MEETING AGENDA

Technical Panel
of the
Nebraska Information Technology Commission

Tuesday, January 8, 2008
9:00 a.m. - 10:30 a.m.
Nebraska State Office Building - Lower Level C
301 Centennial Mall South
Lincoln, Nebraska

AGENDA

Meeting Documents: Click the links in the agenda
or click here for all documents. (xx Pages)

1. Roll Call, Meeting Notice & Open Meetings Act Information

2. Public Comment

3. Approval of Minutes* - November 21, 2007

4. Project Reviews

   - Ongoing Reviews (as needed)
     - Retirement Systems - Jerry Brown
     - Health and Human Services (MMIS and LIMS) - James Ohmberger
     - Nebraska State College System (Student Information Administrative System)
     - University of Nebraska (Student Information System)

5. Standards and Guidelines

   - Request for Waiver*
     - Game and Parks - Request for Waiver from Password Standard and Identity and Access Management Standard for State Government Agencies
   - Set for 30-Day Comment Period*
     - NITC 01-101: Definitions
     - NITC 01-103: Waiver Policy
     - NITC 01-204: IT Procurement Review Policy
     - NITC 08-401: Incident Response and Reporting Standard | Reporting Form

6. Regular Informational Items and Work Group Updates (as needed)

   - Accessibility of Information Technology Work Group - Horn
   - Learning Management System Standards Work Group - Langer
   - Security Architecture Work Group - Hartman

7. Other Business

8. Next Meeting Date - February 12, 2008

9. Adjourn

* Denotes Action Item

(The Technical Panel will attempt to adhere to the sequence of the published agenda, but reserves the right to adjust the order of items if necessary and may elect to take action on any of the items listed.)

NITC and Technical Panel Websites: http://nitc.ne.gov/
Meeting notice was posted to the NITC Website and Nebraska Public Meeting Calendar on November 29, 2007.
The agenda was posted to the NITC Website on 21 DEC 2007.

TECHNICAL PANEL MINUTES

TECHNICAL PANEL
Nebraska Information Technology Commission
Wednesday, November 21, 2007, 9:00 a.m.
Varner Hall - Board Room
3835 Holdrege St., Lincoln, Nebraska

PROPOSED MINUTES

MEMBERS PRESENT:
Brenda Decker, CIO, State of Nebraska
Kirk Langer, Technology Director, Lincoln Public Schools
Walter Weir, CIO, University of Nebraska
Mike Winkle, Assistant GM, Nebraska Educational Telecommunications

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

Mr. Weir called the meeting to order at 9:04 a.m. Roll call was taken. There was a quorum present. The meeting notice was posted to the NITC Website and the Nebraska Public Meeting Calendar on October 4, 2007 (rescheduled on November 8). The meeting agenda posted to the NITC Website on November 19, 2007. A copy of the Nebraska Open Meeting Act was available in the room.

PUBLIC COMMENT

There was no public comment.

APPROVAL OF SEPTEMBER MINUTES

Under the section titled "University of Nebraska (Student Information System)," in the sixth sentence the word consulting was misspelled.

Mr. Winkle moved to approve the September 11, 2007 minutes as corrected. Ms. Decker seconded. Roll call vote: Decker-Yes, Langer-Yes, Weir-Yes, and Winkle-Yes. Results: Yes-4 and No-0. Motion carried.

PROJECT REVIEWS - Ongoing Reviews (as needed)

Retirement Systems, Jerry Brown. A written report titled "PIONEER Transition Project, November 21, 2007" was distributed to members. Highlights of the report include:

- Robin Goracke, new Project Director, was present and was introduced.
- The equipment for development and user acceptance testing has been installed and configured for use.
- Office space in the Atrium is being occupied by the project team.
- The QA Charter has been signed by the University.
- The project is approximately 2 weeks behind schedule, primarily due to preparation time devoted to Columbus Ohio and off-shore staff orientation. It is anticipated to gain back lost time during the Phase II Requirement Validation process.

- Requirements Validation for the financial and employer reporting functions (Phase I) has been completed. User acceptance testing will begin the week of December 5th.
- Phase II planning has begun which includes all remaining online processing that PIONEER performs, plus new requirements, such as Retirement Seminar Tracking. The Phase II Requirements Validation sessions will begin the week of December 19th.
- The project has been working with the OCIO staff to estimate the cost to host the hardware.
- The project was informed last week that 93% of Saber was sold to EDS. Saber did not anticipate any changes that would impact our project.

Health and Human Services (MMIS and LIMS). HHS will have a report at the next meeting.

PROJECT REVIEWS - GOVERNMENT TECHNOLOGY COLLABORATION FUND GRANT APPLICATION - SECURITY ARCHITECTURE WORK GROUP – VULNERABILITY THREAT MANAGEMENT

Steve Hartman, Security Officer, Office of the CIO

The State Government Council recommended approval of the project at their meeting yesterday.

The Security Architecture Work Group is requesting a $75,000 grant from the Government Technology Collaboration Fund to purchase a vulnerability assessment tool for the state. In the past, these grant funds have been used to hire outside entities to perform similar vulnerability testing, which was limited to a specific point in time. The work group wants to purchase a tool which will allow for ongoing and as needed testing. The Office of the CIO has released an RFP for this purpose. Bid openings will occur in December. The Intent to Award is scheduled for January 31 with implementation to begin by February. The RFP states that project is contingent upon funding from the Government Technology Collaboration Fund.

Logical partitions can be created so that agency can see their own scans and run adhoc reports. The Office of the CIO will be taking the lead role working with agencies.

Mr. Langer moved to recommend approval of the grant application for the Vulnerability Threat Management project. Mr. Winkle seconded. Roll call vote: Decker-Abstain, Langer-Yes, Weir-Yes, and Winkle-Yes. Results: Yes-3, No-0, Abstained-1. Motion carried.

PROJECT REVIEWS - PROJECT PROPOSALS FOR FY2008 DEFICIT BUDGET REQUESTS, RECOMMENDATION TO THE NITC*

Nebraska State College System - Student Information Administrative System (Summary Sheet)
University of Nebraska - Student Information System (Summary Sheet)

The Education Council voted to recommend that the projects be designated as a Tier 1 Priority (mission critical for the agency) because of discontinuation of support of the existing student information systems. The Education Council also

added remarks:

- To the extent possible, both the State College System and the University of Nebraska must synchronize their RFP processes and co-evaluate vendors.
- To require an analysis of cost-savings and an analysis of 'effect on students' for two pathways:
  - Centralization and cooperative hosting of Projects 50-01 and 51-01
  - Adoption of a single vendor for Projects 50-01 and 51-01
- To require a unified look at adopting the same vendor by both the State College System and the University of Nebraska; and if not the same result, to provide a justification for divergence.

Mr. Weir indicated that he and Mr. Hoffman are meeting on Monday to continue discussions of partnering and collaboration. They are not convinced collaboration can occur at all phases especially with implementation due to the differences between the University of Nebraska and the State College System. Both institutions are in different stages of the process. The University of Nebraska has hired a consultant to assess their needs and requirements. It is anticipated that to release an RFP in January. The State College System has already released an RFP and in the process of evaluating vendors.

After discussion, the Technical Panel agreed to take action and make recommendations on both projects simultaneously:

Are the projects technically feasible?

Ms. Decker moved that the following comment be included in both projects: "Yes, the Student Information System is technically feasible and the need articulated in the proposal is valid." Mr. Winkle seconded. Roll call vote: Roll call vote: Decker-Yes, Langer-Yes, Weir-Abstain, and Winkle-Yes. Results: Yes-3, No-0, Abstained-1. Motion carried.

Is the proposed technology is appropriate for the project?

Mr. Winkle moved that the following answer be submitted for both projects: "Unknown until the agency completes the RFP process." Ms. Decker seconded. Roll call vote: Winkle-Yes, Decker-Yes, Langer-Yes, and Weir-Abstain. Results: Yes-3, No-0, Abstained-1. Motion carried.

Can the technical elements can be accomplished within the proposed timeframe and budget?

Ms. Decker moved that the following answer be submitted for both projects: "Unknown until the agency completes the RFP process." Mr. Winkle seconded. Roll call vote: Langer-Yes, Weir-Abstain, Winkle-Yes, and Decker-Yes. Results: Yes-3, No-0, Abstained-1. Motion carried.

Ms. Decker moved that the following Additional Comments be submitted for both projects: "The Technical Panel recommends that the State College System and University provide regular updates on these projects to the Panel," and "The Technical Panel recommends that the State College System and University explore the possibility of including the Department of Education in any discussions involving K-20 education in relation to these

projects." Mr. Winkle seconded. Roll call vote: Decker-Yes, Langer-Yes, Weir-Abstain, and Winkle-Yes. Results: Yes-3, No-0, Abstained-1. Motion carried.

STANDARDS AND GUIDELINES

Table of Contents

Mr. Becker provided an update on the changes to the Standards and Guidelines website, including changes listed in the handout. He also discussed the new documents that are being prepared for upcoming meetings.

REGULAR INFORMATIONAL ITEMS AND WORK GROUP UPDATES (AS NEEDED)

Accessibility of Information Technology Work Group, Christy Horn. No report .

Learning Management System Standards Work Group, Kirk Langer. No report.

Security Architecture Work Group, Steve Hartman. The work group will have a revised standard that will be present at the next Technical Panel meeting.

ELECTION - TECHNICAL PANEL CHAIR FOR 2008*

Ms. Decker nominated Walter Weir to serve as Chair of the Technical Panel. Mr. Langer seconded. There were no other nominees. Roll call vote: Winkle-Yes, Decker-Yes, Langer-Yes, and Weir-Abstain. Results: Yes-3, No-0, Abstained-1. Motion carried.

OTHER BUSINESS

Ms. Decker reported that the NITC's Performance Audit hearing was yesterday. Members discussed the audit report.

NEXT MEETING DATE AND ADJOURNMENT

The next meeting of the NTIC Technical Panel is scheduled for Tuesday, January 8, 2008 at 9:00 a.m.

Ms. Decker moved to adjourn. Mr. Winkle seconded. All were in favor. Motion carried.

The meeting was adjourned at 10:35 a.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Rick Becker of the Office of the CIO and NITC.

NITC 01-101 (DRAFT)

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 01-101 (Draft)

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

1. General Provision

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

2. Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Enterprise Project: Enterprise project means an endeavor undertaken over a fixed period of time using information technology, which would have a significant effect on a core business function and affects multiple government programs, agencies, or institutions. Enterprise project includes all aspects of planning, design,

implementation, project management, and training relating to the endeavor. Neb. Rev. Stat. § 86-506.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

made available to the general public from federal, state, or local government records.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

agency workers.

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

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

State: The State of Nebraska.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Web Page: A document stored on a server, consisting of an HTML file and any related files for scripts and graphics, viewable through a web browser on the World Wide Web. Files linked from a Web Page such as Word (.doc), Portable Document Format (.pdf), and Excel (.xls) files are not Web Pages, as they can be viewed

without access to a web browser.

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

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

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

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

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

NITC 01-103 (DRAFT)

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 01-103 (Draft)

Title	Waiver Policy
Category	General Provisions
Applicability	General applicability

1. Purpose

Some agencies may have special circumstances or requirements that justify non-compliance with a standard issued by the NITC. This document authorizes the Technical Panel to issue waivers relating to the requirements contained in any of the NITC Standards and Guidelines documents and establishes the procedures for the submission and review of waiver requests.

2. Policy

Upon a determination of good cause shown, the Technical Panel may grant a waiver from any requirement contained in any NITC Standards and Guidelines document. Section 3 establishes the procedures for the submission and review of waiver requests.

3. Waiver Process

3.1 Submitting a "Request for Waiver"

Any agency may apply for a waiver by submitting a "Request for Waiver."

The "Request for Waiver" should include the following information:

- Agency name
- Name, title, and contact information for the agency contact person regarding the request
- Title of the NITC Standards and Guidelines document at issue
- Description of the problem or issue
- Description of the agency's preferred solution, including a listing of the specific requirement(s) for which a waiver is requested
- Any additional information and justification showing good cause for the requested waiver

Requests should be submitted via email to: rick.becker@nebraska.gov.

3.2 Technical Panel Review and Decision

The Technical Panel will consider the "Request for Waiver" at their next regularly scheduled public meeting. The panel may request additional information from the submitting agency and may table their decision for one meeting. After reviewing the request, and any comments received, the panel may approve the request, approve the request with conditions, or deny the request.

3.3 Appeal to the NITC

A denial or an approval with conditions by the Technical Panel may be appealed to the NITC.

VERSION DATE: Draft - December 19, 2007
HISTORY:
PDF FORMAT: (to be added)

REPEAL CLAUSE
Language regarding exemptions and waivers contained in previously adopted NITC Standards and Guidelines documents is repealed.

NITC 01-204 (DRAFT)

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 01-204 (Draft)

Title	IT Procurement Review Policy
Category	General Provisions
Applicability	Applies to all state agencies, boards, and commissions, excluding the University of Nebraska

1. Policy

By statute, certain state agency purchases of communications equipment and information management items require the approval of the Office of the Chief Information Officer (OCIO). This policy provides guidance to agencies for compliance with these statutory requirements.

1.1 Criteria for Reviews of Information Technology Equipment, Software, and Services

1.1.1 Does the procurement comply with NITC standards and enterprise architecture?
1.1.2 Does the procurement avoid unnecessary duplication of expenditures?
1.1.3 Does the procurement address opportunities for collaboration or data sharing, if applicable?
1.1.4 Does the procurement represent the right technology for the job?
1.1.5 Does the procurement require skills or resources that exceed the capability of the agency to provide or acquire?

1.2 Information for Reviews

1.2.1 Documentation for purchase requisitions and purchase orders in NIS (document types ON and 06)
- Agencies should attach sufficient information in NIS that allows the reviewer to determine what is being purchased, the purpose being served, total cost, and a contact for additional information. This information can be provided as either a text note or an attachment to the header in NIS. In addition, the following types of documents are helpful, if available:
• Bill of materiel from the vendor
• Quotation from the vendor
1.2.2 Documentation for Competitive Solicitations (request for

proposals, requests for information, invitations to bid)
- Agencies should provide a draft copy to the OCIO of the solicitation (RFP, RFI, ITB) at least 30 days prior to its planned release.

1.2.3 Documentation for Sole Source Requests / Requests for Deviation from the Competitive Process
- Agencies should document the reasons for not following the competitive process.

1.3 Approval Timelines

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

1.3.2 Procurement requests that are more complex will be reviewed and acted upon within 3 workdays. The action may be a request for clarification or additional information. The goal is to resolve all issues and provide a final action within 10 workdays, excluding the time an agency requires to respond to requests for additional information.

1.3.3 Reviews of major solicitations (RFPs, RFIs, ITBs) will be reviewed and acted upon within 7 workdays. The action may be a request for clarification or additional information. The goal is to resolve all issues and provide a final action within 12 workdays, excluding the time an agency requires to respond to requests for additional information.

1.4 List of Preapproved Items for Purchase

1.4.1 For the purpose of procurement reviews pursuant to Neb. Rev. Stat. §§ 81-1117, 81-1120.17 and 81-1120.20, the Office of the CIO will maintain a list of preapproved items for purchase by agencies. The list will identify communications equipment and information management items that by their nature are low cost and pose little risk of violating the criteria established in Section 1.1. The list may also designate certain items as not requiring a review because the primary purpose of the items is other than information management. Agencies have prior approval to purchase items on this list.

1.4.2 The list described in this section will appear in Attachment “A” to this document. The Technical Panel may approve revisions to Attachment “A” as requested.

2. Purpose and Objectives

2.1 Statutory Requirements

2.1.1 Communications Equipment

Section 81-1120.17 requires the Division of Communications to “(1) coordinate the purchase, lease, and use of communications services equipment and facilities for state government.” Subsections 4 and 5 require DOC to consolidate and integrate

radio communications systems and services, consolidate telephone and telephone-related activities, to provide for joint use of communications services, and to “approve all purchases and contracts for such communications activities.” Section 81-1120.20 requires state agencies to “coordinate all communications services or facilities procurement through the Director of Communications.”

2.1.2 All Other Information Management Items

Section 81-1117(2)(e) states that “No state agency shall hire, purchase, lease, or rent any information management item listed in subsection (a) of this section without the written approval of the information management services administrator.”

2.2 Objectives

The procurement review process should serve the following objectives established in statute:

2.2.1 “Substantial economies can be effected by joint use of a consolidated communications system by departments, agencies, and subdivisions of state government.” [Section 81-1120.01]

2.2.2 “To coordinate the purchase, lease, and use of communications services equipment and facilities for state government.” [Section 81-1120.17(1)]

2.2.3 “To advise departments and agencies of the state and political subdivisions thereof as to systems or methods to be used to meet requirements efficiently and effectively.” [Section 81-1120.17(2)]

2.2.4 “To prevent unnecessary duplication of information management operations and applications in state government.” [Section 81-1116.02]

2.2.5 “To assure the most cost-effective use of state appropriations” ... and “To coordinate the state’s investments in information technology in an efficient and expeditious manner.” [Section 86-513]

2.2.6 To “adopt minimum technical standards, guidelines, and architectures...” [Section 86-516(6)]

2.2.7 To “coordinate efforts among other noneducation state government technology agencies and coordinating bodies.” [Section 86-520(4)]

2.2.8 To “work with each governmental department and noneducation state agency to evaluate and act upon opportunities to more efficiently and effectively deliver government services through the use of information technology.” [Section 86-520(7)]

2.2.9 To “recommend ... methods for ... making information sharable and reusable, eliminating redundancy of data and programs, improving the quality and usefulness of data, and improving access to data...” [Section 86-520(8)]

2.2.10 To “aggregate demand, reduce costs ... and encourage collaboration between communities of interest” [Section 86-524(1)(c)]

2.2.11 To "encourage competition among technology and service providers." [Section 86-524(1)(c)]
2.2.12 To coordinate the state's investments in information technology in an efficient and expeditious manner ... and avoid "cumbersome regulations or bureaucracy." [Section 86-515]

3. Definitions

3.1 Communications

Section 81-1120.02 includes the following definitions:
"(3) Communications system shall mean the total communications facilities and equipment owned, leased, or used by all departments, agencies, and subdivisions of state government; and
(4) Communications shall mean 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."

3.2 Information Management Item

Pursuant to Section 81-1117(1), "information management item" includes but is not limited to: (a) Computer equipment; (b) Peripheral devices (such as data input, data output, data storage, or data communications); (c) Computer code, programs or operating systems; and (d) Service contracts for information technology.

4. Related Documents

4.1 Direct Market Purchase Authority (DAS Materiel Memo dated July 1 of each year)
4.2 NIS Procurement Manuals, Document Flows and Menu Selections - Exception Order Purchases for Communication Equipment and Information Management Items
4.3 NIS Final Level of Approvals
4.4 Entering a Purchase Requisition (Including Information Management Items)
4.5 Entering a Purchase Requisition for OT Equipment (Communications Equipment)

Attachment A: List of Preapproved Items for Purchase

VERSION DATE: Draft - December 20, 2007
HISTORY:
PDF FORMAT: (to be added)

NITC 01-204
Attachment A

Office of the CIO

List of Preapproved Items for Purchase

For the purpose of procurement reviews conducted pursuant to NEB. REV. STAT. §§ 81-1117, 81-1120.17 and 81-1120.20, the following items are preapproved for purchase by agencies:

1. Cables for connecting computer components
2. Power Cords / Adapters
3. Extender Cables for Keyboards / Mice
4. KVM (Keyboard - Video - Mouse) Switches
5. USB / PS2 Connectors
6. Memory Chips
7. Laptop Batteries
8. UPS (Uninterruptible Power Supply)
9. Keyboards
10. Mice
11. Speakers
12. Monitors that are ordered without a system
13. Smart Board Overlays
14. Projectors and Projector Lamps
15. Desktop Printers
16. Printer Toner and Ink
17. Desktop Scanners
18. Small Label Printers
19. Blank CDs or DVDs
20. Blank Tapes
21. Digital Voice Recorders
22. Flash Drives
23. Software Books
24. Training CDs or DVDs
25. Logic boards and computers that are integral parts of equipment that serves a primary purpose other than information management, including digital cameras, lab equipment, and motor vehicles.

Date of Last Revision: November 28, 2007
[The current version of this document is available at: http://nitc.ne.gov/standards/xxx.htm]

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Incident Response and Reporting Standard

Category	**Security Architecture**
Title	**Incident Response and Reporting Standard**
Number	

Applicability

☑ State Government Agencies
- ☐ **All**.....Not Applicable
- ☑ **Excluding higher education institutions**.....Standard

☐ State Funded Entities - **All entities receiving state funding for matters covered by this document**.....Not Applicable

☑ Other: **All Public Entities**.....Guideline

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of _____.
Guideline - Adherence is voluntary.

Status	☐ **Adopted**	☐ **Draft**	☐ **Other:**_____
Dates	**Date:** **Date Adopted by NITC:** **Other:**		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1. Purpose and Objectives

Computer systems are subject to a wide range of mishaps; from corrupted data files, to viruses, to natural disasters. These mishaps can occur at anytime of the day or night. Many mishaps are fixed through day-to-day operating procedures, while more severe mishaps are addressed in other plans, e.g. Continuity of Operations (COOP) plans. In some cases, incident handling actions will not be performed by a single person or on a single system. Responses to an incident can range from recovering compromised systems to the collection of evidence for the purpose of criminal prosecution. Therefore, preparation and planning for incidents, and ensuring the right resources are available, are critical to an agencies ability to adequately detect, respond and recover.

A formally documented and coordinated incident response capability is necessary in order to rapidly detect incidents, minimize loss and destruction, mitigate exploited weaknesses, and restore computing services. It prepares agencies to: efficiently respond, protect systems and data, and prevent disruption of services across multiple platforms and between agencies across the State network. Incorporated within these standards are accepted best practices within the law enforcement and Information Technology (IT) security communities. These standards will facilitate cooperation and information exchange among those responsible for responding to and reporting on incidents on any State of Nebraska information system.

2. Standard

It is the responsibility of all State of Nebraska agencies that support information systems to develop, disseminate, and periodically review/update a formal, documented, incident response capability that includes preparation, analysis, containment, eradication, and recovery. In addition, lessons learned from prior and ongoing incident activities should be incorporated into the incident response capability. Agency plans should cover all potential types of incidents, including but not limited to:

- Information system failures and loss of service;
- Denial of service;
- Breaches of confidentiality

In addition to plans that recover systems or services as quickly as possible, the plan should also cover:

- Analysis and identification of the cause;
- Planning and implementation of remedies to prevent recurrence, if necessary;
- Collection of audit trails and similar evidence;
- Communication with those either affected by or potentially affected by the incident; and
- Reporting the incident

2.1 Incident Response Team

Agencies should identify knowledgeable staff that can rapidly respond to, manage, and support any suspected incident to minimize damage to State information system(s), network(s) and data by identifying and controlling the incident, properly preserving evidence, and reporting to appropriate entities. An agency contact list should be developed and maintained for incident response personnel, which includes the names, telephone numbers, pager numbers, mobile telephone numbers, e-mail addresses, organization names, titles, and roles and responsibilities for all key incident response resources, including but not limited to agency personnel and management, other key state agencies, vendors, and contacts.

2.2 Initiate an Incident Log

Documentation of information is critical in situations that may eventually involve authorities, as well as provides a historical event of the actions taken to resolve the event. Manually written incident logs are preferable since electronic logs can be altered or deleted. The minimum information that should be recorded is:

- When (date and time) and how the incident was reported, discovered or occurred;
- Who reported or discovered the incident;
- Description of the incident;
- Incident-related tasks and who performed each, and the amount of time spent on each task;
- Individuals contacted regarding the incident; and
- Information system(s), program(s) or network(s) affected.

2.3 Classification of Incidents

The agency Information Security Officer (ISO) should review the incident information to determine if an actual incident has occurred. Incidents are classified into four tiers based on the severity of the incident: Tier 1, Tier 2, Tier 3, or Tier 4.

Tier	Definition	Examples	Report to SISO	Activate Agency IRP
1	Localized, minor incidents. Non-critical systems.	- Localized virus attacks - Internet abuse, excluding criminal behavior - Incidents traceable to user error or system failure - Minor attempts at intrusion, scanning or pinging - Missing IT devices or equipment with storage capabilities	Report verbally to the SISO within one business day	No
2	Incidents affecting critical systems or information; or affecting more than one agency.	- Coordinated, distributed attacks - Any attack which causes Denial of Service - Financial fraud - Unauthorized activity involving a server, host, or Confidential system (HR, Legal, Financial, etc.) - Theft of proprietary information - Internet abuses violating Federal/ State law - Theft of IT devices with storage capabilities	Report verbally to the SISO immediately for determination of escalation, and/or assistance.	Yes
3	Incidents impacting multiple agencies	- Service provider outage - Core network outage - Mainframe outage	Report verbally to the SISO immediately.	Yes
4	Governor declared emergency	- Activation of COOP Plan	No	As directed

2.4 Cyber Security Incidents

Each agency shall securely maintain any information collected, generated, or assessed in the course of determining whether an incident is a potential cyber security incident warranting prosecution. Data collection shall focus on identifying who, what, when, where, and the how of an incident. Collected information shall be properly documented and safeguarded. Evidence such as system and network log files, user files, system administrator logs and notes, backup-up tapes, and intrusion detection system logs, alarms or alerts shall be securely maintained and the chain of custody preserved by:

- Ensuring the evidence has not been altered;
- Ensuring the evidence is accounted for at all times;
- Verifying the passage of evidence from one party to another is fully documented; and
- Verifying the passage of evidence from one location to another is fully documented.

If an incident is determined not to be a cyber security incident, agencies are still required to maintain any evidence and its chain of custody because future incidents may require the previously captured evidence.

2.4.1 Security Incident Evidence File

An evidence file shall be created to record and maintain an inventory of all actions taken, action timestamps and correspondence associated with a security incident.

2.4.2 Notification of Personal Information Security Breach

Agencies shall determine if the incident resulted in a breach to a system containing personal information and then notify affected individual as required by Neb. Rev. Stat. § 84.121 or other State or Federal regulatory guidelines.

2.4.3 Security Incident Confidentiality

Communication shall be on a need-to-know basis and shall be considered confidential during a security incident investigation. Incident responders are not to share any details with anyone other than the Incident Response team, agency management or the State Information Security Officer (SISO) (see Section 2.12)

2.5 Reporting to the State Information Security Officer

Agencies shall report incident information to the SISO. The SISO will contact appropriate authorities in accordance with State or Federal incident reporting procedures, applicable laws, directives, policies, regulations, standards, and procedures; and to US-Cert and law enforcement, if necessary. Reporting to the SISO does not relieve agencies from other reporting requirements.

The SISO has the responsibility to inform other agencies about incidents impacting multiple agencies that may become a potential threat.

2.6 Escalation Process

Agencies should periodically review the incident conditions and determine if escalation to a higher tier is appropriate. An incident may be escalated in any of the following ways:

- Determination by the Chief Information Officer or State Information Security Officer;
- Additional related events (i.e. emergence of a distributed, coordinated attack, etc.)
- Requested by agency management.

2.6.1 Escalation Thresholds

Agencies should consider escalating an incident when certain conditions are met. The following thresholds of incident actions, are examples of when to consider incident escalation:

- Multiple machines per LAN segment showing Intrusion Prevention System signature;
- Multiple machines showing multiple Intrusion Prevention System signatures;
- One or more critical infrastructure/application showing Intrusion Prevention system signatures;
- Significant impact on bandwidth;
- When a concerted effort is shown to be attacking the network, either internally or externally;
- Any known or reported compromise of Personal Identifiable Information (PII);
- Any website defacement.
- Abnormal increases in any of the above.

2.7 Response to Incidents

Priority in incident response is given to preventing further damage to State information systems. Therefore, the Office of the CIO reserves the right to quarantine any potentially threatening agency or system.

2.7.1 Incident Containment

Agencies shall identify containment strategies to control an incident's impact to compromised systems, limit the extent of the incident, prevent further damage and regain normal operations of affected systems. Agency containment measures should take into consideration available resources, the classification of an incident, agency Continuity of Operations Plans (COOP) and procedures regarding response methods. Containment measures shall also be evaluated against the potential loss or corruption of security incident evidence. Containment methods shall include as a minimum:

- Ensuring redundant systems and data have not been compromised;
- Monitoring system and network activity;
- Disabling access to compromised shared file systems;
- Disabling specific system services;
- Changing passwords or disabling accounts;
- Temporarily shutting down the compromised or at risk system; and
- Disconnecting compromised or at risk systems from the network.

2.7.2 Incident Eradication

Agencies shall develop and employ mitigation strategies prior to returning compromised systems to service to protect against like or similar types of incidents in the future. Mitigation strategies may include, but are not limited to:

- Changing passwords on compromised systems;
- Disabling compromised accounts;
- Identifying and removing an intruder's access method
- Installing system patches for known weaknesses or vulnerabilities;
- Adjusting or deploying firewall or intrusion detection system technologies to detect access and intrusion methods;
- Code changes to internal applications.

2.8 Recovery

Agencies shall evaluate and determine when to return compromised systems to normal operations. Access to compromised systems shall be limited to authorized personnel until the security incident has been contained and root cause mitigated. Analysis and mitigation procedures shall be completed as soon as possible, recognizing agency systems are vulnerable to other occurrences of the same type. Recovery procedures shall address:

- Recovery Requirements. The agency shall define and prioritize the requirements to be met before returning an affected or compromised system to normal operations. Recovery strategies may include, but are not limited to:
  - Reinstalling compromised systems from trusted backup-ups; and
  - Reinstalling system user files, startup routines, or settings from trusted versions or sources;
- Validate Restored Systems. Agencies shall validate the restored systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons.
- Increased Security Monitoring. The agency shall heighten awareness and monitoring for a recurrence of the incident.

2.9 Follow-up Analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up analysis should be performed within three to five days of recovering from the incident to discuss actions that were taken and lessons learned. Extended delays may reduce the effectiveness of relating critical information. Follow-up analysis include a review of the chronological events, identifying all containment and eradication actions taken, identification of mitigation strategies, examining the lessons learned, and assessing the incident costs. Questions to be addressed may include, but are not limited to:

- Did detection and response systems work as intended? If not, what methods would have prevented the incident?
- Are there additional procedures that would have improved the ability to detect the incident?
- What improvements to existing procedures and tools would have aided in the response process?
- What improvements would have enhanced the ability to contain the incident?
- What correction procedures would have improved the effectiveness of the recovery process?
- What updates to agency policies and procedures would have allowed the response and recovery processes to operate more smoothly?
- How could user and system administrator preparedness be improved?
- How could communication throughout the detection and response processes be improved?
- Was the incident previously identified as a potential threat?
- What was the impact in terms of financial loss, loss of public or customer trust, legal liability, or harm to public health and welfare?

Results of these questions should be documented and incorporated into existing procedures, if necessary.

2.10 Incident Response Training

2.10.1 All Users

Agencies will provide education and awareness programs for users in incident response procedures and reporting methods. The programs shall address:

- What types of events are incidents;
- Agency notification procedures; and
- Existing and emerging threats.

2.10.2 Agency IT Staff

Agency staff responding to incidents are encouraged to obtain the following training, according to their roles and responsibilities:

- State and Federal security and privacy laws and procedures
- Technical training on all platforms, operating systems and applications they may be responding to.

2.11 Incident Response Testing

Testing should be conducted at least annually, either in response to an identified incident or as part of a formal readiness test, using defined tests, simulated events, and exercises to determine the effectiveness of the incident response capability.

2.12 Release of Information

Control of information during the course of an incident or investigation of a possible incident is very important. Only the affected agency can authorize the release of all incident information. Specific information concerning the incident, such as accounts involved, programs or system names, are not to be provided to any callers regardless of who they claim to be.

3.0 Applicability

3.1 State Government Agencies
All State agencies, boards, and commissions are required to comply with the standard listed in Section 1.0.

3.2 Exemption
There is no exemption allowed to this Standard by any agency, board, or commission.

4.0 Responsibility

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

4.2 State of Nebraska Information Security Officer
The SISO serves as a security advisor to all State of Nebraska agencies and shall act as the incident response coordinator for the state. In that capacity, the SISO shall perform the following functions:

- Create a statewide incident response reporting procedure and instruct agencies as to the requirements of the procedure.
- Maintain a central list of agency Information Security Officers or incident response point of contact information.
- Receive incident reports, and evaluate, verify, validate and as needed disseminate alerts to State of Nebraska agencies. Alert notification will not include the name of impacted agencies or agency specifics, unless permitted.
- Coordinate with affected agencies in determining the need to disseminate alerts to federal entities, law enforcement, and any other appropriate parties.

4.3 State Agencies
When an incident occurs, agencies must provide a verbal report to the SISO based upon the guidelines listed in section 2.3. A written preliminary report must be completed within two (2) working days using the Incident Reporting Form. This report is to be completed by the individual handling the incident; however all people involved are responsible for providing information regarding their actions. Within ten (10) working days of the resolution of an incident, a written final report must be submitted. In cases where incident resolution is expected to take more than thirty (30) days, a weekly status report must be submitted to the SISO.

Should an incident be serious enough to warrant prosecution, law enforcement will need to demonstrate a chain of custody and provide records of actions taken; therefore a log must be kept, including recovery steps and other regular or routine work performed on the affected system(s). This log should be separate from normal system logs, since it may be used as evidence.

Agencies are responsible for training personnel in incident response capabilities according to their roles and responsibilities.

Agencies that support information systems shall provide a support resource, i.e. a Help Desk, which serves as the primary contact to report incidents.

4.3.1 Agency Incident Response Contacts

Agencies are responsible for providing a primary and secondary point of contact to act as a liaison with the SISO. The agency point of contact can be the agency Information Security Officer (ISO) or some other designee. See Information Security Policy, Appendix B for Roles and Responsibilities of the (ISO).

4.4 Users

All information system(s) users are responsible for understanding their role and complying with agency incident handling procedures. Users must immediately report suspicious activities to their manager and/or agency or State of Nebraska HelpDesk and fully cooperate with personnel tasked with resolving the incident.

5.0 Definitions

Availability. The assurance that information and services are delivered when needed.

Breach. Any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

Chain of Custody. 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.

Compromise. 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.

Confidentiality. The assurance that information is disclosed only to those systems or persons that are intended to received that information.

Continuity of Operations (COOP) Plans – Provides for the continuation of government services in the event of a disaster.

Cyber Security Incident. Any electronic, physical, natural, or social activity that threatens the confidentiality, integrity, or availability of State of Nebraska information systems, or any action that is in violation of the Information Security Policy. For example:

- Any potential violation of Federal or State law, or NITC policies involving State of Nebraska information systems.
- A breach, attempted breach, or other unauthorized access to any State of Nebraska information system originating from either inside the State network or via an outside entity.
- Internet worms, Trojans, viruses, malicious use of system resources, or similar destructive files or services.
- Any action or attempt to utilize, alter, or degrade an information system owned or operated by the State of Nebraska in a manner inconsistent with State policies.
- False identity to gain information or passwords

Denial of Service. An inability to use system resources due to unavailability; for example, when an attacker has disabled a system, or a network worm has saturated network bandwidth.

Incident. An occurrence having actual or potentially adverse effects that causes an interruption of the agency's business activities. It may or may not apply to an Information System.

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

Incident Response Team. A group of professionals within an agency trained and chartered to respond to identified information technology incidents.

Information System. 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, E-mail, and web based services.

Integrity. The assurance that information is not changed by accident or through a malicious or otherwise criminal act.

Recovery. A defined step or process within an incident response plan with the goal of returning the affected or compromised systems to normal operations.

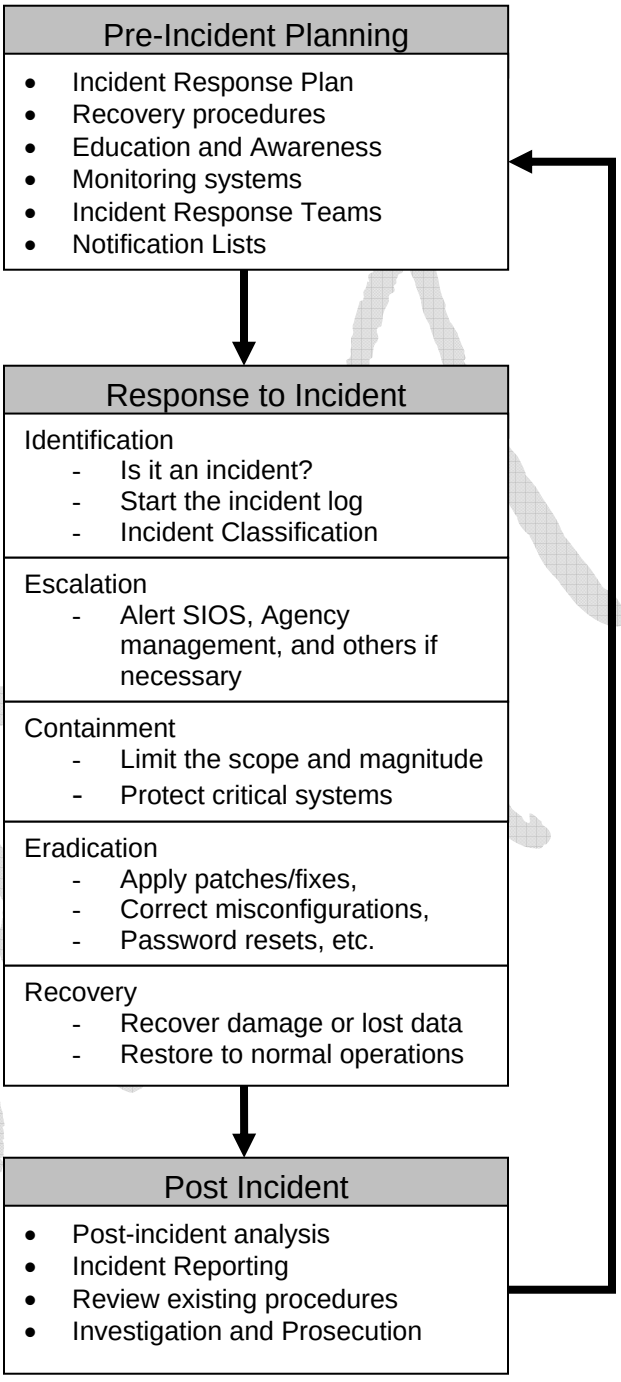
6.0 Related Documents

6.1 NITC Security Officer Handbook (http://www.nitc.state.ne.us/standards/security/so_guide.doc)
6.2 NITC Information Security Policy (http://www.nitc.state.ne.us/standards/index.html)
6.3 State of Nebraska INCIDENT RESPONSE FORM – Attachment A

7.0 References

7.1 National Institute Standards and Technology (NIST) Special Publication, 800-61, "Computer Security Incident handling Guide." (http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf).

State of Nebraska
Incident Handling Lifecycle



State of Nebraska INCIDENT RESPONSE FORM

This form is based on the State of Nebraska Incident Response Standard, which agencies are required to use when reporting an incident. An automated version of this form can be found at ??????????. For urgent assistance, contact the State Information Security Officer at (402) 471-7031 or 416-3668.

1. Point of Contact Information for this Incident:

Name:	Agency:
Phone:	Cell/Pager:

2. Physical Location of Affected Computer/Network:

(include building number, room number, etc)

3. Date and Time Incident Occurred and Duration:

(mm/dd/yy)	(hh:mm:ss am/pm)	Duration:

4. Type of Incident (check all that apply):

☐ Intrusion	☐ Access Control Avoidance
☐ Denial of Service	☐ Unauthorized Access
☐ Virus / Malicious code (complete 4a)	☐ User Account Compromise
☐ System Misuse	☐ Hoax
☐ Social Engineering	☐ Network Scanning / Probing
☐ Technical Vulnerability (complete 4b)	☐ Root Compromise
☐ Equipment Missing or Lost (complete 4c)	☐ Web Site Defacement
☐ Equipment Stolen or Damaged (complete 4c)	☐ Other (specify)

4a. Provide the name(s) of the virus(es) and any URLs used to obtain information specific to the virus. Provide a synopsis of the incident and any actions taken to disinfect and prevent further infection.

4b. Generally describe the nature and effect of the vulnerability. Describe the conditions under which the vulnerability occurred and the specific impact of the weakness or design deficiency. Has the application vendor been notified?

4c. Provide the make, model, serial number, and tag number:

5. Information on Affected System:

IP Address:	Computer/Host Name:	OS (include release number):	Other Applications:

6. Information on Affected Hardware/Software:

(include version and release information)

7. Number of Host(s) Affected:

☐ < 10 ☐ 10 to 50 ☐ 50 to 100 ☐ > 100

8. IP Address of Apparent or Suspected Source:

Source IP Address:	Other information available:

9. Incident Assessment:

Is this incident a threat to life, limb, or a critical agency service? ☐ Yes ☐ No If yes, elaborate:

List the most restricted classification of the data residing on the system.

Damage or observations resulting from the incident:

10. Information Sharing:

Who can this information be shared with, outside the Office of the CIO? (do not leave blank and check all that apply)

☐ Other Agencies ☐ Law Enforcement ☒ US-CERT ☐ **No sharing is Authorized**

11. Additional Information:

If this incident is related to a previously reported incident, include previous incident information

Return this form to: State Information Security Officer, 501 S. 14th Street, Lincoln, NE