contain CONFIDENTIAL or RESTRICTED 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.

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.

8-403. Network Architecture Requirements

1 All devices that store, access, or process CONFIDENTIAL or RESTRICTED 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 CONFIDENTIAL or RESTRICTED 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.

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.

8-404. External Connections

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

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.

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.

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. 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.

No wireless network or wireless access point will be installed without the written approval of the Office of the CIO.

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.

ARTICLE 5

SYSTEM SECURITY

8-501. System 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.

8-502. Minimum User Account Configuration

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.

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.

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.

8-503. Minimum Server Configuration and Patch Management

The state recognizes the National Institute of Standards and Technology (NIST) as a source for recommended security requirements that provide minimum baselines of security for servers.

NIST provides instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All state system administrators should examine NIST 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 NIST standards, guidelines, and checklists as identified below.

- NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-70, The NIST Security Configuration Checklists Program
- NIST SP 800-44, Guidelines on Securing Public Web Servers

Server Hardening

All servers that store, process, or have access to CONFIDENTIAL or RESTRICTED data 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 state information security officer.

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 sensitive 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 IT authorized personnel only, and all vendor supplied patches must be applied. All software and hardware components should be currently supported. All unsupported hardware and software components must be identified and have a management plan that is approved by the state information security officer.
3. All unnecessary software, system services, accounts and drivers must be removed unless doing so would have a negative impact on the server.
4. Logging of auditable events, as defined in NIST 800-53 control objectives, will be enabled. Audit logs will be secured and only accessible to accounts with privileged access.
5. Security parameters and file protection settings must be established, reviewed, and approved by the state information security officer.
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 Department and as referenced in the National Vulnerability Database (HTTP://nvd.nist.gov).
7. Hardened servers will be scanned monthly for unauthorized software or unauthorized changes to the configuration baselines.
8. Hardened servers will be monitored with active intrusion detection, intrusion protection, or 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 changes to hardened 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 hardened servers must be performed over secured channels only. 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.

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. In addition to adherence to the required images, the following standards are defined for all workstations that connect to the state network. The degree of protection of the workstation should be commensurate with the data classification of the resources stored, accessed, or processed from this computer.

1. Endpoint security (anti-virus) software, approved by the Office of the CIO, must be installed and enabled.
2. The host-based firewall must be enabled if the workstation is removed from the state network.
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.
7. Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion.
8. 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.
9. Shared login accounts are forbidden on multi-user systems where the manipulation and storage of CONFIDENTIAL or RESTRICTED information takes place.
10. Users need to lock their desktops when not in use. The system must automatically lock a workstation after 5 minutes of inactivity.
11. Users are required to store all CONFIDENTIAL or RESTRICTED 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.
12. All workstations shall be re-imaged with standard load images prior to re-assignment.
13. Equipment scheduled for disposal or recycling must be cleansed following agency media disposal guidelines

8-505. Minimum Laptop Configuration

In addition to the requirements contained in section 8-504, all laptops that connect to the state network are required to meet the following requirements.

1. Remote access to CONFIDENTIAL or RESTRICTED information must occur through a state-managed endpoint, using the state VPN or other connections that have been approved by the Office of the CIO.
2. Remote access to any privilege functions, such as administrator accounts, must employ multi-factor authentication and all activity must be logged for audit purposes.
3. Remote access users are responsible for all actions incurred during their session in accordance with all state and agency standards and policies.
4. All home networks connected to the Internet via a broadband connection should have a firewall installed, updated and operational.
5. Laptops with remote access to, or the capability to store, CONFIDENTIAL or RESTRICTED data are required to be fully encrypted using technology approved by the state information security officer.

8-506. Minimum Mobile Device Configuration

All mobile computing 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.

1. Mobile computing 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 computing devices and mobile storage devices must not be left in a vehicle unattended.
3. Storing CONFIDENTIAL or RESTRICTED information on any mobile device or any removable or portable media (e.g., CDs, thumb drives, DVDs) is prohibited unless arrangements and mechanisms for securing the data has been explicitly approved by the state information security officer. In those cases, all mobile computing devices or portable media shall be encrypted using technology that is approved by the state information security officer.
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 15 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.
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.

8-507. System Maintenance

1. All systems involved in the processing, storage, or access to any CONFIDENTIAL or RESTRICTED 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 any secured environment, 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. Critical patches must be applied within 24 hours of receipt. High risk patches must be applied within 7 days of receipt. All other patches must be appropriately applied in a timely manner as determined by the agency.
9. All vendor supplied software deployed and operational must be currently supported by the vendor.

ARTICLE 6

APPLICATION SECURITY

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 CONFIDENTIAL or RESTRICTED 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.

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.

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:

- Access to compilers, editors and other system utilities must be removed from production systems when not required.

- Logon procedures and environmental identification must be sufficiently unique for production testing and development.
- 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.
- 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.

8-604. Application Development

The following standards are required to be followed for agency developed application software that create, process, or store CONFIDENTIAL or RESTRICTED 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:
    a. Change summary, justification, and timeline
    b. Functionality, regression, integrity, and security test plans and results
    c. Security review and impact analysis
    d. Documentation and baseline updates
    e. 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.
11. Applications must be configured such that CONFIDENTIAL or RESTRICTED data will be encrypted when transmitted outside the agency internal network.

8-605. Security Standards for 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).

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 CONFIDENTIAL or RESTRICTED 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.
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 or SANS websites:

https://www.owasp.org/index.php/Category:OWASP_Guide_Project

http://www.sans.org/top25-software-errors/

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 CONFIDENTIAL or RESTRICTED information with these services, unless the storage is encrypted with approved technology, and has been approved in advance by the state information security officer.

8-607. Cloud Computing Standard

1. DEFINITIONS

1.1 NIST Definition of Cloud Computing

This standard incorporates the following definition from the National Institute of Standards and Technology (*The NIST Definition of Cloud Computing*, NIST Special Publication 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).

1.2 Other Deployment Models

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

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
RESTRICTED	✓				⊘	
CONFIDENTIAL	✓		✓		⊘	
MANAGED ACCESS PUBLIC	△ ✓	△ ✓ △	✓	△ ✓	✓	✓
PUBLIC	△ ✓	✓ △	✓	△ ✓	✓	✓

(✓) 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.

△

2.1 **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.

3. EXEMPTION FOR EXISTING SERVICES

Cloud computing services in use on December 31, 2017, are exempt from the requirements of this standard. 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.

4. 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 CONFIDENTIAL or RESTRICTED data, the following conditions must be met or addressed in an agreement with the CSP:

1. 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.
2. Access to the cloud service must require multi-factor authentication based on data classification levels.
3. De-provisioning of credentials must occur within two (2) hours of de-provisioning of the internal system credentials.

4. Information must be encrypted using IT approved technology for information in transit as well as information stored or at rest.
5. 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.
6. 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.
7. CSP/3PH must provide vulnerability scanning and testing on a schedule approved by the state information security officer. Results will be provided to agency.
8. Patch management of hardware and software at the CSP/3PH are required to meet the same standards that are required at state.
9. 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.
10. 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.
11. 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.
12. 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.
13. CSP/3PH's must have SLAs in place that clearly define security and performance standards.
14. CSP/3PH will provide adequate security and privacy training to its associates, and provide the state information security officer with evidence of this training.
15. CSP/3PH will provide the state with the functionality to conduct a search of the data to meet public records requests.
16. 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.

ARTICLE 7

AUDITING AND COMPLIANCE

8-701. Auditing and Compliance Security Standard

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 CONFIDENTIAL or RESTRICTED 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 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:

- Reviews of the technical and business analyses required to be developed pursuant to this policy.
- 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 RESTRICTED 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.

8-702. Awareness and Training

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.

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.

Periodic 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.

8-703. Security Reviews and Risk Management

This policy is based on the NIST 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 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.

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.

8-704. Logging and Review of Auditable Events

All systems that handle CONFIDENTIAL or RESTRICTED 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:

- What activity was performed?
- Who or what performed the activity, including on what system the activity was performed?
- What the activity was performed on (object)?
- When was the activity performed?
- What tool(s) was the activity performed with?
- What was the status (such as success vs. failure), outcome, or result of the activity?

Log Format, *S*torage, 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.

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:

- Log on and off the system;
- Change of password;
- All system administrator commands, while logged on as system administrator;
- Switching accounts or running privileged actions from another account (e.g., Linux/Unix SU or Windows RUNAS);

- Creation or modification of super-user groups;
- Subset of security administrator commands, while logged on in the security administrator role;
- Subset of system administrator commands, while logged on in the user role;
- Clearing of the audit log file;
- Startup and shutdown of audit functions;
- Use of identification and authentication mechanisms (e.g., user ID and password);
- Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);
- Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system;
- Changes made to an application or database by a batch file;
- Application-critical record changes;
- Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);
- All system and data interactions concerning FTI;
- Additional platform-specific events, as defined by agency needs or requirements;
- 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
- Physical entrance or access to secured and restricted areas or facilities where system and network infrastructure reside.

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:

- Type of action (e.g., authorize, create, read, update, delete, and accept network connection);
- Subsystem performing the action (e.g., process or transaction name, process or transaction identifier);
- 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;
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time;
- Whether the action was allowed or denied by access-control mechanisms;

- Description or reason-codes of why the action was denied by the access-control mechanism, if applicable; and
- Depending on the nature of the event that is logged, there may be other information necessary to collect.

Audit Review, Monitoring, Findings and Remediation

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 of suspicious activity must be reviewed as soon as possible.
- Logs of system capacity and log integrity must be reviewed on a weekly basis.
- Logs of privilege access account creation or modification must be reviewed on a weekly basis.
- All other logs must be reviewed at least monthly.

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.

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 CONFIDENTIAL information.

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.

8-705. Security Requirements for External Service Providers

All external service providers with access to CONFIDENTIAL or RESTRICTED information must have a written agreement with the state 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.

ARTICLE 8

VULNERABILITY AND INCIDENT MANAGEMENT

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.

All agencies that process, store, or access CONFIDENTIAL or RESTRICTED 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;
2. Incident Triage and Identification;
3. Containment;
4. Incident Communication;
5. Preservation of Evidence;
6. Root Cause Analysis; and
7. Recovery and Permanent Remediation.

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.

A. <u>Preparation - Scope and Responsibilities</u>

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 e-mail containing CONFIDENTIAL or RESTRICTED 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.

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.

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.

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:

- 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.
- Conduct the initial triage. Perform a damage and impact assessment and document the findings.
- Report to state of agency management on a regular schedule with status and action plans.
- Maintain confidentiality of the circumstances around the incident.

- Follow procedures to maintain a chain of trust and to preserve evidence.
- Initiate the root cause analysis; bring in other resources as necessary.
- Initiate return to normal operations; bring in other resources as necessary.

B. 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 any 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 RESTRICTED information.

C. 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.

D. 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 CONFIDENTIAL or RESTRICTED 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 CONFIDENTIAL or RESTRICTED information, including the potential for unauthorized disclosure (such as information spillage), will be considered incidents. Information spillage refers to instances where either CONFIDENTIAL or RESTRICTED 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.

E. 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 CONFIDENTIAL or RESTRICTED 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.

F. 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.

G. 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.

g. Log all steps.

H. 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 RESTRICTED 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.

I. 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:

- Reinstalling compromised systems from trusted backup-ups, if required;

- Reinstalling system user files, startup routines, or settings from trusted versions or sources, if required;
- Validating restored systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons; and
- Increasing security monitoring and heighten awareness for a recurrence of the incident.

8-802. 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.

8-803. 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.

8-804. 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.

8-805. Security Deficiencies

All security deficiencies reported or identified in any security review, scan, assessment, or analysis must be documented in the state or agency Security POAM. These gaps must be managed to mitigation, remediation, or approved risk acceptance.

ARTICLE 9

DATA SECURITY

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.

8-902. Data Classification Categories

Data owned, used, created or maintained by the state is classified into the following four categories:

(1) **RESTRICTED.** This classification level is for sensitive information intended for use by a limited number of authorized staff with an explicit "need to know" and controlled by special rules to specific personnel. Examples of this privileged access information include: attorney-client privilege information, agency strategies or reports that have not been approved for release, audit records, network diagrams with IP addresses specified, and privileged administrator credentials. This level requires internal security protections and could have a high impact in the event of an unauthorized data disclosure.

(2) **CONFIDENTIAL.** This classification level is for sensitive information intended for use within an agency and controlled by special rules to specific personnel. Examples of this type of data include: federal tax information (FTI), protected health information (PHI) and other Patient Medical Records covered by Health Insurance Portability and Accountability Act (HIPAA), payment card industry (PCI) information, and personally identifiable information (PII).

(3) **MANAGED ACCESS PUBLIC**. This classification level is for information that is public in nature but may require authorization to receive it. This type of information requires a minimal level of security and would not have a significant impact in the event of data disclosure. This type of information does not include personal information but may carry special regulations related to its use or dissemination. This data may also be data that is sold.

(4) **PUBLIC**. This classification is for information that requires no security and can be handled in the public domain.

8-903. Data Inventory

Each agency shall identify and classify all information according to this policy. Each agency shall maintain an inventory of where CONFIDENTIAL and RESTRICTED information reside, so those environments can be assessed for security adequacy.

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.

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.

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 CONFIDENTIAL or RESTICTED 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.

Sec.2. In section 5-204(2.2.6), strike the sentence beginning with “Section”.

Sec.3. Strike section 5-204(4) in its entirety.

Sec.4. In Attachment A to section 5-204, strike the sentence beginning with “See NITC 8-101”; strike the bulleted sentence beginning with “Approved remote access”; and strike the subsection titled: “Identified NITC policies that apply to use, access and protecting information:” in its entirety.

Sec.5. In Attachment B to section 5-204, strike the sentence beginning with “See NITC 8-101”; strike the bulleted sentence beginning with “Approved remote access”; and strike the subsection titled: “Identified NITC policies that apply to use, access and protecting information:” in its entirety.

Sec.6. Staff shall reformat and re-enumerate the provisions of this proposal for consistency prior to final publication.

Sec.7. Original sections 5-204, 8-101, 8-102, 8-103, 8-201, 8-301, 8-302, 8-303, 8-304, and 8-401 are repealed. Resource documents 8-RD-01, 8-RD-02, 8-RD-03, 8-RD-04, 8-RD-05, and 8-RD-06 are repealed.

Sec.8. This proposal becomes operative on December 1, 2017.

Attachment 4-b-ii

Amendment 1 to Proposal 17-01

Strikethrough Version

Section 1. The following provisions constitute a new CHAPTER 8 of the Technical Standards and Guidelines:

CHAPTER 8

INFORMATION SECURITY POLICY

Article.

1. Purpose; Scope; Roles and Responsibilities; Enforcement and 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; ENFORCEMENT AND POLICY EXCEPTION PROCESS

8-101. Purpose

~~The Nebraska Information Technology Commission (NITC) has statutory responsibility to adopt minimum standards and guidelines for acceptable and cost-effective use of information technology, and to provide strategic direction for all State agencies and educational institutions for information technology.~~

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 of Nebraska~~state. This Information Security Policy contains the safeguards, responsibilities and acceptable behaviors required to establish and maintain a secure environment.

8-102. Scope

This policy is applicable to ~~State of Nebraska full-time and temporary employees, third-party contractors and consultants, volunteers and other agency workers (hereafter referred to as "Staff"), all State Agencies, Boards and Commissions (hereafter referred to as "Agency")~~state agencies, boards, and commissions, excluding higher education entities.

This ~~Information Security Policy encompasses~~policy applies to all information technology systems~~, automated and manual,~~ for which the ~~State~~ state has administrative responsibility, including systems managed or hosted by third parties on behalf of an ~~Agency~~agency.

~~Guidelines and standards, published by the NITC, which are associated with this policy, provide specific details for compliance with this Information Security Policy.~~

In the event an ~~Agency~~ agency has developed policies or additional requirements for ~~Information~~ information ~~Security~~security, the more restrictive policy ~~shall~~ will apply.

8-103. Roles and Responsibilities

State Agencies~~:~~

Agencies that create, use, or maintain information systems for the ~~State of Nebraska~~state must create and maintain an information security program consistent with this policy to ensure the confidentiality, availability, and integrity of the ~~State's~~ state's information assets.

Office of the Chief Information Officer ~~(OCIO)~~

The Office of the Chief Information Officer is ~~the executor of this Information Security Policy, which establishes and monitors the effectiveness of information security, standards and controls within the~~

~~State of Nebraska~~responsible for recommending policies and guidelines for acceptable and cost-effective use of information technology in noneducation state government.

~~The Office of the CIO will modify this policy as directed by the NITC, or as needed to keep current with continually changing threats and technology.~~

State Information Security Officer ~~(SISO)~~

The state information security officer~~State Information Security Officer, operating through the Office of the Chief Information Officer,~~ performs as a security consultant to ~~Agencies~~ agencies and ~~Agency Information Security Officers~~ agency information security officers to assist the ~~Agencies~~ agencies in meeting the requirements of this policy. The state information security officer~~State ISO~~ may also perform periodic reviews of agency security for compliance with this and other security policies and standards.

Agency Information Security Officer ~~(AISO)~~

The ~~Agency Information Security Officer~~agency information security officer has overall responsibility for ensuring the implementation, enhancement, monitoring, and enforcement of the information security policies and standards for their ~~Agency~~agency. The ~~Agency Information Security Officer~~agency information security officer is responsible for providing direction and leadership to the ~~Agency~~ agency through the recommendation of security policies, standards, processes and education and awareness programs to ensure that appropriate safeguards are implemented, and to facilitate compliance with those policies, standards and processes. The ~~Agency Information Security Officer~~agency information security officer is responsible for investigating all alleged information security violations. In this role, the ~~Agency Information Security Officer~~agency information security officer will follow agency procedures for referring the investigation to other investigatory entities, including law enforcement. The ~~agency Information Security Officer~~agency information security officer will coordinate and oversee security program activities and reporting processes in support of this policy and other security initiatives.

Nebraska Information Technology Commission ~~(NITC)~~

The ~~NITC~~ Nebraska Information Technology Commission is the owner of this policy with statutory responsibility to ~~promote information security through adoption of policies, standards, and guidelines. The NITC develops strategies for implementing and evaluating the effectiveness of information security~~adopt minimum technical standards, guidelines, and architectures.

~~NITC~~ Technical Panel

The ~~NITC~~ Technical Panel~~, with advice from the Security Architecture WorkGroup,~~ is responsible for recommending ~~security policies and guidelines and making available best practices to operational entities~~technical standards and guidelines to be considered for adoption by the Nebraska Information Technology Commission.

~~NITC~~ State Government Council

The ~~NITC~~ State Government Council~~, with advice from the Security Architecture WorkGroup, is responsible for recommending security policies and guidelines and making available best practices to~~

~~operational entities~~ is an advisory group chartered by the Nebraska Information Technology Commission to provide recommendations relating to state government agencies.

~~NITC~~ Security Architecture ~~WorkGroup~~Workgroup

The ~~NITC~~ Security Architecture ~~WorkGroup~~ Workgroup is a workgroup chartered by the State Government Council to ~~prepares policies, standards, and guidelines for state government. Make~~ make recommendations to the State Government Council and Technical Panel on matters relating to security within state government~~.~~; ~~Provide~~ provide information to state agencies, policy makers, and citizens about security issues~~.~~; ~~Document~~ document existing problems, potential points of vulnerability, and related risks~~.~~; and, ~~Determine~~ determine security requirements of state agencies stemming from state and federal laws or regulations.

8-104. Enforcement and Policy Exception Process

~~The State of Nebraska has established security policies and standards to describe~~This policy establishes the controls and activities necessary to appropriately protect information and information technology ~~(IT)~~ resources. While every exception to a policy or standard weakens the protection for ~~Nebraska~~ 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~~ agency believes it needs an exception to ~~an NITC Policy or Standard~~this policy, the ~~Agency~~ agency may request an exemption by following the procedure outlined in ~~NITC Policy 1-103: Waiver Policy~~section 1-103.

ARTICLE 2

GENERAL PROVISIONS

8-201. Acceptable Use ~~Policy~~

~~State of Nebraska IT Resources can be effective tools for the staff provided they are used appropriately and adequately protected. It is the responsibility of every member of the staff to understand and comply with these standards. Should a violation of these standards occur, it is the responsibility of the Management for the department in violation to mitigate or remediate the violation in a timely manner.~~

~~Any violation of these standards by a party working directly for a Vendor may result in termination of the Vendor's contract or other measures in accordance with applicable state and federal laws and penalty provisions of the Vendor's contract.~~

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) NITC 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 acceptable use provisions are established by this policy:
   (a) ~~A~~all ~~State of Nebraska~~state electronic business ~~shall~~must be conducted on approved IT devices only;~~.~~
   (b) ~~Confidential and Restricted data, as defined in NITC 8-903: Data Classification Standard, should never be sent via email unless it has been encrypted using technology approved by the State Information Security Officer (SISO) or the Agency Information Security Officer (AISO). Confidential or Restricted data should never be place on portable media unless the portable media device is encrypted and approved by the SISO/AISO. A~~accessing or attempting to access ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information for other than a required business "need to know" is prohibited; and~~.~~
   (c) Misrepresenting yourself as another individual or organization is prohibited.

~~Forwarding email messages containing State Information from a State of Nebraska email account to a personal email account is prohibited unless that activity is approved by the OCIO, SISO, or AISO.~~Use of state information technology resources may be monitored to verify compliance with this policy.

~~Acceptable Use of IT Resources~~

~~IT devices are defined as desktop computers, servers, laptop computers, PDA's (personal digital assistant), MP3players, 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. Hereinafter referred to as "IT devices". All State of Nebraska electronic business shall be conducted on approved IT devices only.~~

~~Use of State IT resources for any purpose other than to perform approved activities and as permitted by the Information Security Policy will be considered a violation of this standard. While not an exhaustive list, approved activities include company business and limited personal use that does not interfere with business activity. In all cases, users of IT resources are~~

~~responsible for exercising good judgment regarding the reasonableness of a use of IT resources. In the event of any uncertainty, users should consult their manager or the SISO/AISO. The State of Nebraska owns all information compiled, stored, and used by the staff on State equipment and reserves the right to monitor all IT resources to verify compliance of this policy.~~

~~IT devices used by members of the staff to perform authorized business activities must be owned, leased, managed or approved by the State of Nebraska OCIO and meet specifications and requirements published by OCIO.~~

~~Members of the Staff are responsible for the reasonable protection and use of the Internal Network access assigned to them and must follow all State of Nebraska Information Security policies. State of Nebraska IT resources may not be used for any inappropriate or unlawful purpose.~~

- ~~Sharing your access credentials is prohibited. You are responsible for protecting your credentials just like you would protect access to your own bank account.~~
- ~~Confidential and Restricted data, as defined in NITC 8-903: Data Classification Standard, should never be sent via email unless it has been encrypted using technology approved by the State Information Security Officer (SISO) or the Agency Information Security Officer (AISO). Note, password protecting email attachments is NOT the same as encrypting it.~~
- ~~Confidential or Restricted data should never be place on portable media unless the portable media device is encrypted and approved by the SISO/AISO. Portable media includes laptops, thumb drives, removable disk drives, DVDs, etc. This data may not be stored, accessed, or processed on any equipment or media that is not owned, managed, or approved by the Department.~~
- ~~The State of Nebraska infrastructure, including the network and all equipment, may not be used for any file storage, sharing, or downloading any music, video, or software unless approved by the OCIO.~~
- ~~Accessing or attempting to access Confidential or Restricted information for other than a required business "need to know" is prohibited.~~
- ~~Posting, texting, or otherwise distributing citizen, department, or employee information on any social media is prohibited.~~
- ~~Remotely accessing systems containing Confidential or Restricted information from any equipment not specifically authorized or maintained by the OCIO is prohibited. All remote access to State resources containing Confidential or Restricted information shall be restricted to an approved remote connection (such as VPN) using multi-factor authorization.~~
- ~~Conducting or soliciting illegal activities such as attempting to gain unauthorized access to restricted sites (hacking) is prohibited.~~
- ~~Misrepresenting yourself as another individual or organization is prohibited.~~

- ~~Sending, posting, recording or encouraging receipt of messages or information that may be offensive or harassing because of their sexual, racist or religious content, is obscene or threatening, and/or is defamatory is prohibited.~~

- ~~Creating unauthorized Intranet sites or pages or sharing of any copyrighted material is prohibited.~~

- ~~No Individual may implement wireless technology without the review and approval of the OCIO. Only authorized IT staff may install a wireless access device to the Internal Network connection jack, port, PC, or other devices connected to the Internal Network.~~

- ~~Use of the Internal Network to perform any malicious activity, including the deliberate spread software viruses, unsolicited email messages, or intentional installation of malicious software of any kind is strictly forbidden.~~

- Email messages are property of the State of Nebraska. ~~Forwarding email messages containing State Information from a State of Nebraska email account to a personal email account is prohibited unless that activity is approved by the OCIO, SISO, or AISO.~~

~~8-202. Personnel Security~~

~~New Hires~~

~~New hires are required to attend Security and Privacy training within 30 days of receiving their credentials, and shall be prohibited from accessing Confidential or Restricted information until this training is complete.~~

~~Access shall be limited to the minimum necessary access required to perform assigned duties, and all personnel are required to read and understand this policy and their obligations in protecting State of Nebraska information.~~

~~Terminations~~

~~Accounts that have been inactive for 180 consecutive days will be disabled. Accounts that have been inactive for thirteen (13) months will be deleted. Activity logs and records related to all accounts shall be maintained for a minimum of five (5) years after the account is deleted. These logs and records will be classified as Restricted information and secured appropriately.~~

~~Temporary accounts for the Staff and Vendors will be terminated or renewed annually, and records will be kept on this activity. Records shall be maintained for five (5) years. Staff that has terminated employment will have their credentials disabled immediately, but no later than 24 hours of their departure.~~

~~Individual Accountability~~

~~Each user must understand his/her role and responsibilities regarding information security issues and protecting State information. Access to State of Nebraska computer(s), computer systems, and networks where the data owner(s) has authorized access, based upon the "Principle of Least Privilege", must be provided using individually assigned unique computer identifiers, known as UserIDs, or other technologies including biometrics, token cards, etc.~~

~~Every individual is responsible for reasonably protecting against unauthorized activities performed with their UserID.~~

~~Associated with each UserID is an authentication token, such as a password or pin, which must be used to authenticate the person accessing the data, system or network. These authentication tokens or similar technology must be treated as confidential information, and must not be shared or disclosed.~~

~~Segregation of Duties~~

~~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.~~

~~8-203. Software Management~~

~~System Software~~

~~Access to operating system code, services and commands must be restricted to only those individuals necessary in the normal performance of their job responsibilities.~~

~~Shared accounts are prohibited for systems that store, process, or access Confidential or Restricted information.~~

~~Default administrator accounts must be renamed, removed or disabled. Default passwords for renamed or disabled default administrator accounts must be changed. Passwords are subject to periodic password change requirements.~~

~~OCIO shall maintain an accurate inventory of all system software, including licensing and usage information, used within the State of Nebraska infrastructure.~~

~~Changes to system software shall follow change management procedures as defined in 8-207.~~

~~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 shall be backed up and access restricted to authorized personnel only. Application changes are required to go through a SDLC process that ensures the confidentiality of information, and integrity/availability of source and executable code. Application changes shall follow Change Management processes as defined in 8-207.~~

~~8-204. Hardware Management~~

~~Computer assets must be physically protected from physical and environmental hazards to reduce the risk of unauthorized access to information and to protect against loss or damage. Special controls may be necessary for electrical supply and uninterruptible power, fire protection and suppression, air and humidity controls, and cabling infrastructure in data centers, wiring closets, server rooms, and storage facilities where computers and computer peripherals are stored.~~

~~Agencies are required to keep an inventory of all information technology hardware used within their environment. This inventory shall include specific details including:~~

- ~~Network diagram of hardware location related to security protections~~
- ~~Hardware Manufacturer~~
- ~~Hardware Model Number~~
- ~~Serial numbers~~
- ~~Firmware Version (if applicable)~~
- ~~Configuration settings and hardening requirements (for "sensitive" hardware)~~

~~Hardware changes shall follow Change Management processes as defined in 8-207.~~

~~8-205~~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. ~~These change control procedures will apply to agency business applications as well as systems software used to maintain operating systems, network software, hardware changes, etc.~~

The change management process ~~can~~ 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~~ state's environment. All changes to network perimeter protection devices should be included in the scope of ~~Change~~ change ~~Management~~management.

IT Infrastructure - The following change management standards are required to be followed for all IT infrastructure.

1. The ~~OCIO~~ 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 ~~OCIO~~Office of the CIO, ~~Department IT~~agency, ~~State Information Security Officer~~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.

2. All records, meetings, decisions, and rational of the ~~Change~~ change ~~Control~~ control group ~~shall~~ 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:

A. Change summary, justification and timeline;

B. Functionality, ~~Regression~~regression, ~~Integrity~~integrity, and ~~Security~~ security ~~Test~~ test plans and results;

C. Security review and impact analysis;

D. Documentation and baseline updates; and

E. Implementation timeline and recovery plans.

3. The ~~OCIO or A~~agency is required to maintain baseline configuration documentation in use throughout the infrastructure. These baseline configuration documents shall be categorized as ~~Confidential~~ CONFIDENTIAL 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.

4. 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.

~~5. All ports, services, protocols, etc. on all technology that is not needed to support State business shall be disabled. This information shall be documented, and the State Information Security Officer will conduct a review of the environment on a periodic basis to ensure that only necessary and required ports, services, protocols, etc. remain enabled.~~

Application Development – The following change management standards are required to be followed for application software systems that create, process, or store ~~Confidential~~ CONFIDENTIAL or ~~Restricted~~ RESTRICTED data.

1. Application change management processes ~~shall~~ must be performed with assigned responsibilities to ensure all changes to ~~appropriate OCIO or Agency~~ application software are approved and documented. Change management teams will include appropriate application development staff and appropriate staff to represent ~~State~~ state ~~Information~~ information ~~Security~~ 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 will retain a documented history of the change process as it passes through the ~~SDLC~~ software development life cycle with documentation securely stored for audit purposes. Documentation should address a review of the following:

A. Change summary, justification, and timeline;

B. Functionality, ~~Regression~~regression, ~~Customer~~ customer ~~Acceptance~~acceptance, and ~~Security~~ security ~~Test~~ test plans;

C. Security review and impact analysis;

D. Documentation and baseline updates; and

E. Implementation timeline and recovery plans.

4. Changes to software applications must be controlled and production installations ~~shall~~ must be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code ~~shall~~ 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~~ that ensure the confidentiality, integrity, and availability of the data maintained in the production library.
6. Application development changes that impact IT infrastructure must be submitted to the ~~Infrastructure~~ infrastructure change management process for review, approval, and implementation coordination.

~~8-206. Identification Badges~~

~~Only authorized individuals are allowed to enter State of Nebraska facilities that contain sensitive information. Those individuals will be issued an electronic identification (ID) badge. All authorized individuals are required to scan their ID badge before entry into these sensitive facilities. ID badges must be visible always, 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 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 unsupervised areas such as data centers. If it is necessary for a Visitor to enter an unsupervised 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.~~

~~Access to certain secured areas requires additional approval. Access to secured IT areas, such as data centers and network closets, must be approved by the OCIO, and access to certain other secured areas must be approved by the SISO before access is allowed. All access to secured areas shall be electronically logged and monitored, and any temporary access to these areas must include an authorized escort.~~

~~8-207. Operational and Functional Responsibilities~~

~~Agencies that create, use or maintain information systems for the State of Nebraska must create and maintain an information security program that ensures the confidentiality, availability, integrity, of the State's information assets.~~

~~All information processing facilities must have detailed documented operating instructions, management processes and formal incident management procedures authorized by agency management and protected from unauthorized access. Where an agency provides a server, application or network services to another agency, operational and management responsibilities must be coordinated by both agencies.~~

~~Agency Accountability~~

~~All agency information must be protected from unauthorized access to help ensure the information's confidentiality and privacy while maintaining its integrity and availability. As with other assets, not all information has the same use or value, and therefore information requires different levels of protection. Each agency will follow established data classification processes as defined in **Data Classification** (see Policy 8-900). All information will be classified and managed based on its level of sensitivity.~~

~~Including Security in Job Responsibilities~~

~~Specific security roles and responsibilities for those individuals responsible for information security must be documented. Each Agency will have an individual assigned to ensure all security policies and procedures are implemented and managed within that Agency, and meet all State of Nebraska Information Security Policies and Procedures.~~

~~8-208. Right to Monitor and Record~~

~~Consistent with applicable law, employee contracts, and agency policies, the OCIO reserves the right to monitor, inspect, and/or search all State of Nebraska information systems at any time. Since agency computers and networks are provided for business purposes, staff shall have no expectation of privacy of the information stored in or sent through these information systems. The OCIO additionally retains the right to remove from agency information systems any unauthorized material.~~

~~Monitoring System Access and Use~~

~~Activities of information systems and services must be monitored and events logged to provide a historical account of security related events. Agencies will implement appropriate audit logs to record events, exceptions and other security-relevant events. The Agency Information Security Officer or designee will regularly review logs for abuses and anomalies. Logs will be kept consistent with Record Retention schedules developed in cooperation with the State Records Administrator and agency requirements to assist in investigations and access control monitoring.~~

~~Only individuals with proper authorization from the OCIO will be permitted to use "sniffers" or similar technology on the network to monitor operational data and security events on the State network. Network connection ports should be monitored for unknown devices and unauthorized connections.~~

~~8-209. Mobile Computing Devices and Portable Media~~

~~Portable Devices~~

~~All portable computing devices (e.g. notebooks, USB flash drives, PDA's, laptops and mobile phones) and information must be secured to prevent compromise of confidentiality or integrity. No device may store or transmit confidential or restricted information without approved encryption enabled on the device or other suitable protective measures that are approved by the agency data owner(s) and the State Information Security Officer.~~

~~Special care must be taken to ensure that information stored on the device is not compromised. Appropriate safeguards must be in place for the physical protection, access control, cryptographic technique, back up, virus protection, and proper connection to the State network. All mobile devices must utilize the screen locking feature on their device when not in use and after 15 minutes of inactivity.~~

~~Devices storing sensitive and/or critical information must not be left unattended and, where possible, must be physically locked away, or utilize special locks to secure the equipment.~~

~~Employees in the possession of portable devices must not check these devices in airline luggage systems. These devices must remain in the possession of the traveler as hand luggage unless restricted by Federal or State authorities.~~

~~All mobile computing devices containing or accessing Confidential or Restricted Information must be provisioned to meet these security policies and be approved by the OCIO and SISO. All devices that will be connected to the network must be logged with device type and approval date.~~

~~8-210~~8-203. ~~Multi Function~~Multi-Function Devices ~~(MFD)~~

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

Configuration and management of ~~MFDs~~ multi-function devices ~~shall~~must include minimum necessary access to the processing, storing, or transmitting functions ~~of the MFD~~. All unnecessary network protocols and services ~~shall~~ must be disabled. Access controls ~~shall~~ must be in place, and administrator privileges ~~shall~~ must be controlled and monitored. Auditing and logging ~~of MFDs shall~~must be enabled. Access to the internal storage ~~of the MFD will~~must be physically controlled.~~, and those storage devices shall~~ The devices must be securely disposed or cleansed when no longer needed. Software and firmware ~~of the MFD shall~~must be updated to the latest version supported by the ~~Vendor~~vendor. All ~~Confidential~~ CONFIDENTIAL or ~~Privileged~~ RESTRICTED ~~Information~~ information ~~shall~~ 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 ~~MFD~~ device stores information and is not capable of encrypting internal storage, then it must be physically secured or not used for ~~Confidential~~ CONFIDENTIAL or ~~Restricted~~ RESTRICTED information. Encryption technology must be approved by the ~~SISO~~ state information security officer or ~~AISO~~agency information security officer.

~~Auditing and logging of MFDs shall be enabled. This includes creating and securing logs on the MFD and its print spoolers, auditing of user access and fax logs (if fax is enabled), and review of audit logs by authorized personnel.~~

~~8-211~~8-204. Email~~, Messaging, and Communication~~

~~**Electronic Mail**~~

~~Electronic mail provides an expedient method of creating and distributing messages both within the organization and outside of the organization. Users of the state E-mail system are a visible representatives of the state and must use the system in a legal, professional and responsible manner. An account holder, user, or administrator~~ Users of the ~~State~~ 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 of Nebraska~~state network unless approved by the state information security officer or the agency information security officer.

~~Email containing Confidential or Restricted information may not be sent to an account outside of the State of Nebraska network unless the contents of that email are encrypted.~~CONFIDENTIAL or RESTRICTED data should not be sent by email unless it has been encrypted using technology approved by the state information security officer or the agency information security officer.

~~**Telephones and Fax Equipment**~~

~~Communication outside the state telephone system for business reasons is sometimes necessary, but it can create security exposures. Employees should take care that they are not overheard when discussing~~

~~sensitive or confidential matters; avoid use of any wireless or cellular phones when discussing sensitive or confidential information; and avoid leaving sensitive or confidential messages on voicemail systems.~~

~~**Modem Usage**~~

~~Connecting modems to computer systems on the state network is prohibited unless a risk assessment is performed, risks are appropriately mitigated, and the Office of the Chief Information Officer approves the request.~~

8-205. Portable Media

CONFIDENTIAL or RESTRICED data should not be stored on portable media unless it has encrypted using technology approved by the state information security officer or the agency information security officer.

~~8-212. Printed Material~~

~~Regardless of its form, electronic or printed, all Information shall be classified and secured with controls that are commensurate with its classification. It is required to maintain two barriers to access any printed material containing Confidential or Restricted information always. Barriers to access include, but are not limited to:~~

- ~~Physical presence and observation by trusted personnel~~
- ~~Locked file cabinets or drawers~~
- ~~Locked office~~
- ~~Locked trunk of a car~~
- ~~The secured State campus and locked facilities~~
- ~~Video surveillance with motion sensor and alerting~~
- ~~Sealed envelope~~

~~Unattended Confidential or Restricted information shall be secured, even when located in a secured facility.~~

~~8-213~~8-206. Facilities; Physical Security Requirements ~~for system facilities~~

~~To detect and prevent unauthorized access attempts in areas within facilities that house sensitive or confidential information, where possible, agencies must utilize physical access controls designed to permit access by authorized users only that identify, authenticate and monitor all access attempts to restricted areas within agency facilities.~~

Agencies ~~will~~ must perform a periodic threat and risk assessment to determine the security risks to facilities that contain ~~State~~ 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 ~~confidential~~ CONFIDENTIAL or ~~restricted~~ RESTRICTED 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. ~~Confidential~~ CONFIDENTIAL or ~~Restricted~~ RESTRICTED information must maintain at least two barriers to access at all times.

8-206. Facilities; Identification Badges and 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.

~~8-214~~8-207. State and Agency Security Planning and Reporting

~~It is the Policy of the State of Nebraska that the Information Security Program includes oversight and reporting as defined by these standards. The purpose of the Nebraska Information Security Reporting Policy and Procedures is to provide the State and Agency leadership with appropriate information in a consistent format to support their information security planning, fact-based decision-making and allocation of future funding. Consistent reporting standards will also help to ensure that information security controls are consistent across the State of Nebraska's Information Technology infrastructure, meet all necessary regulations and requirements, and are appropriate for the level of risks facing the State and various Agencies. Formal reporting helps keep the information security mission consistent, well understood and continually progressing as planned.~~

~~***Required Reports and Standards:***~~

The following standard and recurring reports are required to be produced by the ~~SISO~~ state information security officer and each ~~AISO~~agency information security officer:

1. Information ~~Security~~ security ~~Strategic~~ strategic ~~Plan~~ plan;~~for the State/Agency~~
2. System ~~Security~~ security ~~Plan~~plan(s); and
3. Plan of ~~Actions~~ actions and ~~Milestones~~ milestones (POA&M).

These reports will reflect the current and planned state of information security at the ~~Department~~agency.

A. Information Security Strategic Plan

Proper risk-based planning is critical to ensure the most appropriate projects are prioritized and funded by the ~~State~~ state and its ~~Agencies~~agencies. Information ~~Security~~ security planning is no exception. Planning for information protection ~~will~~ should be given

the same level of executive scrutiny at the ~~State~~ state as planning for information technology changes. This plan ~~shall~~ must be updated and published on an annual basis, and should include a 5-year projection of key security business drivers, planned security infrastructure implementation, and forecasted costs. It should include an educated view of emerging threats and protections, and an analysis of the potential impacts to ~~State/Agency~~state information assets. This plan is necessary to ensure that information security is viewed as a strategic priority, and is included as part of the overall ~~State of Nebraska~~ 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~~ for the State/Agency~~, and the corresponding changes required for ~~Information~~ information ~~Security~~ security to stay aligned with these plans.
3. Summary of the overall ~~State/Agency Information~~ information ~~Risks~~ risks ~~Assessments~~ assessments and current risk levels. Detailed descriptions of significant security risks, and plans to mitigate or remediate those risks.
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~~policies, ~~Standards~~standards, and ~~Procedures~~ procedures for ~~State/Agency Information~~ information ~~Security~~security, and projected changes necessary to stay current and relevant.
6. Summary of the ~~Information~~ information ~~Security~~ security ~~Education~~ education and ~~Awareness~~ awareness ~~Program~~program, progress, and timeline of events.
7. Summary of ~~Disaster~~ disaster ~~Recovery~~ recovery and ~~Business~~ business ~~Continuity~~ continuity activity and plans.
8. Analysis of the regulatory and contractual compliance environment, including potential new regulations or pending contractual requirements that will affect ~~State/Agency Information~~ information ~~Security~~security.
9. Proposed five-year timeline of events and key deliverables or milestones.
10. Line item cost projections for all information security activity that is itemized by:
    a. Steady ~~State~~ state ~~Investments~~investments: The costs for current care and maintenance of the information security program.
    b. Risk ~~Management~~ management and ~~Mitigation~~mitigation: The line item expenses necessary to mitigate or resolve security risks for the ~~Agency~~ agency in a prioritized order.
    c. Future ~~Technology~~technology: The line item forecasted expenses and timelines necessary to support emerging or changing technology, and to be ready for new and emerging threats~~ to State/Agency information~~.

d. Regulatory: The line item expense necessary to meet all regulatory and contractual compliance requirements.

B. System Security Plan

~~State and Agency information assets have become increasingly more difficult to protect due to advances in technology such as easy-to-use high-level query languages, the use of personal computers, the accelerating use of the Internet and other networks, as well as universal familiarity with data processing. Because new technology is too often adopted before protective measures are developed, these factors have resulted in increased vulnerability of information and information systems. Without a corresponding growth in good information security practices, such advances could result in a higher likelihood of inadvertent or deliberate corruption of State information assets and even the loss of the public's trust in the State of Nebraska information integrity and credibility.~~

The ~~State~~ state and ~~Agency~~ agency ~~System~~ system ~~Security~~ security ~~Plan~~ plan (SSP) provides an overview of the security requirements of the information system including all ~~State/Agency~~ 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~~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 address all ~~Control~~ control ~~Areas~~ areas identified in the NIST 800-53 control framework, and ~~shall~~ will describe the current controls in place to protect information at a level commensurate with the sensitivity level of the system.

The ~~State Information Security Officer~~state information security officer will work with each ~~AISO~~ agency information security officer to maintain an SSP incorporating each identified system managing information or used to process ~~Agency~~ agency business.

The ~~AISO~~ agency information security officer and the ~~SISO~~ state information security officer are required to develop or update the SSP in response to each of the following events:

- New system
- Major system modification
- Increase in security risks / exposure
- Increase of overall system security level
- Serious security violation(s)
- 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~~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~~ business ~~Process~~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. Describe information flow and how information is handled. 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 sensitive information, including ~~Confidential~~ CONFIDENTIAL and ~~Restricted~~ RESTRICED 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. Detailed information security descriptions, procedures, protocols, and~~/or~~ implemented controls for all NIST 800-53 control areas within the scope of the system. Identify compensating controls or compliance gaps within this section of the SSP.

8. System interconnection or information sharing: Describe all interfacing or connections between two or more systems or business partners.

9. Applicable laws, regulations, or compliance requirements:~~-~~ ~~list~~ List any laws, regulations, or specific standards, guidelines that specify requirements for the ~~Confidentiality~~confidentiality, ~~Integrity~~integrity, or ~~Availability~~ availability of information in the system.

10. Review of security controls and assessment results that have been conducted within the past three years.

11. Information ~~Security~~ security ~~Risk~~ risk ~~Assessment~~ 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.

C. Plan of Action and Milestones Report (POA&M)

The POA&M is a reporting tool that outlines weaknesses and delineates the tasks necessary to mitigate them. The ~~State/Agency Information~~ information ~~Security~~ security POA&M process will be used to facilitate the remediation of ~~Information~~ information ~~Security~~ security and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions
- Defining roles, responsibilities, and accountabilities for weakness resolution

- Assisting in identifying the security funding requirements necessary to mitigate weaknesses
- Tracking and prioritizing resources
- Ensuring appropriate progress and priorities are continually addressed
- Informing decision makers

The POA&M process provides significant benefits to the ~~State of Nebraska~~state. It is a dynamic management tool useful for ongoing efforts to address programmatic and system-specific vulnerabilities. It assists in essential decision-making activities, facilitating and helping to ensure the oversight and mitigation of security weaknesses and the cost-effective use of mitigation resources. To function effectively, a POA&M must be continually monitored and diligently updated. The ~~SISO~~ state information security officer and ~~AISOs~~ agency information security officers are responsible for maintaining the POA&M and for providing quarterly updates to the ~~State/Agency Leadership~~ leadership~~team~~.

Contents of the Information Security Plan of Action with Milestones:

1. Source – Identifies the audit, review, event or procedure which identified this action item
2. ID – Identification tracking number of this action item which can be tied to the source and timeframe of identification
3. Project/Task – Defines the project, task objective and goals of the action item
4. Key ~~Content~~ content and ~~Description~~ description – Narrative describing the key elements of the action item
5. Key ~~Milestones~~ milestones – Lists each measurable activity required to complete the action item
6. Milestone ~~Status~~ status – Lists the status of each milestone (Open, Completed, Closed Assigned, In Progress)
7. Target or ~~Completion~~ completion ~~Date~~ date – Expected date each milestone will be completed. The ~~Department~~ agency should also accommodate approved changes to target dates in a manner that reflects the new date while keeping record of the original due date.
8. Responsible ~~Party~~ party – List of individuals or support unit assigned to address the action item

ARTICLE 3

ACCESS CONTROL

8-301. Remote Access Standard

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

~~**Purpose and Objectives**~~

~~As employees and organizations utilize remote connectivity to the State of Nebraska networks, security becomes increasingly important. Accompanying and contributing to this trend is the explosive growth in the popularity of broadband connections and other technologies for remote access. These standards are designed to minimize the potential exposure from damages which may result from unauthorized use of resources; which include loss of sensitive or confidential data, intellectual property, damage to public image or damage to critical internal systems, etc. The purpose of this document is to define standards for connecting to any State of Nebraska agency from any host.~~

~~Objectives include:~~

- ~~Provide requirements to State of Nebraska agencies for employees, contractors, vendors and any other agent that requests remote access to any State of Nebraska network.~~
- ~~Provide a high level of security that uses standardized technology and remains adaptable in the face of changing technology products.~~
- ~~Ensure a solution that is scalable to meet the current and future needs of state agencies, their employees, clients and customers, and business partners.~~
- ~~Meet federal security requirements for remote access control.~~

~~**Remote Access Standards and Requirements**~~

The following standards apply to all ~~Workforce (employees and contractors)~~staff that connect to ~~State of Nebraska IT assets~~the state network through the Internet. This includes all approved work-from-home arrangements requiring access to ~~State~~ state systems and ~~Agency~~ agency office locations that use the Internet to access the ~~State of Nebraska~~state network. Each state agency will be responsible for ensuring that remote access to ~~State~~ state resources is secured and compliant with this ~~Policy~~policy.

~~External access from a personally owned computer or a computer not owned, maintained, or approved by OCIO is prohibited from accessing any State of Nebraska network resources that store, process, or access Confidential or Highly Restricted information. Exceptions must be approved in advance by the AISO, OCIO and the SISO. All remote access must occur via an OCIO or Agency authorized and configured remote access connection. Remote access for Staff must have prior authorization by and be requested by their~~

~~Supervisor or Division Management. No classified information other than Public information may be stored on a personal device. These requirements do not apply to remote access to web applications or systems intended for public access.~~

(1) The following are the general requirements for remote access:

(a) Requests for remote access must be reviewed and approved by the state information security officer and the agency information security officer prior to access being granted.

(b) Staff approved for remote connectivity are required to comply with all policies and standards~~, and are required to have approval from AISO and the SISO. Staff are prohibited from using such equipment for private or inappropriate purposes as defined in State and Agency Acceptable Use Policies~~.

(c) All ~~personal~~ 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 ~~S~~state equipment.

(d) All remote access sessions ~~shall~~must be logged. ~~OCIO,~~The Office of the CIO or the ~~A~~agency ~~IT Team shall~~will perform periodic monitoring of ~~the~~ remote access sessions ~~and~~with random inspections of the user security settings and protocols to ensure compliance with this policy ~~and standards~~.

(e) Remote access logon failures ~~shall~~must be logged. Credentials ~~shall~~must be disabled after three (3) consecutive failed login attempts.

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

(g) ~~Nebraska workforce~~Staff with remote access privileges must ensure that their computer which is remotely connected to the ~~S~~state network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.

(2) The following are additional requirements for remote access to data classified as CONFIDENTIAL or RESTRICTED:

(a) Requests for remoted access must indicate if CONFIDENTIAL or RESTICTED data may be accessed.

(b) Mechanisms must be employed to ensure personally identifiable information, or other sensitive information cannot be downloaded or remotely stored.

(c) All ~~S~~state owned or managed ~~portable~~ devices ~~that have the ability to store Confidential or Highly Restricted information~~ must be password protected and full-disk encrypted using approved technology. Encryption technology ~~will~~must be provided or approved by the ~~OCIO~~Office of the CIO ~~and should be FIPS 140-2 compliant~~.

(d) Remote sessions that store, process, or access ~~Confidential or~~CONFIDENTIAL or ~~Highly Restricted~~RESTRICTED information or systems must use access control credentials and an approved form of multi-factor authentication before connecting to the ~~S~~state network. Remote sessions must employ ~~OCIO~~Office of the CIO approved cryptography during the entire session when connected to the ~~S~~state network.

~~1. Staff approved for remote connectivity are required to comply with all policies and standards, and are required to have approval from AISO and the SISO. Staff are prohibited from using such equipment for private or inappropriate purposes as defined in State and Agency Acceptable Use Policies.~~

~~1. It is the responsibility of all Staff with remote access privileges to the State of Nebraska network to ensure that their remote access work environment is given the same security consideration as the user's on-site connection to the State network. All personal 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. This monitoring shall ensure the remote computer is free from Spyware, Adware, rootkits, or any other threats that would place State resources in jeopardy.~~

~~2. Staff shall use State provided or approved equipment and software for authorized activities only.~~

~~3.~~1. ~~All remote access sessions shall be logged. OCIO, or the Agency IT Team shall perform periodic monitoring of the remote access session and random inspection of the user security settings and protocols to ensure compliance with policy and standards.~~

~~4. All remotely accessible information systems containing Confidential or Restricted data must employ mechanisms to ensure Personally Identifiable Information (PII), or other sensitive information cannot be downloaded or remotely stored.~~

~~5. Remote access to Confidential or Restricted information, unless explicitly approved by the SISO and/or AISO, is prohibited.~~

~~6.~~1. ~~All State owned or managed portable devices that have the ability to store Confidential or Highly Restricted information must be password protected and full disk encrypted using approved technology. Encryption technology will be provided or approved by the OCIO and should be FIPS 140-2 compliant.~~

~~7.~~1. ~~Remote sessions that store, process, or access Confidential or Highly Restricted information or systems must use access control credentials and an approved form of multi-factor authentication before connecting to the State network. Remote sessions must employ OCIO approved cryptography during the entire session when connected to the State network.~~

~~8. Staff with remote access privileges to the State network must only use their assigned State @nebraska.gov email account to conduct State of business. Use of personal email accounts such as Hotmail, Yahoo, Gmail or other external resources to conduct official business will be considered an unauthorized disclosure and may result in a disciplinary action.~~

~~9. Remote access logon failures shall be logged. Credentials shall be disabled after three (3) consecutive failed login attempts.~~

~~10. Remote sessions shall be locked after 15 minutes of inactivity until the user re-establishes access with the appropriate credentials and authentication procedures.~~

~~11. At no time, should any State employee or contractor provide their login or email password to anyone, not even family members.~~

~~12. Nebraska workforce with remote access privileges must ensure that their computer which is remotely connected to the State network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.~~

~~13. OCIO will authorize, document, and monitor all remote access capabilities and connections used on the system. The SISO and AISO are required to approve all remote access requests.~~

~~14. The SISO and or AISO will provide annual training for all staff authorized for remote access to the State network. This training shall include details on remote work location security, protection of mobile devices, and incident identification and reporting.~~

~~**Remote Access from Non-State Owned and/or Managed Devices, when approved**~~

~~Remote access from devices not owned, controlled or managed by the OCIO or Agency IT department must be approved by the OCIO or Agency before accessing State of Nebraska networks.All Remote Access Users must sign and renew annually an agreement with the State and/or Agency which addresses at a minimum the following:~~

- ~~Remote access users are responsible for all actions incurred during their session in accordance with all State of Nebraska and agency standards and policies.~~
- ~~All home networks connected to the Internet via a broadband connection should have a firewall installed, updated and operational.~~
- ~~Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion.~~
- ~~Operating systems should contain the most current security patches.~~
- ~~All home computers must contain an Anti-Virus program with current signatures and that the computer is free from Spyware, Adware, and rootkits.~~
- ~~Devices must have "split tunneling" disabled, which prevents unauthorized connections to the State network.~~
- ~~Remote access to Confidential or Restricted information is prohibited on these devices, unless approval is granted by the Office of the CIO.~~

8-302. Minimum Password Configuration

A. Minimum Password Requirements

The following are the minimum password requirements for ~~State of Nebraska~~state government passwords:

- Must contain a minimum Eight (8) characters
- Must contain at least Three (3) of the following Four (4):
- At least One (1) uppercase character
- At least One (1) lowercase character
- At least One (1) numeric character

- At least One (1) symbol (!@#$%^&)
- Cannot repeat any of the passwords used during the previous 365 days.

In addition to the ~~Minimum~~ minimum ~~Password~~ password ~~Complexity~~ 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 of Nebraska~~state shall use a password that follows at least a confidential level of authentication when logging into a state network or application.

B. Additional Access Requirements for ~~Restricted~~ RESTRICTED Information

Information that is ~~deemed Restricted~~~~requires~~classified as RESTRICTED requires the highest level of security. This includes ~~Root~~root/~~Admin~~ admin level system information accessed by ~~Privileged~~ privileged accounts. A password used to access ~~Restricted~~ RESTRICTED information must follow the password complexity rules outlined in ~~8-303 (A)~~subsection A, and must contain the following additional requirements:

- Multi-factor authentication
- Expire after 60 days
- Minimum Password Age set to 15 days
- Accounts will automatically be disabled after three unsuccessful password attempts

C. Additional Access Requirements for ~~Confidential~~ CONFIDENTIAL Information

Information that is ~~deemed Confidential~~classified as CONFIDENTIAL requires a high level of security. A password used to access ~~Confidential~~ CONFIDENTIAL information must follow the password complexity rules outlined in ~~8-303 (A)~~subsection A, and must contain the following additional requirements:

- Expire after 90 days
- Accounts will automatically lock after three consecutive unsuccessful password attempts

D. Password Requirements for ~~Managed Access Public~~MANAGED ACCESS PUBLIC Information

Information that is ~~deemed Managed Access Public~~classified as MANAGED ACCESS PUBLIC requires minimal level of security and need not comply with ~~section 8-303 (A). of this policy~~subsection A. Typically, this data would not include personal information but may carry special regulations related to its use or dissemination. ~~Managed Access Public~~MANAGED ACCESS PUBLIC data may also be data that is sold as a product or service to users that have subscribed to a service.

E. Password Requirements for Accessing ~~Public~~ PUBLIC Information

Information that is ~~deemed Public~~classified as PUBLIC requires no additional password security and need not comply with ~~section 8-303 (A) of this policy~~subsection A.

F. 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 ~~8-303 (A)~~subsection A. The additional requirements for access to ~~Confidential or Highly Restricted~~ CONFIDENTIAL or RESTICTED ~~Information~~ data with a non-expiring password are:

- Extended password length to 10 characters
- Independent ~~Remote~~ remote ~~Identity~~ identity ~~Proofing~~ proofing may be required
- Personal security question may be asked
- Multi-factor authentication
- Any feature not included on this list may also be utilized upon approval of the ~~State Information Security Officer~~ state information security officer~~or upon enactment of federal, state or departmental laws, policies or directives~~.

G. 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~~state information security officer.

H. 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 ~~Confidential~~ CONFIDENTIAL or ~~Highly Restricted~~RESTRICTED information.

I. 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~~ user ID is used to authenticate the device itself to the system and not a person.

8-303. Identification and Authorization

A. All ~~Workforce~~ staff authorized to access any ~~State of Nebraska Information~~state information or IT ~~Resources~~resources, that have the potential to process, store, or access non-public information, must be assigned a unique user ID ~~identification (ID)~~ with the minimum necessary access required to perform their duties.

B. ~~The Workforce is responsible for, and can be held accountable for, the actions conducted with their user ID and~~ Staff are required to secure their user IDs from unauthorized use. ~~It is the responsibility of Management to ensure that only minimum necessary access is provided within their department.~~

C. Sharing user IDs is prohibited.

D. 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.

~~Each user requiring access to the State network, with the potential to process, store, or access non-Public information, has an individual user ID issued to them.~~

8-304. Privilege Access Accounts

Privileged access ~~Accounts~~ 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 State of Nebraska requires~~ the following standards and procedures ~~to~~ must be followed to minimize the risk of incidents caused by these accounts:

- All privileged access accounts must be assigned to an individual with an approved business need for the privileged access. These accounts ~~will~~must not be shared.
- Default administrator accounts must be renamed, removed or disabled. Default passwords for renamed or disabled default administrator accounts must be changed.
- Default system account credentials for hardware and software must be either disabled, or the password ~~shall~~ must be changed ~~immediately~~. Use of anonymous accounts is prohibited, and unassigned accounts must be assigned to an individual prior to use. When no longer needed, the account ~~shall~~ must be disabled ~~and password changed~~. At all times, the ~~State~~ state requires individual accountability for use of privilege accounts.
- ~~Accounts with p~~Privileged access accounts will have enhanced activity logging enabled~~, pursuant to *8-708 Audit Requirements*~~. The ~~OCIO~~ Office of the CIO and all applicable ~~Agencies~~ agencies will perform a quarterly review of privileged access account activity~~;~~.
- ~~All privileged access accounts must be assigned to an individual with an approved business need for the privileged access. These accounts will not be shared.~~
- Privileged access through remote channels will be allowed for authorized purposes only and must include ~~Multi~~multi~~-Factor~~ factor ~~Authentication~~authentication.
- Passwords for these accounts must be changed every 60 days~~;~~.
- The password change process ~~shall~~ 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,~~.
- ~~Requests for privileged~~ Privileged access accounts must ~~include~~ be ~~approval~~ approved,~~from the OCIO and must be~~ provisioned, and maintained by the ~~OCIO~~Office of the CIO.

~~8-305. Account Termination~~

~~Accounts that have been inactive for 45 consecutive days will be disabled. Accounts that have been inactive for thirteen (13) months will be deleted. Activity logs and records related to all accounts shall be maintained for a minimum of five (5) years after the account is deleted. These logs and records will be classified as Privileged information and secured appropriately. Deleted accounts will not be reused. Temporary accounts for the Workforce and Vendors will be terminated or renewed annually, and records will be kept on this activity. Records shall be maintained for five (5) years. Staff that has terminated employment will have their credentials disabled immediately, but no later than 24 hours of their departure.~~

ARTICLE 4

NETWORK SECURITY

~~The OCIO 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 OCIO 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 Chief Information Officer.~~

~~Where an agency has outsourced a server or application to a third party service (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 or designee will perform the security review on behalf of all Agencies.~~

~~Additions or changes to network configurations, including through the use of third party service providers, must be reviewed and approved through the OCIO change management process.~~

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 of Nebraska~~state internal network are required to adhere to these standards.

The ~~OCIO~~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 ~~OCIO~~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 ~~S~~state network and direct connections between agencies must be authorized by the Office of the ~~Chief Information Officer~~CIO.

Where an agency has outsourced a server or application to ~~a third party service~~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 ~~or designee~~ will perform the security review on behalf of all ~~A~~agencies.

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

8-402. Network Transmission Security

1 All encryption must be approved by the ~~OCIO or SISO~~state information security officer. Any transmissions over unsecured networks (such as the Internet) that contain ~~Confidential~~ CONFIDENTIAL or ~~Highly Restricted~~RESTRICTED information must be encrypted using technology that is FIPS 140-2 ~~Compliant~~compliant~~, or approved by the SISO~~.

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

3 ~~OCIO~~ The Office of the CIO shall ensure that all networks and systems are monitored 24x7 with authorized tools (such as ~~Network~~ network ~~Based~~ based ~~Intrusion~~ intrusion ~~Detection~~ detection and ~~Prevention~~ prevention ~~Systems~~systems) and personnel to detect system anomalies or security events.

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

8-403. Network Architecture Requirements

1 All devices that store, access, or process ~~Confidential~~ CONFIDENTIAL or ~~Highly Restricted~~RESTRICTED information ~~shall~~ must not reside in the public tier, and must be protected by at least two firewalls. Firewalls ~~shall~~ 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 ~~Confidential~~ CONFIDENTIAL or ~~Restricted~~ RESTRICTED 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 ~~shall~~ 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 of Nebraska~~state network ~~shall~~ will have an annual verification of all open ports, protocols, and services for publicly accessible systems.

~~5~~6 Any requests for public IP addresses or for additional open ports must be approved by the ~~SISO~~state information security officer.

~~6~~7 Staff will follow approved change control and configuration management procedures for ~~Network~~ network devices. Patches and hot-fixes recommended by network hardware or software vendors must be installed as soon as practical after testing.

~~7~~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.

8-404. External Connections

Direct connections between the ~~State~~ state network and external networks must be implemented in accordance with these policies and standards. 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's private~~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.

~~Third party~~External network and~~/or~~ workstation connection~~(s)~~s to the state network must have an agency sponsor and a business need for the network connection. ~~An agency non-disclosure agreement may be required to be signed by a legally authorized representative from the third-party organization. In addition to the agreement, t~~The ~~third party's~~external network equipment must also conform to the state's security policies and standards, and be approved ~~for connection~~ by the ~~OCIO~~Office of the CIO.

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.

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

No wireless network or wireless access point will be installed without the written approval of the ~~OCIO~~Office of the CIO.

All wireless networks ~~shall~~ will be inspected annually by the ~~SISO~~ state information security officer and ~~AISO~~ agency information security officer to ensure proper security protocols are in place and operational.

ARTICLE 5

SYSTEM SECURITY

8-501. System Documentation

1. Only ~~OCIO~~Office of the CIO approved hardware or software is permitted within the ~~State of Nebraska~~state's information technology infrastructure. ~~and on state-owned devices. Personal devices (e.g. smart phones, tablets, laptops etc.) that connect to the Internal Network for email, must use the State of Nebraska provided interface on that device for this access. Requests for additional software must be submitted as directed by the OCIO. Personal software is not allowed on any state-owned equipment.~~

~~2. Documentation of key systems within the State of Nebraska will be maintained and secured as Proprietary information.~~

~~3. Staff are prohibited from downloading or installing software on state owned equipment unless this activity is approved as part of work assignment and authorized by the OCIO.~~

~~4. The State will create and maintain an inventory of all approved hardware and software that can be connected to the Internal Network. All other devices must be approved and recorded by the OCIO before being connected to the Internal Network. The SISO will perform regular monitoring and tracking to ensure that only approved hardware and software exist within the State of Nebraska environment.~~

~~5.~~2. All authorized hardware and software shall be inventoried~~,~~ and documented. Results shall be secured in an auditable fashion.

8-502. Minimum User Account Configuration

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

Administrator level access is ~~a~~ privileged and ~~shall~~ 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.

Local accounts ~~shall~~ 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.

~~8-504~~8-503. Minimum Server Configuration and Patch Management

The ~~State of Nebraska~~state recognizes the National Institute of Standards and Technology (NIST) as ~~the adopted author of~~a source for recommended security requirements that provide minimum baselines of security for servers ~~on the State of Nebraska network~~.

NIST provides instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All ~~State of Nebraska~~state ~~System~~ system ~~Administrators~~

administrators should examine NIST documents when installing ~~and~~ or configuring servers. The documents are not all inclusive, but rather meant as a means of prompting and guiding ~~Administrators~~ administrators through the installation process.

~~**Purpose and Objectives**~~

~~Information technology (IT) is a vital resource to the State of Nebraska; therefore, it is critical that services provided by these systems can operate effectively.~~

~~The purpose of this standard is to establish base configurations and minimum server standards on internal server equipment that is owned and/or operated by the State of Nebraska. Effective implementation of this policy will reduce the risk of unauthorized access and other IT security related events to the State of Nebraska's information and technology systems.~~

~~All state agencies, boards and commissions will~~Agencies must comply with ~~NIST~~the NIST standards, guidelines, and checklists as identified below.

- NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-70, The NIST Security Configuration Checklists Program
- NIST SP 800-44, Guidelines on Securing Public Web Servers

Server Hardening

All servers that store, process, or have access to ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED data are required to be hardened according to these standards. In addition, these servers ~~shall~~ must have a published configuration management plan as defined below and approved by the ~~State Information Security Officer~~state information security officer.

1. Servers may not be connected to the ~~State~~state network until approved by ~~Agency and~~the ~~OCIO~~Office of the CIO ~~Management~~. This approval will not be granted for sensitive servers until these hardening standards have been met or risk levels have been ~~officially~~ accepted by ~~Agency~~agency ~~Management~~management.
2. The ~~Operating~~ operating ~~System~~ system~~(OS)~~ must be installed by IT authorized personnel only, and all vendor supplied ~~OS~~ patches must be applied. All software and hardware components should be currently supported. All unsupported hardware and software components must be identified and have a management plan that is approved by the ~~State Information Security Officer~~state information security officer.
3. All unnecessary software, system services, accounts and drivers must be removed unless doing so would have a negative impact on the server.
4. Logging of auditable events, as defined in NIST 800-53 control objectives, will be enabled. Audit logs will be secured and only accessible to accounts with privileged access.
5. Security parameters and file protection settings must be established, reviewed, and approved by the ~~State Information Security Officer~~state information security officer.
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 Department and as referenced in the National Vulnerability ~~database~~ Database (HTTP://nvd.nist.gov).

7. Hardened servers will be scanned monthly for unauthorized software or unauthorized changes to the configuration baselines.
8. Hardened servers will be monitored with active intrusion detection, intrusion protection, or end-point security monitoring that has been approved by the ~~State Information Security Officer~~state information security officer. This monitoring ~~shall~~ must have the capability to alert IT administrative personnel within 1 hour.
9. Servers ~~shall~~ 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 changes to hardened servers must go through a formal change management and testing process to ensure ~~all~~ the integrity and operability of all security and configuration settings ~~remain intact~~. Significant changes must have a documented ~~Security~~ security ~~Impact~~ impact ~~Assessment~~ assessment included with the change.
11. Remote management of hardened servers ~~shall~~ must be performed over secured channels only. 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.

~~8-505~~8-504. Minimum Workstation Configuration

Improperly configured workstations are at risk to be compromised. Without proper adherence to these workstation security standards, the ~~State~~state is at increased risk to have data lost, stolen, or destroyed. This standard is necessary to protect the ~~State~~state from unauthorized data or activity residing or occurring on ~~State~~state equipment. It is also necessary to reduce the likelihood of malicious activity propagating throughout the ~~State~~state networks or launching other attacks. All managed workstations that connect to the ~~State~~state's network are required to meet these standards. The ~~OCIO~~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. In addition to adherence to the required images, the following standards are defined for all workstations that connect to the ~~State~~state network. The degree of protection of the workstation should be commensurate with the ~~information~~ data classification of the resources stored, accessed, or processed from this computer.

1. Endpoint security (anti-virus) software, approved by the ~~OCIO~~Office of the CIO, must be installed and enabled.
2. The host-based firewall must be enabled if the workstation is removed from the ~~State~~state ~~internal~~ network.
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~~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.

~~6.~~7. Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion.

~~7.~~8. 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.

~~8.~~9. Shared login accounts are forbidden on multi-user systems where the manipulation and storage of ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information takes place.

~~9.~~10. Users need to lock their desktops when not in use. The system ~~shall~~ must automatically lock a workstation after 5 minutes of inactivity.

~~10.~~11. Users are required to store all ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information on IT managed servers, and not the local hard drive of the computer. Local storage ~~can~~ 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~~state. ~~All State laptops with the ability to store data must be fully encrypted using IT approved technology.~~

~~11.~~12. All workstations shall be re-imaged with standard load images prior to re-assignment.

~~12.~~13. Equipment scheduled for disposal or recycling ~~shall~~ must be cleansed following ~~Department~~ agency media disposal guidelines

~~8-506~~8-505. Minimum Laptop Configuration

In addition to the requirements contained in section 8-504, ~~All~~ all laptops that connect to the ~~State of Nebraska~~state network are required to meet ~~these~~ the following requirements. ~~Each state agency will be responsible for ensuring that any device connected to State resources contain an operating Anti-Virus monitoring with current signatures and that the computer is free from Spyware, Adware, rootkits, or any other threats that would place State resources in jeopardy.~~

1. Remote access to ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information must occur through a ~~State~~state-managed endpoint, using the ~~State~~state VPN or other connections that have been approved by the Office of the CIO.

2. Remote access to any privilege functions, such as administrator accounts, must employ multi-factor authentication and all activity ~~shall~~ must be logged for audit purposes.

3. Remote access users are responsible for all actions incurred during their session in accordance with all ~~State of Nebraska~~state and agency standards and policies.

4. All home networks connected to the Internet via a broadband connection should have a firewall installed, updated and operational.

~~5. Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion.~~

~~6. Operating systems should contain the most current security patches.~~

~~7. All home computers must contain an Anti-Virus program with current signatures and that the computer is free from Spyware, Adware, and rootkits.~~

~~8.~~5. Laptops with remote access to, or the capability to store, ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED data are required to be fully encrypted using technology approved by the ~~SISO~~state information security officer.

~~8-507~~8-506. Minimum Mobile Device Configuration

~~The purchase and use of all~~All mobile computing devices ~~containing or~~ accessing the ~~State of Nebraska~~state network~~s~~ ~~and~~ or containing state information must be provisioned to meet these security policies and be approved by the ~~OCIO~~Office of the CIO. All devices that will be connected to the state network must be logged with device type and approval date. ~~Accessories used on corporate computers must be provided by IT or approved by the OCIO.~~

1. Mobile computing devices must be shut down or locked when not in use. These devices ~~may~~ 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 ~~may~~ should not be ~~used by or~~ shared ~~with anyone~~.
2. Mobile computing devices and mobile storage devices must ~~never~~ not be left in a vehicle unattended.
3. Storing ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information on any mobile device or any removable or portable media (e.g., ~~such as.~~ CD~~'~~s, thumb drives, DVD~~'~~s~~, etc.~~) is prohibited unless arrangements and mechanisms for securing the data has been explicitly approved by the ~~SISO~~state information security officer. In those cases, all mobile computing devices or portable media shall be encrypted using technology that is approved by the ~~SISO~~state information security officer.
4. Personally owned mobile devices (e.g., ~~such as~~ smartphones and tablets) may be used for approved ~~State~~state purposes, including email, when configured to access the ~~State of Nebraska~~state ~~Information~~ information through a managed interface or sandbox only. Devices that are not configured to use the authorized interface are prohibited from accessing any ~~State~~state information, including email.
5. ~~It is required to lock or secure~~The device must have security settings ~~so users cannot delete or change~~ that block users from changing mandatory settings.
6. Strong passwords are required, and passwords must change regularly per ~~State~~state policy regarding passwords.
7. ~~It is required that t~~The device must lock after no more than 15 minutes of inactivity~~,~~ and ~~cannot be unlocked without~~must require the re-entry of a password or PIN code to unlock.
8. After 10 unsuccessful password attempts, the device or the ~~State~~state container will be erased. In the event that the device becomes lost or stolen, ~~OCIO~~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 of Nebraska~~state ~~internal~~ 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 ~~are required to~~must be properly disposed of using mechanisms approved by the ~~SISO~~state information security officer. State data ~~needs to~~must be cleared and devices properly disposed of or recycled. The disposition process is required to be documented and periodically audited.
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~~ devices need to be validated before being made available for users to request.

~~8-508~~8-507. System Maintenance

1. All systems ~~using third party software that is~~ involved in the processing, storage, or access to any ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information ~~shall~~ must be maintained per manufacturer specifications. Maintenance personnel ~~shall~~ must be approved for this activity by the ~~State Information Security Officer~~state information security officer and ~~shall~~ must be briefed on the requirements for protecting sensitive information.
2. Maintenance activity ~~will~~ 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 any secured environment, the equipment ~~will~~ must be approved for release and validated by the ~~State Information Security Officer~~state information security officer ~~(or his designate)~~ that all non-public information has been encrypted, secured, or permanently deleted from the equipment. When equipment is returned, it ~~shall~~ 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 ~~shall~~ must be tested. The Office of the CIO ~~and each Agency shall~~must maintain a list of approved maintenance tools that is reviewed and updated at least annually~~, or when required~~.
5. Nonlocal or ~~Remote~~ remote maintenance must be approved in advance by the ~~State Information Security Officer~~state information security officer or the ~~OCIO~~Office of the CIO, and must also comply with all ~~Agency~~agency and ~~OCIO~~Office of the CIO requirements for remote access.
6. All remote maintenance activity ~~will~~ must be logged and reviewed.
7. Maintenance of agency-developed software must follow the ~~State~~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. Critical patches must be applied within 24 hours of receipt. High risk patches must be applied within 7 days of receipt. All other patches must be appropriately applied in a timely manner as ~~defined~~ determined by the ~~Agency~~agency.
9. All ~~third-party~~vendor supplied software deployed and operational ~~within the State~~ must be currently supported by the ~~Vendor~~ vendor~~unless an exception has been requested and approved through the Policy Exception Process~~.

ARTICLE 6

APPLICATION SECURITY

8-601. ~~System~~ Application Documentation

To ensure that security is built into ~~information systems~~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~~agency information security officer ~~or designee~~ must be involved in all phases of the ~~System~~ application ~~Development~~ development ~~Life~~ life ~~Cycle~~ cycle ~~(SDLC)~~ from the requirements definition phase, through implementation and eventual application retirement.

Controls in ~~systems and~~ applications ~~can~~ 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 ~~systems~~ applications that store, access, or process ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information must go through a formal change management process. For recurring maintenance of these ~~systems~~applications, an abbreviated change management process ~~can~~ may suffice if that abbreviated process has been approved by the ~~State Information Security Officer~~state information security officer ~~and the Office of the CIO~~.

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.

~~8-602~~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:

- Access to compilers, editors and other system utilities must be removed from production systems when not required~~; and~~.
- Logon procedures and environmental identification must be sufficiently unique for production testing and development.
- 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.
- 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 ISO~~state information security officer, and to implement production-class controls in the applicable test environment to protect that information.

~~8-603~~8-604. Application Development

The following standards are required to be followed for ~~Department~~ agency developed application software ~~systems~~ that create, process, or store ~~Confidential~~CONFIDENTIAL ~~and~~ or ~~Restricted~~RESTRICTED data.

1. The ~~Agency~~agency ~~will~~ 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~~state ~~Information~~ information ~~Security~~ 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 ~~will~~ must retain a documented history of the change process as it passes through the ~~SDLC~~ application development life cycle with documentation securely stored for audit purposes. Documentation should address a review of the following:
    a. Change summary, justification, and timeline
    b. Functionality, ~~Regression~~regression, ~~Integrity~~integrity, and ~~Security~~ security ~~Test~~ test plans and results
    c. Security review and impact analysis
    d. Documentation and baseline updates
    e. Implementation timeline and recovery plans
4. Changes to software applications must be controlled and production installations ~~shall~~ must be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code ~~shall~~ 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 ~~Department~~ agency IT infrastructure must be submitted to the Infrastructure Change Control Team for review, approval, and implementation

7. The security requirements of new ~~systems~~ applications must be established, documented and tested prior to their acceptance and use. ~~Agency Information Security Officer~~The agency information security officer ~~or designee will~~must ensure that acceptance criteria are utilized for new ~~information systems~~ applications and upgrades. Acceptance testing ~~will~~ must be performed to ensure security requirements are met prior to the ~~system~~ 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 ~~shall~~ must have an appropriate warning banner displayed, applicable to the data being accessed (e.g., PHI, FTI, PII~~, etc~~).

10. Application credentials, where possible, should be inherited from the ~~State~~state ~~Managed~~ managed ~~Authentication~~ authentication ~~Source~~source. If that is not possible, credentials should have the same level of management and approval as other ~~Agency~~agency access credentials.

11. Applications must be configured such that ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED data will be encrypted when transmitted outside the ~~Department~~ agency internal network.

8-605. Security Standards for 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~~state websites, web services, and all ~~third-party~~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).

1. Consider the threats, vulnerabilities, and risks to your application. If you are unsure, follow the ~~Threat~~ threat ~~Risk~~ 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~~confidentiality, ~~Integrity~~integrity, ~~Availabilityof~~ 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 ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED outside of the secured ~~Department~~ agency internal network, that information must be encrypted in all cases – whether stored or in transit. Encryption technology must be approved by ~~OCIO~~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 ISO~~state information security officer. Higher risk or impact applications should be tested annually. This test shall be coordinated and supervised by the ~~SISO~~state information security officer, ~~and ISO~~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.
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 or SANS websites:

https://www.owasp.org/index.php/Category:OWASP_Guide_Project

http://www.sans.org/top25-software-errors/

~~8-604~~8-606. ~~External Hosting of State Data and Cloud Security~~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~~state purposes is prohibited ~~by~~ unless approved by the employee's supervisor or manager. Even if approved, it is prohibited to process or store any ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information with these services, unless the storage is encrypted with approved technology, and has been approved in advance by the ~~SISO~~state information security officer.

8-607. Cloud Computing Standard

~~The following standard provides guidance on the acceptable use of cloud computing services by Nebraska state government agencies.~~

1. DEFINITIONS

1.1 ~~The~~ NIST Definition of Cloud Computing~~:~~

This standard incorporates the following definition from the National Institute of Standards and Technology (*The NIST Definition of Cloud Computing*, NIST Special Publication 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).

1.2 Other Deployment Models

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 ~~State of Nebraska,~~ Office of the ~~Chief Information Officer~~CIO.

~~Other Definitions~~

~~*Data classification*. The data classification system created in the Information Security Policy (NITC 8-101, § 4.6).~~

2. STANDARD

The following table contains the acceptable uses of cloud computing by ~~Nebraska state government~~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 ~~will~~ must be used.

Data Classification	Cloud Deployment Models					
	State Cloud	Private Cloud	Government Community Cloud	Community Cloud	Public Cloud	Hybrid Cloud
~~Restricted~~RESTRICTED	✓				⊘	
~~Confidential~~CONFIDENTIAL	✓		✓		⊘	
~~Managed Access Public~~MANAGED ACCESS PUBLIC	✓	✓	✓	✓	✓	✓
~~Public~~PUBLIC	✓	✓	✓	✓	✓	✓

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

2.1 Prior Approval Process

An agency requesting prior approval of a cloud computing service must submit a ~~Service~~ service ~~Request~~ request to the ~~OCIO~~ 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 ~~OCIO~~ Office of the CIO will respond to the request within four business days. The ~~OCIO~~ Office of the CIO may approve the request, approve the request with conditions, deny the request, or request additional information.

3. EXEMPTION FOR EXISTING SERVICES

Cloud computing services in use on December 31, ~~2016~~2017, are exempt from the requirements of this standard. 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.

4. FedRAMP COMPLIANCE

If the ~~Cloud~~ cloud ~~Service~~ service ~~Providers~~ provider (CSP'~~s~~) does not have an official FedRAMP certification by an accredited third-~~Party~~ party ~~Assessor~~ assessor ~~Organization~~ organization (3PAO) and the CSP may store or process any CONFIDENTIAL or RESTRICTED data, ~~and the CSP is being considered for use by the State,~~ the following conditions must be met or addressed ~~via~~ in an agreement with the ~~service provider~~CSP ~~before engaging any cloud service providers when that cloud service may store or process any Confidential or Restricted data~~:

1. The ~~Cloud~~ cloud ~~Service~~ service ~~Provider~~ 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~~state's internal systems.
2. Access to the cloud service ~~will~~ must require multi-factor authentication based on data classification levels.
3. De-provisioning of credentials must occur within two (2) hours of de-provisioning of the internal system credentials.
4. Information ~~will~~ must be encrypted using IT approved technology for information in transit as well as information stored or at rest.
5. Encryption key management will be controlled and managed by the ~~State~~state unless explicit approval for key management is provided to CSP/3PH by ~~IT~~the agency. ~~This may require an escrow service for key storage.~~
6. All equipment removed from service, information storage areas, or electronic media that contained ~~State of Nebraska~~state information must have ~~all this~~the information purged using appropriate means. Data destruction must be verified by the ~~State before~~state before allowing that equipment, information storage space, or media to be destroyed or assigned for reuse. A ~~Certificate~~ certificate of ~~Destruction~~ destruction must be provided for equipment that has been destroyed.
7. CSP/3PH ~~will~~ must provide vulnerability scanning and testing on a schedule approved by the ~~State ISO~~state information security officer. Results will be provided to ~~Department~~agency.
8. Patch management of hardware and software at the CSP/3PH are required to meet the same standards that are required at ~~State~~state.
9. CSP/3PH ~~will~~ must meet all ~~State of Nebraska~~state requirements for chain of custody and ~~Confidential / Restricted~~ information breach notification ~~if State requires forensic analysis~~. CSP/3PH will maintain an incident management program that notifies ~~State~~the state within one (1) hour of a breach.

10. 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 ~~Department~~gency-authorized parties.
11. CSP/3PH is required to advise the ~~State~~state on all geographic locations of stored ~~State~~state information. CSP/3PH will not allow ~~State~~state information to be stored or accessed outside the ~~USA~~ United States~~without explicit approval by the OCIO~~. This includes both primary and alternate sites.
12. Privileged access roles at the CSP/3PH are required to meet the same vetting standards of privileged access personnel at the ~~State~~state, such as background checks, etc.
13. ~~Contracts with~~ CSP/3PH's ~~shall~~ must have SLAs in place that clearly define security and performance standards. ~~Contracts will address how performance and security will be measured, monitored, and reported. Contracts will also establish an enforcement mechanism for SLA compliance.~~
14. ~~.~~ CSP/3PH will provide adequate security and privacy training to its associates, and provide the ~~SISO~~state information security officer with ~~adequate~~ evidence of this training.
15. CSP/3PH will provide the ~~State~~state with the ~~ability~~ functionality to conduct a ~~reasonable~~ search of the data to meet ~~Nebraska Public Records Law~~public records requests.
16. Before contracting with a CSP/3PH, the ~~State~~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.
17. ~~CSP/3PH will provide documentation, evidence, or reasonable access by the OCIO and SISO to ensure compliance with these standards.~~

ARTICLE 7

AUDITING AND COMPLIANCE

~~8-700~~8-701. Auditing and Compliance Security Standard

It is the responsibility of the ~~SISO~~state information security officer to ensure an appropriate level of ~~Security~~ security oversight is occurring at all potential exposure points of ~~State~~state and ~~Agency~~agency systems and operations so that the ~~State~~state has reasonable assurance that the overall security posture continuously remains intact. The ~~SISO~~state information security officer and ~~AISO~~agency information security officer have the responsibility to ensure the overall security program meets state and federal ~~statutes as they apply to the State of Nebraska and its Agency operations and resources~~legal requirements.

The ~~SISO~~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~~ technology ~~Acquisition~~ acquisition ~~Process~~process, ~~Hardware~~ hardware and ~~Software~~ software ~~Change~~ change ~~Management~~ management ~~Process~~process, and the ~~Contract~~ contract ~~Management~~ management ~~Process~~ process when changes involve access to or potential exposure of ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED 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~~state information security officer. ~~The failure to comply with this or any other security policy that may or may not result in the compromise of State information confidentiality, integrity, and/or availability may result in action as permitted by law, rule, regulation or negotiated agreement. Each agency will take appropriate steps necessary, including legal and administrative measures, to protect its assets and monitor compliance with this policy.~~

An agency review to ensure compliance with this policy and applicable NIST 800-53 security guidelines must be conducted at least annually. ~~and each Agency management will certify and report the agency's level of compliance with this policy~~

The ~~SISO~~state information security officer may periodically review ~~Agency~~agency compliance with this policy and the related NIST control framework. Such reviews may include:

- Reviews of the technical and business analyses required to be developed pursuant to this policy.
- 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 ~~shall~~ must be documented in an ~~Agency~~agency ~~Security~~ security ~~Corrective~~ corrective ~~Action~~ action ~~Plan~~ plan that shall be made available to the ~~State Information Security Officer~~state information security officer as necessary. ~~The~~ This ~~Security Corrective Action~~ plan is classified as a ~~Restricted~~RESTRICTED 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~~agency and ~~OCIO~~Office of the CIO management to ensure acceptable progress is being made on mitigating or remediating security gaps.

~~8-701~~8-702. Awareness and Training

The ~~State of Nebraska~~state provides information technology resources to authorized ~~Users~~ 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~~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.

New Hire and Refresher Training

~~Every member of the Staff is required to attend~~All new hires must complete security training, including information about this policy, as part of their ~~new-hire~~ orientation. On an annual basis, ~~every member of the Workforce is required to~~all staff must complete a security and privacy training session. The ~~State~~state will maintain records of all attendance for new hire and refresher training.

Periodic Briefings

Management ~~shall~~ should periodically incorporate ~~Information~~information ~~Security~~ security topics into their meetings with ~~Workforce~~staff. ~~The SISO and/or agency AISO shall be available to conduct periodic briefings on various security topics as requested.~~ Additionally, the ~~SISO~~state information security officer ~~shall~~ 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.

~~Annual Employee Acknowledgement~~

~~New members of the Workforce will sign an acknowledgement of understanding of the Policy and their obligations to comply with the Policy no later than one (1) week after their hire date. Members of the Workforce are required to sign an understanding of the Policy and agreement to comply with the Policy annually.~~

~~8-702~~8-703. Security Reviews and Risk Management

This ~~Policy~~ policy is based on the NIST 800-53 Security Controls framework. ~~As such~~Pursuant to that framework, the ~~State~~state ~~is required to~~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 ~~SISO~~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 800-53 Security Controls, such that over a three-year timeframe all control areas will have been assessed.

This review ~~shall~~ must be conducted for each major system used within the ~~State~~state, and ~~shall~~ must include all infrastructure and peripheral processes that are used to support ~~State~~state business processes.

Unscheduled Risk Assessments

Unscheduled risk assessments ~~will~~ may be performed at the discretion of the ~~SISO~~state information security officer or ~~AISO~~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~~ security ~~Officer~~ officer shall document the business area, reason for the review, scope of inspection, and dates of the review in the ~~Corrective~~ corrective ~~Action~~ action ~~Planning~~ planning documentation. All findings and results will also be documented in the ~~Security~~ security ~~Corrective~~ corrective ~~Action~~ action ~~Plan~~plan.

~~8-703~~8-704. Logging and Review of Auditable Events

All systems that handle ~~Confidential~~CONFIDENTIAL or ~~Restricted~~ RESTRICTED information, allow interconnectivity with ~~or from~~ other systems, or make access control (authentication and authorization) decisions, ~~shall~~ must record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including on what system the activity was performed~~.~~?
- What the activity was performed on (object)?
- When was the activity performed?
- What tool(s) was the activity performed with?
- What was the status (such as success vs. failure), outcome, or result of the activity?

Log Format, *S*torage, and Retention

The ~~State of Nebraska~~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. ~~OCIO~~Office of the CIO and the ~~Agency~~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 ~~shall~~ must be regularly monitored and reported, and action will be taken to keep an approved level of ~~freespace~~free space available for use.

Automated notification of ~~Agency~~agency or ~~OCIO~~Office of the CIO personnel ~~shall~~ must occur if the capacity of log files reaches defined threshold levels, or the audit logging system fails for any reason.

The ~~Audit~~ audit ~~Logging~~ logging process is required to provide system alerts to appropriate ~~Agency~~agency or ~~OCIO~~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~~, etc.~~). ~~It is required that a~~All system logs ~~shall~~ 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 ~~shall~~ be retained ~~or recoverable~~ for seven years.

Auditable Events

~~The State System and Network infrastructure are defined as "the LAN, WAN, Servers, firewalls, and Routers/Switches use to provide electronic communication and data /information processing, whether supported by the Agency directly or the OCIO".~~

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 ~~System and Network Infrastructure~~ events should be logged and reviewed on a weekly basis:

- Log on and off the system;
- Change of password;
- All system administrator commands, while logged on as system administrator;
- Switching accounts or running privileged actions from another account~~,~~ (e.g., Linux/Unix SU or Windows RUNAS);
- Creation or modification of super-user groups;
- Subset of security administrator commands, while logged on in the security administrator role;
- Subset of system administrator commands, while logged on in the user role;
- Clearing of the audit log file;
- Startup and shutdown of audit functions;
- Use of identification and authentication mechanisms (e.g., user ID and password);
- Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);
- Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system;
- Changes made to an application or database by a batch file;
- Application-critical record changes;
- Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);
- All system and data interactions concerning FTI;

- Additional platform-specific events, as defined by ~~Agency~~agency needs or requirements;
- Detection of suspicious~~/~~ or malicious activity such as from an ~~Intrusion~~ intrusion ~~Detection~~ detection or ~~Prevention~~ prevention ~~System~~ system (IDS/IPS), anti-virus system, or anti-spyware system; and
- Physical entrance or access to secured and restricted areas or facilities where system and network infrastructure reside.

Audit Log Contents

Audit logs ~~shall~~ must contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The logs ~~shall~~ must identify or contain at least the following elements, or enough information in which to infer the following elements with reasonable assurance~~.~~:

- Type of action~~;~~ (~~Examples include~~e.g., authorize, create, read, update, delete, and accept network connection~~.~~);
- Subsystem performing the action~~;~~ (~~Examples includes~~e.g., ~~-~~process or transaction name, process or transaction identifier~~.~~);
- Identifiers (as many as available) for the subject requesting the action~~;~~ (~~Examples include~~e.g., user name, computer name, IP address, and MAC address). Note that such identifiers should be standardized to facilitate log correlation~~.~~;
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time;
- Whether the action was allowed or denied by access-control mechanisms;
- Description ~~and/~~or reason-codes of why the action was denied by the access-control mechanism, if applicable; and
- Depending on the nature of the event that is logged, there may be other information necessary to collect.

Audit Review, Monitoring, Findings and Remediation

Security safeguard regulations require regular inspections of system audit logs for indications of inappropriate or unusual activity. Additionally, these logs ~~shall~~ must be reviewed by authorized personnel to facilitate investigations of suspicious activity or suspected violations. All reports of findings ~~shall~~ must be reported to appropriate officials who will prescribe the appropriate and necessary actions.

- Logs of suspicious activity ~~shall~~ must be reviewed as soon as possible.
- Logs of system capacity and log integrity ~~shall~~ must be reviewed on a weekly basis.

- Logs of privilege access account creation or modification ~~shall~~ must be reviewed on a weekly basis.
- All other logs ~~shall~~ must be reviewed at least monthly ~~at a minimum~~.

When possible, the ~~Agency~~agency or ~~OCIO~~Office of the CIO will employ automated mechanisms to alert the ~~OCIO~~Office of the CIO, ~~SISO~~state information security officer, or ~~AISO~~agency information security officer when inappropriate or unusual activities with security implications are discovered. Any automation used for log analysis ~~will~~ 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.

All relevant findings discovered because of an audit log review ~~shall~~ must be listed in the appropriate problem tracking system or the ~~Corrective~~ corrective ~~Action~~ action ~~Planning~~ planning ~~(CAP)~~ 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 ~~Department~~agency management within one week of ~~project/task~~ completion. This report ~~will~~ should be considered ~~Confidential~~CONFIDENTIAL ~~Information~~information.

Application Logging Review and Monitoring

~~The State requires that application development or acquisition activity include applicable application~~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 might also be used to record other types of events too.~~ 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 ~~will~~ must be reviewed at least monthly. Corrective actions to address application deficiencies ~~will~~ must be managed through the application development process or the applicable ~~Security CAP~~corrective action planning process.

~~8-704~~8-705. Security Requirements for ~~Third Parties and Vendors~~External Service Providers

All ~~third-party organizations who have~~external service providers with access to ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information ~~are required to~~ must have ~~documented agreements and/or Memorandums of Understanding that describes~~ a written agreement with the state that includes the minimum security requirements necessary for the protection of this information. ~~they must follow to appropriately protect this information. This includes vendors who have access to equipment or infrastructure that stores, accesses, or processes Confidential or Restricted Information. All technology contracts with vendors or third parties who have access to non-public information are required to include information security requirements. The required language must describe the Confidentiality, Integrity, Availability, and Privacy controls required for the third party to follow.~~

~~Any discrepancies or inability to follow these requirements must be documented and approved by the Office of the CIO and the State Information Security Officer so that mitigating or alternative plans may be considered.~~ The ~~State Information Security Officer~~state information security officer ~~will have the authority to~~ may inspect these ~~third-party~~external service provider arrangements to ensure compliance ~~to~~ with ~~State~~state ~~Policies~~ policies and requirements.

~~For information to be released outside an agency or shared between agencies, a process must be established that, at a minimum:~~

- ~~evaluates and documents the sensitivity of the information to be released or shared;~~
- ~~identifies the responsibilities of each party for protecting the information;~~
- ~~defines the minimum controls required to transmit and use the information;~~
- ~~records the measures that each party has in place to protect the information;~~
- ~~defines a method for compliance measurement;~~
- ~~provides a signoff procedure for each party to accept responsibilities;~~
- ~~establishes a schedule and procedure for reviewing the controls (Refer to Section 4.6. Data Classification).~~

~~Non-public State information must not be made available through a public network without appropriate safeguards approved by the data owner(s). The agency must implement safeguards to ensure access control, and data protection measures are adequately protecting State information and logs are collected and protected against unauthorized access. Non-public information includes, but is not limited to:~~

- ~~critical infrastructure assets which are so vital that their infiltration, incapacitation, destruction or misuse could have a debilitating impact on health, welfare or economic security of the citizens and businesses of the State of Nebraska~~

- ~~data that identifies specific structural, operational, or technical information, such as: mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities;~~
- ~~personally identifiable information (PII) as defined under Neb. Rev. Stat. § 87-802;~~
- ~~protected health information (PHI) as defined at 45 CFR § 160.103;~~
- ~~federal tax information (FTI) as defined at 26 U.S. Code § 6103~~

ARTICLE 8

VULNERABILITY AND INCIDENT MANAGEMENT

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~~ disaster ~~Recovery~~ 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 of Nebraska~~state's ability to adequately detect, respond and recover from security incidents.

~~The State of Nebraska and all Agencies~~All agencies that process, store, or access ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information are required to maintain an ~~Incident~~ incident ~~Response~~ response ~~Plan~~ plan~~per this policy~~. This plan ~~shall~~ must include operational and technical components, which provide the necessary functions to support all the fundamental steps within the ~~Incident~~ incident ~~Management~~ management ~~Life~~ life ~~Cycle~~ cycle, ~~-~~ including the following:

1. Preparation;
2. Incident Triage and Identification;
3. Containment;
4. Incident Communication;
5. Preservation of Evidence;
6. Root Cause Analysis; and
7. Recovery and Permanent Remediation.

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~~ state's ~~Senior~~ senior ~~Management~~ management and ~~Agency~~ agency officials responsible for reporting to federal offices~~,~~.

These procedures also describe the way ~~OCIO~~ Office of the CIO or ~~Agency~~ 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.

A. Preparation - Scope and Responsibilities

A security incident is any adverse event whereby some aspect of the ~~State~~state ~~infrastructure~~ infrastructure is threatened (e.g., personal violation, loss of data confidentiality, disruption of data integrity, denial of service, security breach~~, etc.~~). 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 e-mail containing ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information (e.g. Federal Tax Information, Personally Identifiable Information~~, etc.~~) sent outside the secured ~~State of Nebraska~~state network is a security incident and should be reported as such.

All security incidents must be reported to the ~~State Information Security Officer~~state information security officer, ~~Department~~agency ~~Management~~management, ~~or~~ and the ~~OCIO~~ Office of the CIO ~~Help~~ Service Desk ~~IMMEDIATELY~~immediately. Security incidents will be tracked by the ~~SISO~~state information security officer. Any ~~State~~ state ~~employee or contractor~~staff who observe, experience, or are notified of a security incident, should immediately report the situation to the ~~AISO~~agency information security officer, ~~SISO~~ state information security officer or the ~~OCIO~~ Office of the CIO ~~Help~~ Service Desk, but at the very least to their supervisor. All ~~State of Nebraska~~state management are responsible to ensure that their ~~employees and contractors~~staff understand that awareness of the incident are to be reported immediately~~ to the SISO, Department Management, or the OCIO Help Desk~~.

~~State and Agency Legal and/or Privacy Office~~

~~These departments are required to work with the Information Technology teams and the SISO/AISO during triage to assess reportable conditions. They are responsible for crafting any communications for customers, government officials and the public in the event of a reportable breach. They are also responsible for ensuring all third-party agreements have requirements to comply with the State's Incident Management requirements.~~

State Information Security Officer and Agency Information Security Officer

The ~~Security~~ security ~~Officers~~ officers are responsible for assembling, engaging, and overseeing the ~~applicable Incident~~ incident ~~Response~~ response ~~Team~~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~~ information ~~Technology~~ technology personnel to perform analysis and triage of incident impact and reportable conditions.

The ~~Security~~ security ~~Officers~~ officers will finalize and sign off on any ~~Security~~ security ~~Incident~~ incident ~~Reports~~reports, and determine follow-up activity, root cause analysis, long term mitigation, and updates to the security awareness training.

~~They~~ Agency information security officers are also responsible for ensuring that all technical areas within the ~~State~~agency have an understanding and ability to meet this standard. They are required to perform education and training of this standard to all applicable ~~Department~~agency personnel, and then test the ~~Incident~~ incident ~~Response~~ response ~~Process~~ process annually.

Incident Response Team

The ~~State~~state information security officer ~~shall~~ will identify key personnel who will serve as members of the state ~~Incident~~ incident ~~Response~~ response ~~Team~~team. ~~Agencies may also identify additional Incident Response teams for their specific environment.~~ 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~~state information systems, networks and data by identifying and controlling the incident, properly preserving evidence, and reporting to appropriate entities. This team ~~can~~ 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

~~SISO~~state information security officer or ~~AISO~~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~~ incident ~~Response~~ response team include:

- The ~~State of Nebraska direction~~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.
- Conduct the initial triage. Perform a damage and impact assessment and document the findings.
- Report to ~~State~~state of ~~Agency~~agency management on a regular schedule with status and action plans.
- Maintain confidentiality of the circumstances around the incident.
- Follow procedures to maintain a chain of trust and to preserve evidence.
- Initiate the ~~Root~~ root ~~Cause~~ cause analysis~~,~~; bring in other resources as necessary.
- Initiate return to normal operations~~,~~; bring in other resources as necessary.

B. Incident Management Procedures

Incident ~~Management~~ 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~~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 ~~shall~~ should be carefully managed and controlled by the ~~OCIO~~ Office of the CIO and ~~Agency~~agency ~~Senior~~ senior ~~Management~~management. ~~Only previously identified officials are authorized to communicate to other State of Nebraska officials, the public/press, or any other government agency.~~ All personnel involved any incident management support activity will communicate only with the parties necessary for incident analysis or recovery activity, and to the ~~SISO~~state information security officer, ~~OCIO~~Office of the CIO, or the ~~Agency~~ agency ~~Information~~ information ~~Technology~~ technology team. No other communication, unless explicitly authorized, is allowed.

A ~~Security~~ security ~~Incident~~ incident ~~Report~~ report ~~information~~ is classified as ~~Restricted~~ RESTRICTED ~~Information~~information. ~~Sharing or distribution of the information will be limited to only those individuals with a valid need-to-know. The OCIO or Agency management, with consultation from the SISO/AISO, will review all requests for the release of security incident information and make determinations regarding its release, ensuring that it is consistent with applicable policies, regulations, and external customer requirements. Overall questions regarding this procedure should be directed to the SISO and AISO.~~

C. Incident Management Training and Testing

~~The State and/or Agency shall provide annual training on incident recognition and reporting requirements to all staff and contractors. More in depth training and awareness will be given to all applicable staff in incident response and recovery procedures and reporting methods.~~ Annually, the ~~SISO~~state information security officer and ~~AISO~~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~~state or ~~Agency~~agency ~~Security~~ security ~~Incident~~ incident ~~Response~~ response team. This test ~~shall~~ will simulate a variety of security related incidents.

D. 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 ~~shall~~ will be conducted by the ~~SISO~~state information security officer/~~AISO~~agency information security officer, ~~OCIO~~Office of the CIO ~~Help~~ Service Desk, or the ~~Information~~ information ~~Technology~~ technology team to understand the scope and impact of the incident and initiate appropriate action. Once an incident has been identified and reported, the ~~SISO~~state information security officer/~~AISO~~agency information security officer ~~(or designate)~~ 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 ~~SISO~~state information security officer/~~AISO~~agency information security officer and IT ~~Management~~ management ~~reserve the right to~~may quarantine any potentially threatening system and terminate any threatening activity ~~using all means necessary~~. The ~~SISO~~state information security officer will ensure that a ~~Security~~ security ~~Incident~~ incident ~~Report~~ report is completed for all incidents.

For more complicated incidents that may require further analysis, the ~~Incident~~ incident ~~Response~~ response team will be assembled via direction from the ~~SISO~~state information security officer, ~~OCIO~~Office of the CIO, ~~AISO~~agency information security officer, or ~~Agency~~agency IT ~~Management~~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 ~~SISO~~state information security officer ~~and/~~or the ~~Incident~~ incident ~~Response~~ response ~~Team~~team. They will determine if the incident impacts organizations outside of the ~~Department~~agency's internal network. They will also determine if any reportable conditions, such as unauthorized disclosure of ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information exists. If the incident appears to have ~~ANY~~ any citizen information compromised, immediate notification to the ~~Senior~~ agency ~~Management~~management, ~~SISO~~state information security officer, and ~~AISO~~agency information security officer~~, or OCIO~~ is ~~REQUIRED~~required. ~~This person will then notify other appropriate senior State officials ore relevant parties and will determine the communication plan for any government agencies or the public and press.~~ ~~Senior~~ Agency ~~Management~~ management ~~or designates~~ will oversee and coordinate all communication actions.

All forms of unauthorized disclosure of ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED information, including the potential for unauthorized disclosure (such as information spillage), ~~shall~~ will be considered ~~Incidents~~incidents. Information spillage refers to instances where either ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED 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~~ incident has occurred and corrective action is required.

~~All compromised systems will be disconnected from external communications immediately upon discovery. Senior Management will be notified of analysis results and citizen impact immediately upon discovery, and shall be kept abreast of all analysis findings, impact assessments, and remediation progress.~~

E. Incident Containment ~~and Recovery~~

Any IT resources that are engaged in active attacks against other IT resources must be isolated and taken off the ~~State~~state network immediately. Incidents involving the exposure, or potential exposure, ~~(or POTENTIAL exposure)~~ of ~~Confidential~~CONFIDENTIAL or ~~Restricted~~RESTRICTED 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 ~~SISO~~state information security officer has the authority to coordinate with the ~~OCIO~~Office of the CIO to block compromised services and hosts that present a threat to the rest of the ~~State~~state network. Notifications of outages or service interruptions will follow normal ~~OCIO~~Office of the CIO or ~~Agency~~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.

~~Once the incident has been verified and contained, the OCIO or the Agency IT Department can begin carefully bringing resources back on line and operational.~~

F. Incident Communication

Reportable conditions, such as the breach of PHI, PII or FTI, require notification within specific timeframes ~~(~~as defined in state and federal ~~regulations~~law~~)~~. It is the responsibility of the ~~SISO~~state information security officer and ~~AISO~~agency information security officers to understand these requirements and ensure the ~~State~~state and~~/or~~ ~~Agency~~agency remain~~s~~ 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 ~~SISO~~state information security officer, ~~AISO~~agency information security officer, ~~OCIO~~Office of the CIO, and ~~Agency~~agency management to ensure that all communication regarding any security incident is managed and controlled.

G. 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~~ incident ~~Response~~ response team ~~shall~~ will work with law enforcement to secure the potential evidence without reviewing additional content. Network hardware, software or data may be considered potential evidence.

~~A subpoena, warrant or other official request must be issued before any data is released to law enforcement. Only senior State and Agency Officials are authorized to release any evidence to law enforcement. Evidence from incidents that involve an immediate threat to persons or property~~

~~may be provided to law enforcement in advance of a public records request, subpoena or warrant, but may only be provided by authorized parties.~~

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 ~~Department IT Security Officer~~agency information security officer immediately after initial steps, but ~~NO LATER~~no later than one hour after becoming aware of the possible incident.

d. Make a bit copy of the drive before investigating (~~i.e.~~e.g., opening files, deleting, rebooting).

e. Dump memory contents to a file.

f. Label all evidence.

g. Log all steps.

H. 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~~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 ~~Restricted~~RESTRICTED ~~Information~~information~~, and copies will only be distributed under direction of State or Agency management~~.

A formal ~~Root~~ root ~~Cause~~ cause ~~Analysis~~ analysis ~~shall~~ must be performed within two weeks of the occurrence of the ~~Security Incident~~incident. This analysis ~~shall~~ 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.

I. Incident Recovery and Permanent Remediation

The ~~Incident~~ incident ~~Response~~ 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 ~~shall~~ will be limited to authorized personnel until the security incident has been contained and root cause mitigated. Analysis and mitigation procedures ~~shall~~ must be completed as soon as possible, recognizing ~~State~~state systems are vulnerable to other occurrences of the same type.

The ~~OCIO~~Office of the CIO, ~~SISO~~state information security officer, and ~~AISO~~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 ~~shall include~~:

- Reinstalling compromised systems from trusted backup-ups, if required;

- Reinstalling system user files, startup routines, or settings from trusted versions or sources, if required;
- Validating ~~Restored~~ restored ~~Systems~~ systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons; and
- Increasing ~~Security~~ security monitoring and heighten awareness for a recurrence of the incident.

8-802. 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~~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~~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~~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~~state information security officer and who have requested and received written consent from the Office of the ~~Chief Information Officer~~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 ~~always~~ to minimize the possibility of disruption. Any other attempts to perform tests or scans will be deemed an unauthorized access attempt.

8-803. 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 ~~Chief Information Officer~~CIO before being installed on the ~~State~~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~~state and as referenced in the National Vulnerability ~~database~~ 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~~state information security officer. Any vulnerability detected will be evaluated for risk by the ~~OCIO~~Office of the CIO or ~~Agency~~agency and a mitigation plan will be created as

required and forwarded to the ~~State Information Security Officer~~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~~ and the scanning must meet State of Nebraska policy~~.

8-804. 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~~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~~ change ~~Management~~ management ~~Process~~process, but all software must have security patches applied as soon as possible.

8-805. Security Deficiencies

All security deficiencies reported or identified in any security review, scan, assessment, or analysis ~~shall~~ must be documented in the ~~State~~state or ~~Agency~~agency Security POAM~~ per policy 8-100~~. These gaps ~~shall~~ must be managed to mitigation, remediation, or approved risk acceptance.

ARTICLE 9

DATA SECURITY

~~8-903. Data Classification~~8-901. State Data

Data is a critical asset of the ~~State of Nebraska~~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~~State of Nebraska~~, irrespective of the medium on which the data resides and regardless of format ~~(such as in electronic, paper or other physical form)~~.

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 ~~S~~state data in compliance with this policy, federal requirements, and ~~the agency Records Retention~~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~~, where it can go, etc~~.

8-902. Data Classification Categories

Data owned, used, created or maintained by the ~~S~~state is classified into the following four categories:

(1) ~~Restricted~~**RESTRICTED.** This classification level is for sensitive information intended for use by a limited number of authorized staff with an explicit "need to know" and controlled by special rules to specific personnel. Examples of this privileged access information include: attorney~~/~~-client privilege information, ~~A~~agency strategies or reports that have not been approved for release, audit records, network diagrams with IP addresses specified, and privileged administrator credentials~~, etc.,~~. This level requires internal security protections and could have a high impact in the event of an unauthorized data disclosure.

(2) ~~Confidential~~**CONFIDENTIAL.** This classification level is for sensitive information intended for use within an ~~A~~agency and controlled by special rules to specific personnel. Examples of this type of data include: ~~F~~federal ~~T~~tax ~~I~~information (FTI), ~~P~~protected ~~H~~health ~~I~~information (PHI) and other Patient Medical Records covered by Health Insurance Portability and Accountability Act (HIPAA), ~~P~~payment ~~C~~card ~~I~~industry (PCI) information, and ~~P~~personally ~~I~~identifiable ~~I~~information (PII) ~~and any other information regulated by State or Federal regulations.~~.

(3) ~~Managed Access Public~~**MANAGED ACCESS PUBLIC**. This classification level is for information that is public in nature but may require authorization to receive it. This type of information requires a minimal level of security and would not have a significant impact in the event of data disclosure. This type of information does not include personal information but may carry special regulations related to its use or dissemination. ~~Managed Access Public~~This data may also be data that is sold ~~as a product or service requiring users to subscribe to this service~~.

(4) ~~Public~~**PUBLIC**. This classification is for information that requires no security and can be handled in the public domain.

~~8-901. State of Nebraska Information 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 OCIO are required to have a security program that meets this information security policy. The AISO shall develop a System Security Plan that must be approved by the SISO. 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 SISO, an approved and signed Interconnection System Agreement (ISA) that describes the security controls and plans will be in place to protect State information.~~

~~8-902~~8-903. Data Inventory

Each ~~Agency~~ agency shall identify and classify all information according to this policy. ~~To aid in this assessment, agencies are required to~~Each agency shall maintain an inventory of where ~~Confidential~~CONFIDENTIAL and ~~Restricted~~RESTRICTED information reside, so those environments can be assessed for security adequacy.

8-904. Data Security Control Assessment

~~Agencies are required to~~ Each agency shall perform a ~~Security~~ security ~~Control~~ control ~~Assessment~~ assessment ~~(SCA)~~ that assesses the adequacy of security controls ~~commensurate with its Data Classification as well as the Agency's level of~~for compliance with this policy ~~and/or~~and any applicable security frameworks (~~such as~~e.g., NIST, PCI, CMS, and IRS~~, etc.)~~). The assessment ~~can~~ may be performed internally by the ~~AISO~~ agency information security officer or with the assistance of the state information security officer~~SISO.~~~~, but each Agency~~ Each agency is required to have an assessment at least once every ~~three years~~year, covering at least ~~1/3~~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.

~~To aid in this assessment, agencies are required to maintain an inventory of where Confidential and Restricted information reside, so those environments can be assessed for security adequacy.~~

~~8-901~~8-905. ~~State of Nebraska Information~~Data Sharing

It is critical that ~~A~~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 ~~A~~agencies that share connectivity and information between the ~~A~~agency and the ~~OCIO~~Office of the CIO are required to have a security program that meets this ~~information security~~ policy. The ~~AISO~~agency information security officer shall develop a ~~S~~system ~~S~~security ~~P~~plan that must be approved by the ~~SISO~~state information security officer. All ~~A~~agencies shall perform a security control assessment that identifies the adequacy of security controls and precautions for protecting ~~S~~state information. If the ~~A~~agency performs this assessment independent of the ~~SISO~~state information security officer, an

approved and signed ~~I~~interconnection ~~S~~system ~~A~~agreement ~~(ISA)~~ that describes the security controls and plans will be in place to protect ~~S~~state information.

~~8-903. Data Classification~~

~~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 of Nebraska, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).~~

~~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 the agency 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, stored, who has access, where it can go, etc.~~

~~Data owned, used, created or maintained by the State is classified into the following four categories:~~

- ~~**Restricted.** This classification level is for sensitive information intended for use by a limited number of authorized staff with an explicit "need to know" and controlled by special rules to specific personnel. Examples of this privileged access information include attorney/client privilege information, Agency strategies or reports that have not been approved for release, audit records, network diagrams with IP addresses specified, privileged administrator credentials, etc., This level requires internal security protections and could have a high impact in the event of an unauthorized data disclosure.~~
- ~~**Confidential.** This classification level is for sensitive information intended for use within an Agency and controlled by special rules to specific personnel. Examples of this type of data include Federal Tax Information (FTI), Protected Health Information (PHI) and other Patient Medical Records covered by Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) information, Personally Identifiable Information (PII) and any other information regulated by State or Federal regulations..~~
- ~~**Managed Access Public.** This classification level is for information that is public in nature but may require authorization to receive it. This type of information requires a minimal level of security and would not have a significant impact in the event of data disclosure. This type of information does not include personal information but may carry special regulations related to its use or dissemination. Managed Access Public data may also be data that is sold as a product or service requiring users to subscribe to this service.~~
- ~~**Public.** This classification is for information that requires no security and can be handled in the public domain.~~

~~8-904~~8-906. ~~Information Retention and~~Data Destruction

~~All information, created, acquired or used in support of State of Nebraska's business activities, must be used for official business only. Agency information is an asset and must be protected from its creation through its useful life, and to its authorized disposal in accordance with the Records Management Act and your agency's retention schedule. State information must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use.~~

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 of Nebraska~~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 ~~confidential~~ CONFIDENTIAL or ~~restricted~~ RESTICTED information must be physically destroyed or securely overwritten when the data contained on the device is ~~no longer required under the provisions of the Records Management Act~~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~~, etc.~~) when any significant change occurs.

Sec.2. In section 5-204(2.2.6), strike the sentence beginning with “Section”.

Sec.3. Strike section 5-204(4) in its entirety.

Sec.4. In Attachment A to section 5-204, strike the sentence beginning with “See NITC 8-101”; strike the bulleted sentence beginning with “Approved remote access”; and strike the subsection titled: “Identified NITC policies that apply to use, access and protecting information:” in its entirety.

Sec.5. In Attachment B to section 5-204, strike the sentence beginning with “See NITC 8-101”; strike the bulleted sentence beginning with “Approved remote access”; and strike the subsection titled: “Identified NITC policies that apply to use, access and protecting information:” in its entirety.

Sec.6. Staff shall reformat and re-enumerate the provisions of this proposal for consistency prior to final publication.

Sec.7. Original sections 5-204, 8-101, 8-102, 8-103, 8-201, 8-301, 8-302, 8-303, 8-304, and 8-401 are repealed. Resource documents 8-RD-01, 8-RD-02, 8-RD-03, 8-RD-04, 8-RD-05, and 8-RD-06 are repealed.

Sec.8. This proposal becomes operative on ~~xxx xx, xxxx~~December 1, 2017.