Technical Panel
of the
Nebraska Information Technology Commission

Draft Document
30-Day Comment Period

Title: Information Technology Disaster Recovery Plan Standard

Notes to Readers:

1. The following document is a draft standard under review by the Technical Panel of the Nebraska Information Technology Commission (NITC). This document is available in both PDF and Word versions at http://www.nitc.state.ne.us/standards/index.html.
2. If you have comments on this document, you can send them by e-mail to rick.becker@nitc.ne.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on May 22, 2006.
4. The Technical Panel will consider this standard and the comments received at their meeting currently scheduled for June 13, 2006. Final approval of the standard would be considered by NITC at their next meeting following the Technical Panel review. Information about these meetings will be posted on the NITC web site at http://www.nitc.state.ne.us/.

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Information Technology Disaster Recovery Plan Standard

Category	**Security Architecture**
Title	**Information Technology Disaster Recovery Plan 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: Review**

Dates

Date: April 17, 2006
Date Adopted by Nebraska Information Technology Commission: April 23, 2001
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/

1.0 Standard

Each agency must have an Information Technology Disaster Recovery Plan that supports the resumption and continuity of computer systems and services in the event of a disaster. The plan will cover processes, procedures, and provide contingencies to restore operations of critical systems and services as prioritized by each agency. The Disaster Recovery Plan for Information Technology may be a subset of a comprehensive Agency Business Resumption Plan which should include catastrophic situations and long-term disruptions to agency operations.

The Information Technology Disaster Recovery Plan should be effective, yet commensurate with the risks involved for each agency. The following elements, at a minimum, must be included:

- Identification of critical computer systems and services to the agency's mission and business functions.
- Critical systems and services preservation processes and offsite storage strategy and methods to protect storage media.
- Documented dependencies upon other State agency's or entities that support critical systems and services.
- Contingency plans for different types of disruptions to critical systems and services, i.e. hardware failure, etc.
- Information technology responsibilities for implementation and disaster management.
- Procedures for reporting events, as well as escalating an event within an agency.
- Identification of copy distribution and multiple site storage of plan documents.
- Multi-year training, exercising, and improvement plans.
- Annual plan review, revision, and approval process.

2.0 Purpose and Objectives

The purpose of this document is to define, clarify, and standardize Information Technology Disaster Recovery Planning of State government agencies.

2.1 Background

Information Technology Disaster Recovery Plans are based on the following premises:

2.1.1 *Information is an asset.* It has value to the organization and needs to be suitably protected.

2.1.2 *Information resources must be available when needed.* Continuity of information resources and supporting critical systems and services must be ensured in the event of a disruption to business or a disaster.

2.1.3 *Risks to information resources must be managed.* Procedures required to ensure critical systems and services can be recovered and business continuity sustained must be cost effective and commensurate with the value of the assets being protected.

2.2 Objectives

The primary objectives of this Standard are:

2.2.1 To communicate responsibilities for the continuity of government operations;

2.2.2 To establish a plan for restoration of operations following a disaster.

2.2.3 To reduce the risk of loss of state information assets.

2.2.4 To provide a process for the recovery of critical systems and services.

3.0 Definitions

3.1 Agency

Any governmental entity, including state government, local government, or third party entities under contract to the agency.

3.2 Agency Business Resumption Plan

Documents how an agency will continue to function during a disaster.

Note: Items found in an Agency Business Resumption Plan may include, but is not limited to:

- *Business impact analysis, including risk assessment, asset classification, and potential disruption to stakeholders.*
- *Mitigation strategies and safeguards to avoid disasters. Safeguards include, but are not limited to, protective measures such as redundancy, fire suppression, power source protection, and environmental issues.*

3.3 Critical Systems and Services
Those systems, system components (hardware, data, or software), or services that if lost or compromised would jeopardize an agency's ability to continue agency operations.

3.4 Disaster
Any event that threatens or causes the destruction or availability of critical systems and services.

4.0 Applicability

This standard applies to all state government agencies, except Higher Education and those agencies receiving an exemption under Section 4.1. Compliance with Nebraska Information Technology Commission (NITC) standards will be a requirement during consideration of funding for any projects requiring review by the NITC and may be used in audit reviews or budget reviews.

4.1 Exception

Exemptions may be granted by the NITC Technical Panel upon request by an agency.

4.1.1 Exception Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion, federal government requirement; or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 521 S 14th Street, Suite 301, Lincoln, NE 68508). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the Technical Panel may be appealed to the NITC.

5.0 Responsibility

5.1 NITC

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

5.2 Agency and Institutional Heads

The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing disaster recovery/business continuity programs consistent with this standard. The authority may delegate this responsibility but delegation does not remove the accountability.

6.0 Related Documents

6.1 Agency IT Disaster Recovery Plan Standard Content

6.2 Information Security Management Policy

http://www.nitc.state.ne.us/tp/workgroups/security/policies/security_policy.pdf

6.3 Security Breaches and Incident Reporting Policy

http://www.nitc.state.ne.us/tp/workgroups/security/policies/incident_reporting_policy.pdf