



State of Minnesota CIO Standard

Enterprise Security Standard on Continuity of Operations *Security Standard 2007 - 01*

Standard Statement

State agencies shall develop, implement, test, and maintain a Continuity of Operations Plan.

Reason for the Standard

Continuity of operation planning is the process of identifying, mitigating and responding to an interruption of services. The purpose of this standard is to establish “*when*” continuity of operations planning is required, “*what*” is required and “*why*”.

Who Should Know about this standard

Leaders of state agencies and continuity planners of agencies in the executive branch of government.

This standard is applicable to any arrangement with third parties who participate, support, or conduct services related to continuity of operations for the State.

This standard is offered as guidance to local government, higher education, K-12 or other government related entities.

Related information

The following sources were used in the development of this standard.

1. Enterprise Security Policy on Continuity of Operations
2. Governor's Executive Order 07-14: Assigning Emergency Responsibilities to State agencies
3. Governor's Executive Order 05-02: Designation of the National Incident Management System (NIMS) as the basis for all incident management situations in the State of Minnesota
4. [Disaster Recovery Institute International Methodology](#)
5. [Business Continuity Institute – Business Continuity Management - Good Practice Guideline, 2005](#)

6. [NIMS Requirements](#)
7. [Minnesota Statute 16B.85 Risk Management](#)
8. [ISO/IEC 17799 - Code of Practice for Information Security Management](#)
9. [NFPA 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs](#)
10. [Federal Preparedness Circular 65](#)

Contacts

Debra Stafford, Corrective and Investigative Security Controls Manager
651-201-1146
debra.stafford@state.mn.us

Chris Buse, Chief Information Security Officer
651-201-1200
chris.buse@state.mn.us

History

This standard is effective on December, 31 2007. Compliance is required by June 30, 2011.

Applicability

All departments, agencies, offices, councils, boards and commissions in the executive branch of Minnesota State Government must comply with this standard by June 30, 2011.

This standard is applicable to any arrangement with third parties who participate, support, or conduct services related to continuity of operations for the State.

This standard is offered as guidance to local government, higher education, K-12 or other government related entities.

Definitions

All Hazards Approach

An approach to continuity planning not based on specific interruption scenarios. A plan developed using this approach will be effective regardless of the incident.

Business Impact Analysis (BIA)

A report identifying the services and processes of an organization, the priority for their restoration and the support services that support them. The BIA ensures that the services of the agency will be restored in the appropriate priority order.

Continuity of Operations Plan (COOP)

Series of plans used to respond, recover, resume and restore from a business interruption.

Controls

Countermeasures used to mitigate the probability of a vulnerability occurring or minimize the impact.

Crisis Management Plan (CMP)

A document defining a communication method and management approach for providing timely, consistent and accurate crisis information to employees, customers and the public.

Disaster Recovery Plan (DRP)

Plans to ensure systems and communications are restored within a predetermined timeframe.

Incident Management Plan (IMP)

A document defining the structure, roles and responsibilities, process and procedures aimed to minimize the impact of a disruption to an agency by managing available resources of various disciplines.

Recovery Time Objective (RTO)

The maximum period of time available for recovering time sensitive processes before there is a significant impact on the agency.

Recovery Point Objective (RPO)

The time to which data must be synchronously restored (e.g. close of business the previous day). RPO refers to the tolerance for the loss of data measured in terms of the time between the last backup of data and the disaster event.

*Procedures***Continuity of Operations Plans**

The following processes are required to develop continuity of operations plans:

Risk Assessment:

Agencies will perform a risk assessment after every major change to the agency or at least every four years. The purpose of a risk assessment is to determine potential events that could adversely affect an agency, the damage such events can cause and the controls needed to prevent or minimize the impact.

Business Impact Analysis:

Agencies will perform a business impact analysis after every major change to the agency or at least every four years to set recovery priorities, recovery time objectives and recovery point objectives. The business impact analysis must:

1. Identify all time-sensitive business services, processes and functions, resources and infrastructure and assess the impact of a disruption.
2. Determine when significant consequences will result if the critical business functions, resources and infrastructure are unavailable.
3. Cover all processes, including operations that interface with other agencies, vendors, and service providers.
4. Include adequate representation from all business units.
5. Be validated and approved by agency management.

Recovery Strategy:

Agencies will participate in recovery strategy solutions centrally managed by the Office of Enterprise Technology. Agencies may have exceptions due to unique requirements (e.g. crime labs, health labs, etc.). All exceptions to this standard will be submitted to the Office of Enterprise Technology – Enterprise Security Office for review and approval.

1. Recovery strategies must be tested to ensure that they can meet the recovery time and recovery point objectives;
2. Copies of the COOP for all Commissioners, senior managers and team leaders who have designated responsibilities will be stored off site.

Plan Documentation:

For ease of understanding, portability, auditing, and geographic roll up, plan documentation must be stored and maintained in a centrally managed, secure tool (currently Living Disaster Recovery Planning System [LDRPS]). The tool must provide accessibility to necessary recovery personnel.

Plan requirements and templates will be provided for:

1. MnIMS compliant recovery team structure;
2. Crisis and incident management plans;
3. Agency policies and state policies necessary for successful implementation of the agencies COOP;
4. Procedures and information to enable the agency to respond to an incident, recover, and resume the critical processes and return to normal operations in a structured, orderly, and timely manner.
5. Continuity of operations considerations as part of any proposed material outsourcing or supply agreement with a third party service provider; and
6. Minimum requirements of:
 - a. Scope and objectives of the plan, planning assumptions and line of succession;
 - b. Procedures to enable the agency to manage the initial impact of the incident, and then recover and resume functions within the identified timeframes;
 - c. Information about the agency's alternate site for work area and IT operations;
 - d. Resources needed to run operations in the event the primary operational site, or designated other critical facility, is unavailable.

Plan Exercises and Maintenance:

Agencies must exercise and maintain their continuity of operations plan at least annually to

verify that it will work and all information is current.

1. Desk check and procedural reviews are acceptable exercise techniques. However, simulation and operational exercises must be completed annually.
2. Formally report the results of the exercise to the Office of Enterprise Technology Business Continuation Management Unit.

Awareness & Training Program:

Agencies must ensure that all employees understand their roles and responsibilities in the event of a disaster.

Forms and Instructions

Available in the LDRPS software:

- Continuity of Operations Plan Prototype
- Exercise Report Format Template

Appendices

Not Applicable