Title	**Disaster Planning Procedures for Information Technology**
Category	**Security Architecture**
Applicability	**All Public Entities** (See the "Applicability" section below.)
Status	☐ **Standard -** A degree or level of requirement that all jurisdictions should use, which would be enforceable by duly authorized entities. With any standard, there may be circumstances that merit exceptions. ☑ **Guideline -** A statement of general policy or procedure by which to determine a course of action. Adherence is voluntary.
Date Adopted	**DRAFT (October 2, 2002)**
Date of Last Revision	
Date of Next Review	

A. Authority

Section 86-516 (6). "[The Nebraska Information Technology Commission shall] adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel."

The Nebraska Information Technology Commission (NITC) has adopted a security policy pertaining to disaster recovery, which states that:

> "Each agency must have a disaster recovery plan that at least identifies and mitigates against risks to critical systems and sensitive information in the event of a disaster. The plan shall provide for contingencies to restore information and systems if a disaster occurs. The disaster recovery plan for information technology may be a subset of an agency's comprehensive disaster recovery plan. The concept of a disaster recovery includes business resumption." (http://www.nitc.state.ne.us/standards/index.html)

B. Purpose and Objectives

Information technology (IT) and automated information systems are vital elements in most business processes. Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

This template provides instructions, recommendations, and considerations for Nebraska State Government IT contingency planning. It discusses essential contingency plan elements and processes, highlights specific considerations and concerns associated with contingency planning for various types of IT systems, and provides examples to assist readers in developing their own IT contingency plans. The scope ranges from minor incidents causing short-term disruptions to disasters that affect normal operations for an extended period. Because IT systems vary in design and application, specific incident types and associated contingency measures are not provided in this document. Instead, the planning guide defines a process that may be followed for any IT system to identify planning requirements and develop an effective contingency plan.

C. Assumptions

Following is a list of typical planning assumptions to be considered in writing the disaster recovery plan. Each agency must review and modify this list to meet their specific requirements. In particular, this list of assumptions does not entail certain worst-case scenarios, such as losing staff that would perform critical functions in exercising the disaster recovery plan.

1. The IT business continuity plan is part of a bigger plan that covers areas outside of IT (i.e., facilities, personnel, etc). The Nebraska Emergency Management Agency (NEMA) is currently revising the State Emergency Operations Plan (SEOP). Changes to the SEOP may provide state and local government with guidance on preparing business continuity plans that address internal operations and the ability to provide public services following a disaster. The relationship between the IT business continuity plan and the overall agency business continuity plan includes the following points:
   - The IT business continuity plan is a subset of the agency's overall business continuity plan.
   - Internal and external dependencies will be listed in the IT business continuity plan.
   - The IT business continuity plan will address internal dependencies, and the agency's overall business continuity plan will address external dependencies.
2. The plan will be approved and endorsed by management.
3. The plan will only cover critical information systems in the order of the highest priority. It will not cover every information system within an organization.
4. Staff is available to perform critical functions defined within the plan.
5. Staff can be notified and can report to the backup site(s) to perform critical processing, recovery and reconstruction activities.
6. Off-site storage facilities and materials will survive.
7. The disaster recovery plan is current.
8. Subsets of the overall plan can be used to recover from minor interruptions.
9. An alternate facility is available.
10. The necessary utilities (i.e., long distance and local communications lines, Wide Area Network and Internet connectivity, power, etc.) are available to the organization as defined in the dependencies section of the plan.
11. Outside organizations, including vendors will perform according to their general commitments to support the organization in a disaster.
12. Development, test, and implementation of new technologies and applications will be suspended during the disaster so that all resources will be available to the recovery.
13. Other assumptions.

D. IT Contingency Planning Process

To develop and maintain an effective IT contingency plan, organizations should use the following approach in the sequence shown:

1. *Develop the contingency planning policy statement.*
   A formal policy provides the authority and guidance necessary to develop an effective contingency plan. The Security Architecture Work Group (a Work Group sponsored by the Technical Panel of the Nebraska Information Technology Commission) developed the

state's Disaster Recovery Policy:
http://www.nitc.state.ne.us/tp/workgroups/security/security_policies.htm.

2. *Conduct the business impact analysis (BIA) and risk analysis (RA).*
The BIA helps to identify and prioritize critical IT systems and components. It's purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. Key steps include listing critical IT resources, identifying disruption impacts and allowable outage times, and developing recovery priorities.

   When working on the BIA phase of the IT continuity plan, there are two goals to keep in mind for each business process: the recovery time objective (RTO) and the recovery point objective (RPO). RTO defines the tolerable maximum length of time that a business process can be unavailable, while RPO defines how much work in progress can be lost.

   The BIA and risk assessment procedures are documented in Chapter 3 of the Security Officer Instruction Guide (http://www.nitc.state.ne.us/tp/workgroups/security/documents.htm). Business continuity coordinators should reference that document for information on conducting an BIA. NIST SP 800-34 contains a sample BIA process and template that may also be used.

   Having determined the impacts, it is now important to consider the magnitude and likelihood of risks. Again, this is a critical activity - it will determine which scenarios are most likely to occur and which should attract most attention during continuity planning. This should include both partial and total system loss as well as least and worst case scenarios. Assessing the probability of an event and the likely loss should it occur associated with specific disaster scenarios helps determine appropriate and cost-effective preventive controls and recovery strategies.

3. *Identify preventive controls.*
In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. Preventive controls should be documented in the contingency plan, and personnel associated with the system should be trained on how and when to use the controls. Adequate insurance coverage is one means to mitigate the financial impact of a disaster.

   Business continuity coordinators should list all preventive controls.

4. *Develop recovery strategies.*
Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. Strategies should address disruption impacts and allowable outage times identified in the BIA. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans. These strategies should be prioritized, based on the scenarios developed in the risk analysis phase.

   The selected recovery strategy should address the potential impacts identified in the BIA/RA and should be integrated into the system architecture during the design and implementation phases of the system life cycle. It should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, type of system, budget resources and its operational requirements as determined in the previous phases.

Assumptions and dependencies should be identified as part of the recovery strategy. These are areas beyond the scope of control of the planners.

5. *Format an IT Contingency Plan.*
IT contingency plan development is a critical step in the process of implementing a comprehensive contingency planning program. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. The contingency plan should document technical capabilities designed to support contingency operations. Each organization must tailor the contingency plan and its requirements to fit their needs. Plans need to balance detail with flexibility; usually the more detailed the plan, the less scalable and versatile the approach.

   The contingency plan comprises five main components:
   - Supporting Information
   - Notification/Activation Phase
   - Recovery Phase
   - Reconstitution Phase
   - Plan Appendices

   See Section IV for more details.

6. *Plan Testing, Training, and Exercises.*
Each IT contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively.

   The ideal disaster test scenario uses a true-to-life model that draws participants into the exercise and allows them to test their procedures realistically. The test scenario may be at any level from a single system to an entire enterprise being affected. Planners should use explicit test objectives and success criteria in their test plan in order to assess the effectiveness of each plan element and the overall plan. Information collected during the test and post-test reviews that improve plan effectiveness should be incorporated into the contingency plan.

7. *Plan Maintenance.*
To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change management process, to ensure new information is documented and contingency measures are revised if required. Responsibility for plan currency must be assigned as part of critical job duties. As a general rule, the plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements will require more frequent reviews, such as contact lists. Based on the system type and criticality, it may be reasonable to evaluate plan contents and procedures more frequently.

   The business continuity plan should be stored away from the organization’s primary facility. Records management has the ability to store these documents in their repository; however, they take no responsibility for the documents.

E. Contingency Plan Development

This section discusses the key elements that comprise the contingency plan. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. It should be tailored to each department or agency.

1. *Supporting Information*

   The Supporting Information component includes an introduction and concept of operations section that provides essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. These details aid in understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found.

   a) Introduction Section

   This section orients the reader to the type and location of information contained in the plan. It contains the following subsections:

   i) Purpose
   ii) Applicability
   iii) Scope
   (1) Scenarios
   (2) Assumptions
   (3) Dependencies
   iv) References/requirements
   v) Record of Changes

   b) Concept of Operations

   This section provides additional details about the IT system, the contingency planning framework; and response, recovery, and resumption activities. This section may include the following elements:

   i) System Description
   ii) Line of Succession
   iii) Responsibilities
   iv) External Communications

2. *Notification/Activation Phase*

   The Notification/Activation Phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify both management and recovery personnel, assess system damage, and implement the plan. Notification/Activation must match the overall organizational recovery plan. At the completion of the Notification/Activation Phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis.

3. *Recovery Phase*

   The Recovery Phase begins after the contingency plan has been activated, damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery phase activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the Recovery Phase, the IT system will be operational and performing the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site. Teams with recovery responsibilities should understand and be able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, they can still perform the necessary activities.

4. *Reconstitution Phase*
   In the Reconstitution Phase, recovery activities are terminated, and normal operations are transferred back to the organization's facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support system processing requirements. Once the original or new site is restored to the level that it can support the IT system and its normal processes, the system may be transitioned back to the original or to the new site. Until the primary system is restored and tested, the contingency system should continue to be operated. The Reconstitution Phase should specify teams responsible for restoring or replacing both the site and the IT system.

5. *After Action Review*
   An After Action Review (AAR) is an assessment conducted after the business continuity activity (i.e., disaster, test, etc.) that allows employees and leaders to discover what happened and why. It may be thought of as a professional discussion of an event that enables employees to understand why things happened during the progression of the process and to learn from that experience. The AAR is an essential element to complete the four-step planning cycle of review, update, modify, and plan.

6. *Contingency Plan Appendices*
   Contingency Plan Appendices provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the given system. Appendices can include, but are not limited to contact information for contingency planning team personnel; vendor contact information, including offsite storage and alternate site POCs; standard operating procedures and checklists for system recovery or processes; equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations; vendor agreements, reciprocal agreements with other organizations, and other vital records; description of, and directions to, the alternate site; and the BIA.

F. Applicability

The issue of disaster recovery planning for information technology applies to any agency or institution that relies on information technology to support critical business functions. Agencies or institutions should follow a structured methodology, such as these guidelines, in developing a disaster recovery plan for information technology.

G. Responsibility

1. Nebraska Emergency Management Agency (NEMA). NEMA is responsible for preparing and maintaining the State Emergency Operations Plan. One element of this plan pertains to continuity of government operations. Disaster planning procedures for information technology is a subset of continuity of government operations.
2. State Records Management Division, Secretary of State’s Office. The Records Management Division serves as a repository for back-up media. The Records Management Division will also store electronic and paper copies of an agencies disaster recovery plan.

3. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs, including disaster recovery plans for information technology. The authority may delegate this responsibility but delegation does not remove the accountability.
4. Agency Information Officer. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest-ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies, including disaster recovery planning for information technology.
5. Agency Security Officer. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for preparing a disaster recovery plan for information technology. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan for information technology.

H. Related Standards and Guidelines

1. NITC Disaster Recovery Policy (http://www.nitc.state.ne.us/tp/workgroups/security/security_policies.htm)
2. NITC Security Officer Handbook (http://www.nitc.state.ne.us/standards/security/so_guide.doc)
3. Nebraska Emergency Management Agency – Information Paper on Continuity of Operations Plan (available from NEMA at 402.471.7430)

I. References

1. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, http://csrc.nist.gov/publications/drafts/ITcontingency-planning-guidelines.pdf
2. Business Continuity Planning & Management on-line, http://www.contingencyplanning.com/
3. Disaster Recovery Journal, http://www.drj.com/
4. Contingency Planning and Disaster Recovery, http://www.disasterplan.com/
5. Kansas, Department of Administration, Contingency Planning On-Line, http://csrc.nist.gov/publications/drafts/ITcontingency-planning-guideline.pdf
6. FEDERAL EXECUTIVE BRANCH CONTINUITY OF OPERATIONS (COOP), http://www.fas.org/irp/offdocs/pdd/fpc-65.htm

J. Additional Information For State Agencies

1. Insurance Coverage. State agencies should consider insurance coverage to mitigate the financial impact of a disaster. The Risk Management Division of the Department of Administrative Services offers two types of insurance coverage. Content insurance applies to fixtures and equipment within a building. Current cost is $.05 per $100 value, with a $5,000 deductible per event. Inland Marine Insurance covers non-permanent fixtures that are highly portable, such as laptops. The cost is $.12 to $.15 per $100 value. When calculating the value of equipment to be covered, agencies should include the cost of any services that might be used to restore services. Insurance should not be used instead of good disaster planning and mitigation strategies.

The Risk Management Division is working with the state's insurance broker to narrow the current exclusion of "terrorism". The state's insurance contracts provide some assistance with conducting risk assessments. The state's insurance broker also offers business continuity planning services for a fee.

2. Personnel issues. Agencies should be aware of labor contract requirements when developing their disaster recovery plans. The labor contract may affect options regarding leave time when the work site is not available, ability to work at an alternate site, working from home, and other issues. Counseling is available through the state's employee assistance program contract. Temporary staff is available through State Personnel's SOS program and IMServices' contractual services agreements.

3. Purchasing Issues. The Materiel Division can assist agencies with replacing equipment. Surplus Property is one option to consider. Existing contracts facilitate acquiring equipment, without the need for bids. The contract with IBM obligates the vendor to give priority and expedite shipment in the event of a disaster. Similar terms are being negotiated with Dell. Agencies should maintain complete equipment lists, including current configurations.

4. Information Management Services Division. IMServices houses much of the state's data and applications either on the mainframe or LAN servers located in the 501 Building. As custodians of this equipment and information, IMServices has its own disaster recovery plans to protect those assets. Agency information technology disaster recovery plans are simplified when IMServices manages the hardware, software and data resources, but agencies should include references and communications with IMServices regarding expectations for how much and how fast their applications and data functions need to be restored. Procurement of replacement LAN servers housed in 501 but owned by an agency are the responsibility of the agency. IMServices provides and manages backup services for mainframes, LAN servers at the 501 Building, and agency-owned servers that may be located anywhere on the campus LAN. Backup tapes (and the Gator backup System) are housed in the Capitol Computing Center and will be available for business resumption once the platform and/or network are restored.

   A Business Impact Analysis process to aid in applying the appropriate level of planning and investment against loss of IT assets and capability is contained in the Security Officer Guide developed by the NITC (http://www.nitc.state.ne.us/standards/security/so_guide.doc).

5. Communications. The Division of Communications (DOC) is currently involved in a feasibility study in conjunction with IMS to determine if the existing core routing equipment can be duplicated off site, or split between two sites. DOC carries a limited amount of spare equipment that can be used at disaster sites, and we require our main vendors (Qwest and Alltel) to carry a certain number of spares. Although we do not have a formal agreement with the telcos, we expect to receive priority service from the telcos in the event of an emergency. DOC also has caches of cellular phones located at strategic positions about the State that can be quickly activated and distributed. DOC also assists agencies, such as NEMA, for coordinating radio communications when needed.