

[Insert state seal]

**STATE OF MINNESOTA
CONTINUITY OF
OPERATIONS PLAN
PROTOTYPE**

DECEMBER 31, 2003

This page is purposely left blank.

Table of Contents

Summary	4
Introduction to Plan	6
Authority of Plan	7
Scope of Plan	8
Objective of Plan	9
Business Impact Analysis Results	10
Risk Analysis Results	11
Assumptions of Plan	12
Recovery Strategies for Services	13
State Policies	15
Agency Policies	16
Recovery Timeline	17
Emergency Response Procedures	18
Statutory Compliance Procedures	19
Defined Disaster Scenarios/Threat Conditions	20
Recovery Team Structure	21
Reporting Structure	22
Team Members	23
Team Roles and Responsibilities	24
Communication Plan	25
Call Tree	26
Employee Information	27
Locations	28
Tasks	29
Recovery Procedures	30
Vendors & Responsibilities	31
Vital Records	32
Customers	33
Software	34
Equipment	35
Supplies	36
Telecommunication Requirements	37
Conclusion	38
Continuity of Operations Planning Resources	39
Glossary of Terms	40

STATE OF MINNESOTA
CONTINUITY OF OPERATIONS PLAN
PROTOTYPE

Summary

The Governor's Order Assigning Emergency Responsibilities to State Agencies (Executive Order xxxx) requires all state agencies to have a Continuity of Operations Plan. The Division of Homeland Security and Emergency Management from the Department of Public Safety awarded the Department of Administration a grant to develop a document that will assist State agencies in continuity of operations planning.

The terms Continuity of Operations Planning and Business Continuity Planning are interchangeable and describe the process of developing advance arrangements and procedures which will enable an organization to respond to an event in such a manner that the time-sensitive services of the organization continue without interruption or essential change. The Federal Department of Homeland Security currently uses the term continuity of operations. To maintain consistency with Federal documentation, it will be used throughout State of Minnesota documentation as well. Continuity of operations plans enable an agency to respond to a business interruption in an orderly, efficient manner. Business interruptions may result in declared emergencies. An emergency is defined as a sudden, unplanned, calamitous event which disables or interrupts the ability to maintain a "business as usual" environment for a period of time that adversely affects the mission of an organization and results in great damage or loss. An emergency can be either natural or man-made, but is not reliant on a Presidential or Gubernatorial disaster declaration. An emergency can be declared by the appointing authority or the Department of Employee Relations (DOER). Only DOER can authorize payment to employees for time off work as a result of an emergency.

A continuity of operations plan contains all of the information that an agency needs to recover its services in the event of an emergency. Typically a plan contains policies that govern the plan, databases of information such as employee, vendor and customer information and procedures or scripts that provide specific instructions to implement recovery of services. Plan development is an arduous process that requires the support of the Executive Management of the agency and staff dedicated to the project. The plan should be maintained through exercise and revision. Although all agency employees may have roles in the execution of the plan, smaller planning teams accomplish plan development more efficiently.

The Continuity of Operations Plan Prototype consists of three parts, the prototype itself plus two supporting documents. The prototype, contained in this document, is an outline and description of the requirements of a complete continuity of operations plan. It follows the same logical order that this information should appear in the plan. The first supporting document is the Continuity of Operations Plan State Policies. This document contains the policies that govern all state agencies and should be followed in the event of a business interruption. Agencies may need to develop their own policies to supplement the state policies or operationalize them within their agency. The second supporting document is the Continuity of Operations Plan Agency Templates. This document contains templates any agency can use to write agency-specific continuity of operations foundation documents or policies.

STATE OF MINNESOTA
CONTINUITY OF OPERATIONS PLAN
PROTOTYPE

The Continuity of Operations Plan Prototype was developed using the following philosophy:

- The prototype is intended to educate agencies on the requirements of a continuity of operations plan, provide guidance on developing the plan, facilitate the development of an agency's plan and consolidate all of the continuity of operations policies of the state.
- The continuity of operations plan is developed in phases. The response phase is the process of planning for and/or implementing the organization's reaction to an incident or emergency. The goals of this phase include the protection of life, ensuring safety and health of personnel; to limit and contain damage to facilities and equipment; to stabilize impacts of an event (operational, service and public image) and to manage and communicate information about the incident. The recovery phase is the process of planning for and/or implementing the recovery of only the most time-sensitive agency services immediately following an interruption or emergency. The resumption phase is the process of planning for and/or implementing expanded recovery operations of less time-sensitive agency services after the most time-sensitive services have been resumed. The restoration phase is the process of planning for the transition of operations from the alternate recovery locations to permanent normal facilities. This includes restoring or replacing a damaged/destroyed facility, replacing its contents and implementing the coordinated movement of personnel, equipment, communications systems and other assets to a permanent location.
- An agency uses a team approach in the recovery of its services. The overall plan is actually several plans, which combined, detail recovery for the entire agency.
- The Agency Templates can be used by an agency in a 'fill in the blank' manner or can be reviewed as examples only.
- Each component of the continuity of operations prototype falls into one of four categories: 1) Foundation document; 2) Policy; 3) Data 4) Procedures or Scripts. The category of each component is identified in this document.

The Continuity of Operations Plan Prototype was completed December XX, 2003. For assistance using it contact bcm.itg@state.mn.us.

Introduction to Plan

The Introduction to the Plan includes the reasons for which an agency has written a continuity of operations plan and the process undertaken to complete the plan.

It should include process details including the data gathering effort (for instance whether or not a Business Impact Analysis or Risk Analysis was completed), the sources of information consulted in plan development and the criteria used to prioritize the services and determine recovery time objectives.

It should identify possible emergency scenarios that an agency might face and the likelihood of those scenarios occurring.

It should identify how the plan is organized including identification and definitions of the phases the plan covers as well as the recovery teams and their responsibilities.

After reading the Introduction to the Plan, the reader should have an understanding of what the plan encompasses and how it should be used.

Category: Foundation Document

Sample Introduction to Plan included in Continuity of Operations Plan Agency Templates.

Authority of Plan

The continuity of operations plan should clearly identify under what circumstances it should be activated and what authority the recovery teams have to act. The recovery teams and positions in a continuity of operations plan may not necessarily align with the organizational structure of an agency. For this reason, the plan should clearly identify when and how the plan structure assumes authority over the agency's organization structure and in what areas this occurs. This delegation of authority must be planned and identified in the plan to allow for smooth execution of the plan and an efficient recovery.

This component identifies the authority of the continuity of operations plan. Individual authority of the teams and the chain of command is documented in the Reporting Structures component.

Category: Foundation Document

Sample Authority of Plan included in Continuity of Operations Plan Agency Templates.

Scope of Plan

The scope of the plan identifies the limitations of the plan and provides focus for the planning effort. It identifies the services that are covered by the plan and those that are not. The plan's scope should encompass all time-sensitive services and processes (those addressed in the response, recovery and resumption phases). However it may also include all of the services and processes of the agency (those addressed in the restoration phase). If this is the case, it is critical to plan for the time-sensitive services and processes first!

The plan should be developed based on "Worst Case Scenario", which implies the inaccessibility or unavailability of an agency's facility and all of its contents. The definition of "Worst Case Scenario" should be included in the scope.

Category: Foundation Document

Sample Plan Scope included in Continuity of Operations Plan Agency Templates.



STATE OF MINNESOTA
CONTINUITY OF OPERATIONS PLAN
PROTOTYPE

Objective of Plan

The objective of the plan identifies the specific intention of the continuity of operations plan. That is, what the agency hopes to accomplish by developing and activating the plan. It should include brief statements that address specific components of the agency's purpose, goal, or mission.

The objective of the plan should include a statement describing the approach the agency is taking to accomplish the identified objectives.

Category: Foundation Document

Sample Plan Objectives included in Continuity of Operations Plan Agency Templates.

Business Impact Analysis Results

A continuity of operations plan should be written to recover the time-sensitive services of an agency. The best way to determine which of the many services of an agency are time-sensitive is to complete a business impact analysis (BIA). The BIA identifies the services and process of the agency, the recovery time objective for restoring each service in the event of a business interruption and the resources that each service needs for recovery. Because the services of an agency and the methods of providing those services change frequently, conduct a complete BIA every four years and review the information every two years.

Include the results of the BIA in the plan. Identify when the BIA was completed and by whom, identify the criteria used for determining the recovery time objectives for the services, document the review schedule of BIA results and assign responsibility for reviewing and conducting BIA's.

Category: Foundation Document

Risk Analysis Results

While a Business Impact Analysis (BIA) identifies the time-sensitive services of an agency and their recovery time objectives, a Risk Analysis identifies the threats that an agency may face due to its geographic location, physical environment, economic conditions or political atmosphere and the risks associated with those threats. The findings of a risk analysis provide management with information to make decisions. Funding to mitigate risks is often limited, so it is important to designate financial resources to address the most probable threats with the highest associated risks.

Include the results of the Risk Analysis in the plan, including which risks were assumed, transferred or mitigated and the controls put in place to mitigate the risks. Identify when the risk analysis was completed and by whom, identify the criteria used for ranking the risks, document the review schedule of risk analysis results and assign responsibility for reviewing and conducting future risk analyses.

Category: Foundation Document

Assumptions of Plan

The continuity of operations plan should be developed based on some basic assumptions, statements accepted to be true in the event of an emergency. This eliminates the need to develop several recovery plans, that is, one plan for fire, one plan for flood, and one plan for explosion. The plan should be written to cover any interruption, regardless of the type, that would affect operations for 30 days or more.

The assumptions should be basic. For example,

- Only one agency building will be affected at one time.
- Vendors will meet contractual obligations.

All of the assumptions used when developing the plan should be documented in the plan. This provides context for the decisions that were made in plan development.

Assumptions not realized are risks. If then, using the example assumptions above, more than one agency building is affected during an incident, the effectiveness of the plan is at risk. The same is true if vendors do not meet contractual obligations during a declared emergency. After plan assumptions are documented, the resulting risks should be reviewed in a risk analysis to ensure that the risks are acceptable and the assumptions are sound.

Category: Foundation Document

Sample Plan Assumptions included in Continuity of Operations Plan Agency Templates.

Recovery Strategies for Services

Recovery strategies are the formation of a vision and direction for continuity of operations planning so that an agency can achieve the purpose set forth by the legislature and protect agency assets in the event of a business interruption. An agency's assets include its services, employees, tangible and intellectual property, and information resources.

Recovery strategies are the alternate operations and data protection used to continue or to recover an agency's time-sensitive services. Recovery strategies must integrate personnel requirements, business operations, information security practices and information technology.

There are two continuity of operations models:

1. Alternate Site Model

This traditional model is based on identifying a recovery location for each primary site. This includes recovery locations for both data processing environments and business operations. The model relies upon relocating personnel and maintaining backup copies of data and redundant technology off-site. This model requires periodically exercising the ability of the alternate location to recover and function as the primary site for delivery of the organization's services for an identified period of time.

The Department of Administration's Real Estate Management unit offers assistance to any State agency looking for alternate sites. Agency continuity of operations plans should identify and document alternate sites for all time-sensitive services.

2. Split Operations Model

This emerging model relies on two or more geographically separated operational sites for an agency's time-sensitive services. This model requires that the capacity at each location be sufficient to accommodate the loss of the other site.

The Department of Administration's InterTechnologies Group offers co-location services that suit this model.

The methods, tools and techniques used to develop an agency's recovery strategies include:

- Business Impact Analysis
- Risk Analysis
- Cost/Benefit Analysis
- PEST Analysis (Political/Environmental/Social/Technical)
- SWOT Analysis (Strength/Weaknesses/Opportunities/Threats)
- Strategic Planning Process Model

STATE OF MINNESOTA
CONTINUITY OF OPERATIONS PLAN
PROTOTYPE

All strategies must be reviewed on an ongoing basis. The frequency of this review is dependent on the dynamics of the changes within the agency. At a minimum, best practices advise reviewing recovery strategies with every change of administration.

The strategic planning team that is assigned to identify and develop recovery strategies for an agency should include representatives from the following groups:

- Agency Attorney General Counsel
- Business Continuity
- Finance
- Facilities
- Human Resources
- Audit
- Service Area Supervisors
- Real Estate Management
- Risk Management (Insurance)
- Telecommunications
- Platform Technical Experts
- Service Experts (where appropriate)

Management support is crucial. Complete and present a cost/benefit analysis to the agency's Executive Management for final approval and funding to obtain this support. Document and present the selected recovery strategies to the Commissioner for his/her signature before fully implementing the selected strategies.

Category: Foundation Document

Sample Recovery Strategy included in Continuity of Operations Plan Agency Templates.



STATE OF MINNESOTA
CONTINUITY OF OPERATIONS PLAN
PROTOTYPE

State Policies

The following policies have been adopted by various governing agencies. These policies must be followed by every State of Minnesota agency and should be included in all continuity of operations plans. The policies can be found in the supporting document, the Continuity of Operations Plan State Policies.

List in the same order and by same name as in other doc. Include page number

Category: Policy

Agency Policies

Each agency should document any policies it has developed specific to its continuity of operations plan and should include them in the plan. These policies govern the execution of the plan and are a critical piece of the plan. These policies may include but are not limited to communication, human resources, plan exercise and maintenance, plan activation and emergency declaration. The agency's Executive Management should approve each policy.

Sample agency policies can be found in the supporting document, the Continuity of Operations Plan Sample Agency Templates. These provide an example of the content that should be included in the agency policies and can be modified for agency use. Although this is a broad list of policies, it is not all encompassing. There may be other policies that should be adopted by your agency.

The policies provided are:

List in the same order and by same name as in other doc. Include page number.

Category: Policy

Recovery Timeline

The recovery timeline is the foundation of a continuity of operations plan. It is a visual representation of all of the services of the agency and identifies chronologically the order in which they will be recovered. From the moment of the business interruption (incident), the timeline identifies what decisions should be made and at what point in time services, support services and technology should be recovered.

The recovery timeline is originally created at the completion of the business impact analysis, but it is a living document. It is changed perhaps more than any other portion of the continuity of operations plan. It should be reviewed and updated whenever recovery strategies change, services are added or removed, technology changes, support service business operations change or decision timeframes change.

If followed, the recovery timeline facilitates an orderly recovery of services.

Category: Foundation Document

Sample Recovery Timeline included in Continuity of Operations Plan Agency Templates.

Emergency Response Procedures

One of the keys to managing a business interruption is an agency's response to the initial incident. An agency's orderly response to a disruptive event saves agency assets and sets the tone for the recovery. An agency's most important asset is its employee. The safety and protection of those employees should be the agency's top priority. For that reason the emergency response procedures of the agency are critical and should be included in the continuity of operations plan. The emergency response procedures should include, but are not limited to:

- A building evacuation plan
- Identified relocation areas
- Response procedures for bomb threats
- Response procedures for fire
- Response procedures for medical emergencies
- Response procedures for civil disturbances
- Response procedures for gas leaks
- Response procedures for severe weather
- Response procedures for power outages
- Communication plan for senior management
- Communication plan for employees and family

All employees of an agency should be trained on the procedures at least annually and the emergency response procedures should be tested twice a year.

Category: Procedures or Scripts

Statutory Compliance Procedures

It is the responsibility of each State agency to know and understand any state statute, federal law or other regulation by which it is governed and to which it is accountable. These regulations may require an agency to provide services within a specific timeframe without regard to a declared emergency or conduct certain functions in the event of a community wide emergency.

The Governor's Order Assigning Emergency Responsibilities to State Agencies (Executive Order **xxxx**), is one such regulation. It assigns specific responsibilities to agencies, which they must fulfill in the event of emergencies. The Minnesota Emergency Operations Plan details these responsibilities. An agency receiving federal funding to provide services may have specific requirements that should be included in its continuity of operations plan.

It is the responsibility of each State agency to understand all of the requirements placed upon it, develop a plan to respond to those requirements and include them in its continuity of operations plan.

Category: Foundation Document and Procedures or Scripts

Sample included in Continuity of Operations Plan Agency Templates. ???

Defined Disaster Scenarios/Threat Conditions

The U.S. Department of Homeland Security has an advisory system that categorizes threat conditions for the United States. It identifies five threat conditions each representing an increased risk of terrorist attack. The threat conditions are: Green (Low), Blue (Guarded), Yellow (Elevated), Orange (High) and Red (Severe). Information regarding the Homeland Security Advisory System can be found at www.dhs.gov.

Minnesota State Agencies may be required by law to perform certain activities at some or all of the threat conditions. A continuity of operations plan should refer to these threat conditions and identify the responsibilities of the agency at each of these levels. The agency's executive management may refer to the threat conditions when assessing an incident to determine whether or not to activate the plan or declare an emergency.

Category: Foundation Document and Procedures or Scripts

Recovery Team Structure

A continuity of operations plan for an agency should be broken into many plans all of which combined make up the agency plan. This is done for ease of development and execution. There will be overall agency teams, that is, teams that support the entire agency and individual recovery teams each with a specific responsibility.

Examples of overall agency teams are: the Emergency Management Team (responsible for declaring an emergency, approving recovery strategies, human resource issues, crisis management, media communication), the Business Continuation Management Team (responsible for site coordination, recovery team communication, team activation), the Support Services Team (responsible for logistics, procurement, administrative support), the Customer and Family Relations Team (responsible for communicating with customers and family members) and the Facilities Team (responsible for damage assessment, salvage and restoration).

Examples of individual recovery teams are: Technology Teams (responsible for recovery of specific technology – there can be more than one technology team), Business Process Teams (responsible for recovery of agency services).

Each recovery team is activated in the appropriate phase of recovery to suit its purpose and meet its objective. The response phase begins at the time of an incident and ends when an emergency is declared. Typically the Emergency Management Team, Business Continuation Management Team and Facilities Team are activated in the response phase. The Support Services Team and Customer and Family Relations Team may also be activated in the response phase. The recovery phase begins once an emergency is declared and ends when technology has been recovered. Technology teams are activated in this phase. The Support Services Team and Customer and Family Relations Team may also be activated in the recovery phase. The resumption phase begins after technology and the most time sensitive services have been recovered and ends when the agency begins moving to its permanent location (either the restored former location or a new location). The Business Process Teams are activated in this phase. The restoration phase begins when the agency moves to its permanent location and ends when business as usual has been restored. All teams are active in this phase.

Recovery teams should be identified at the beginning of the planning process. Each team's purpose, objective and responsibility as well as the phase in which it is activated should be documented in the plan.

Category: Foundation Document

Sample Recovery Team Structure included in Continuity of Operations Plan Agency Templates.

Reporting Structure

The recovery teams and positions in a continuity of operations plan may not necessarily align with the organizational structure of an agency. When an emergency is declared the continuity of operations plan takes affect and it assumes the authority it has been designated by Executive Management. It is important for the efficient activation of the plan, that any changes to the normal reporting structure be clearly identified in the plan and all affected employees understand the changes.

Identify and document in the plan the reporting structure that should be followed during a declared emergency. Identify which position has what authority and identify primary and backup person for each position.

Category: Foundation Document

Sample Reporting Structure included in Continuity of Operations Plan Agency Templates.

Team Members

Document, by team, the positions on each team and the employees who fill those positions. Depending on the complexity of the team, the position titles will vary from specific (e.g., 555 Main Street Site Coordinator) to general (e.g., First Shift Team Member). At a minimum, each team should have a Team Leader and Team Member position. Each position should have at least two employees assigned to it – one being the primary, the other being the alternate. However each agency should determine how many levels of depth it wants for each position to mitigate the risk that personnel may not be available. For some agencies two levels may not be enough.

Category: Data

Team Roles and Responsibilities

This area of the continuity of operations plan documents the purpose, objective and responsibility of each team identified in the reporting structure. As with so many aspects of the continuity of operations plan, activation of the plan and recovery from the emergency is more efficient if this information is determined and documented before an incident occurs. Document in clear, simple language the role of each team and the responsibilities each has. Identify each team's decision-making authority and any exceptions to that authority.

Category: Data and Procedures or Scripts

Examples of team roles and responsibilities can be found in the sample Reporting Structure document included in Continuity of Operations Plan Agency Templates.

Communication Plan

The communication plan details the way each recovery team will share information in the event of a business interruption or declared emergency. The plan should be robust and identify several depths of communication in the event the standard method is unavailable. For instance, in a community-wide emergency normal telephone communications may be overloaded. In this event, it is important to have cellular phones, two-way radios and satellite phones as backups. In an emergency all staff may not be able to gather in the same physical location. In that event it is important to have audio conferencing capabilities available.

Each continuity of operations team has a different recipient with whom it needs to share information concerning the emergency. Internal recovery teams need to share information with each other, whereas the emergency management and business continuation management teams may need to share information outside of the agency. Each audience should not receive the same message, so the communication plan should take all of those audiences into consideration. For instance, the public and media should not receive the same detailed information that the agency's recovery team personnel require. Information about the emergency should be provided following the communication plan. Only authorized persons should provide information to media and public. This message should be truthful, clear and concise.

Category: Foundation Document and Procedures or Scripts

Sample Communication Plan included in Continuity of Operations Plan Agency Templates.

Call Tree

The call tree is a critical piece of an agency communication plan. It details who calls whom in the event of an emergency. It identifies who activates the call tree and provides all contact information for each person on the call tree. Someone outside of the agency, for instance building management or building security, may initiate the call tree. The plan should include their contact information and they should be provided with a copy of all necessary documentation.

Procedures should be established to determine what to do if someone cannot be reached. For example, set a time limit to wait for return calls from pages, determine how to verify that everyone has been contacted, establish how to keep the call tree moving if someone is not available.

Call trees can be automated using several systems currently available on the market. If the call tree is automated, include procedures for initiating the call tree in the continuity of operations plan. Identify who is responsible for maintaining the system. Include maintenance procedures in the continuity of operations plan. Make sure that the system is located away from your primary location. Communication is key to a smooth recovery -- make sure there is an adequate recovery strategy in place for the automated system.

Test the call tree, whether manual or automated at least twice a year.

Category: Procedures or Scripts

Employee Information

Employee information is possibly the most fluid of all information in a continuity of operations plan and the most cumbersome to maintain. Include the following information for each employee included in the agency's recovery teams. If not all employees are assigned to a recovery team, gather and document the same information for those employees so that it is available in the event of an emergency.

- Name
- Address
- Phone Numbers (home, office, cellular, pager)
- Emergency Contact (name, address, phone, work shift)
- Email address
- Primary work schedule
- Security level

Employees are not legally required to provide this data. However, if this information is not available, the agency should not rely on the individual to perform a role in the recovery of its services and should delegate those responsibilities to another employee or consultant who is willing to provide the data. Ask each employee to complete a release when they provide the data that gives a member of the Business Continuation Team permission to contact them in the event of an emergency via any of the contact numbers they provided.

Category: Data

Locations

If an emergency is declared and the continuity of operations plan is activated, recovery teams may be dispatched to alternate recovery locations. An agency may have alternate recovery locations, off-site storage locations and/or off-site gathering locations.

Document the addresses (physical and mailing) of all of these locations in the plan and identify which team reports to each location. Include maps and directions to, security procedures for, as well as a contact at and telephone and fax numbers of the alternate locations in the plan.

Many agencies have more than one physical location. The addresses (physical and mailing) and telephone and fax numbers of all current agency locations should also be documented in the plan.

It is the responsibility of the Business Continuation Management team to ensure that no alternate location is 'overbooked' at the time of an emergency. It is this team's responsibility to know the alternate locations for each recovery team and identify when conflicts for space arise and resolve any issues.

Category: Data

Tasks

Any task that a recovery team should perform in the event of an emergency should be documented in the plan. The tasks can be detailed, such as

- *Report to recovery facility.*
- *Initiate conference call with team members by dialing 800-555-3333, passcode 98999.*
- *Provide update to Emergency Management Team coordinator.*

Or the tasks can refer to procedures included in the plan, such as

- *Update information box. See procedures in Appendix A of plan.*
- *Complete status update. See instructions and form in Appendix B of plan.*

Identify which tasks have dependencies on other tasks in the plan, which position is responsible for completing the task and establish a way of communicating the status of in progress or completed tasks.

Category: Data or Recovery Procedures or Script

Recovery Procedures

Each team should document any procedures or scripts it uses to recover its technology or service. These procedures or scripts should be written so that any person with the same general knowledge could follow them and complete the recovery. For example, a server recovery script should be written so that any LAN administrator (not necessarily from the same agency) could follow them and successfully recover the server. It is not necessary to write them in such detail that a marketing executive could recover the server.

The procedures or scripts should not refer to documentation or information that is not included in the plan. If it refers to a manual, the manual must be stored off-site with the procedure.

The procedures or scripts should be included in the plan and reviewed, tested and updated twice a year. An excellent way to test the procedures or scripts is to have team members who did not participate in developing the scripts, use the procedure or script to perform the recovery. This will find the errors or gaps.

Category: Procedures or Scripts

Vendors & Responsibilities

Most agencies have agreements with vendors for goods or services. These vendors should be contacted in the event of a business interruption or emergency declaration by the agency. Some of these vendors may have contractual obligations to fulfill to assist the agency in recovering from the emergency. Others need to be notified of the emergency and the new operating procedures.

Document in the continuity of operations plan all of the vendors with whom the agency has a relationship. Identify the service or product they provide. Identify the vendor representative who should be contacted in the event of an emergency and who from the agency is responsible for contacting him/her. Identify the responsibility the vendor has to assist in recovery and include copies of the contracts or agreements the agency has with them. Identify the recovery priority the agency has in the event of a community-wide or multiple agency event (i.e. if multiple agencies or businesses are without power, what priority does the agency have for restoration of power).

Identify which, if any, vendors are a sole-source provider of goods or services to the agency. Verify that the recovery strategy for this good or service is adequate.

Category: Data

Sample Vendor Responsibility document included in Continuity of Operations Plan Agency Templates.

Vital Records

Vital records are any document, manual, or form that is required for the recovery of a service. Examples of vital records are warrant stock, letterhead, software manuals, phone lists, stamps, or contracts. Each recovery team should identify the vital records it needs for recovery, store a copy or an extra supply off-site from the primary location and document the vital record and its off-site storage location in the plan.

Category: Data

Customers

Every recovery team should identify any customers that should be notified of an agency emergency declaration by the agency and the subsequent recovery effort. Examples of customers are citizens, private businesses, state agencies, county government, city government, schools and non-profit organizations.

A list of these customers and their contact information should be included in the plan. The communication plan should cover who from the agency should contact the customers, when they should be contacted and how contact should be made. Remember that normal communication lines may not be available (i.e. e-mail and e-mail lists), so alternate communication methods should be included in the plan.

Category: Data

STATE OF MINNESOTA
CONTINUITY OF OPERATIONS PLAN
PROTOTYPE

Software

Each recovery team should identify all of the software it needs for recovery. Even if an agency has standards for software, there may be exceptions throughout the organization and there should be no assumptions made about the software required for recovery. Document in the continuity of operations plan the software required, include the following information:

- Software description
- Level and release
- License number
- Quantity required
- Platform on which it resides
- Space required
- If it's dependent on equipment serial number
- Vendor from whom replacement is available (note: vendor information should be included in vendor list)

Store copies of the software off-site at a location that is accessible 7 x 24 and document the location in the plan.

Category: Data

Equipment

The continuity of operations plan should include two lists of equipment. The first is the inventory of all equipment owned by the agency listed by location. This will be beneficial when doing a damage assessment of the affected facility and for completing insurance claims.

The second is a list of all equipment required at alternate locations to complete recovery. This includes pc's, terminals, printers, fax machines, copiers, general furniture, servers and other technology platforms, telephones, cell phones and special equipment.

Include the following information about the equipment if applicable:

- Description
- Quantity required
- Location of spare equipment, if any
- Insurance coverage, if any
- Vendor from whom replacement is available (note: vendor information should be included in vendor list)
- Model Number
- Serial Number
- Device Address
- Footprint & weight
- Cooling requirements
- Power consumption rate
- Peripherals normally included
- Connection type

Category: Data

Supplies

In the event of an emergency declaration and plan activation, recovery teams will be dispatched to alternate recovery locations. The supplies located at the primary sites, normally taken for granted, will not be available. Therefore it is important that all supplies required for recovery are documented in the plan and available at an off-site storage location for immediate access. The easiest way to plan for supplies is to identify at the beginning of plan development a general supply kit that every recovery team may need and document it in the Support Services Recovery Team plan. The other recovery teams can document in their plans the number of supply kits they require and at what time and any additional supplies they need.

An example of the contents of a general supply kit is:

- 12 Pens
- 12 Pencils
- 12 Lined Notepads
- 1 box 3.5" floppy disk
- 12 CD RW
- 4 staplers
- 1 box of staples
- 4 rolls of scotch tape and dispenser
- 1 box file folders
- 4 scissors
- 12 yellow highlighter
- 1 box 9 1/2 x 12" manila envelopes
- 24 blank timesheets
- 24 vacation/sick leave request forms
- 12 agency business cards (no person or position)
- 12 3x3 post it notes

Category: Data

Telecommunication Requirements

Telecommunication requirements are a critical, yet often overlooked requirement of a continuity of operations plan. Telecommunication requirements include:

- Voice lines
- Voice mail systems
- Interactive Voice Response systems
- Enhanced Call Programs
- Cellular phones
- Wide Area Network components
- Local Area Network components
- Data circuits

The continuity of operations plan should have all of these requirements documented, including network diagrams, circuit id's, equipment inventories and vendor contracts. Each recovery team should identify its own telecommunications requirements, but one technology team (often a Network Recovery Team) should be responsible for recovery of the telecommunication network.

Category: Data

Conclusion

Depending on the size and complexity of the agency, the plan development process can take anywhere from 9 months to three years. When staff is dedicated to the project, the plan development process takes much less time. If staff cannot be dedicated to the project, it could take more than three years to develop a complete continuity of operations plan.

The plan can be created using word processing software or software developed specifically for continuity of operations planning. Regardless of how it is compiled, each team member should have a copy of the plan stored at their home and should carry a copy of the call tree with him/her at all times. An agency should determine its own distribution and retrieval policy, so that team members always have the current version of the plan and that old versions of the plan are destroyed.

This Continuity of Operations Plan Prototype was completed through the collaboration of the Department of Public Safety and the Department of Administration. Funding was made possible through a grant from the Federal Emergency Management Administration. The following are the individuals responsible for the successful completion of the project.

Project Sponsor:

Brian Lamb, Commissioner, Department of Administration

Project Manager:

Debra Stafford, Department of Administration, InterTechnologies Group

Project Administrator:

Tom Chukel, Department of Administration, Risk Management Division

Business Continuity Analysts:

Denise Arel, Department of Administration, InterTechnologies Group

Lisa Belland, Department of Administration, InterTechnologies Group

Siri Johnson, Department of Administration, InterTechnologies Group

Kathy Matter, Department of Administration, InterTechnologies Group

Emergency Management Consultant:

Sharon Smith, Department of Public Safety, Homeland Security Emergency Management

Project Advisors:

Terri Smith, Department of Public Safety, Homeland Security Emergency Management

John Kerr, Department of Public Safety, Homeland Security Emergency Management

Review Team:

Donna Baker, Department of Revenue

Don Beckering, Minnesota State Colleges and Universities

JoAnn Champagne,

Jeff Davidman, Governor's Office

Susan Estes, Department of Administration

Jean Henning, Department of Finance

Beverly Kroiss,

Debra Teske,



STATE OF MINNESOTA
CONTINUITY OF OPERATIONS PLAN
PROTOTYPE

Continuity of Operations Planning Resources

This section will contain a list of resource information for users.

Glossary of Terms

Alert

Notification that a possible emergency situation has occurred. Stand by for possible activation of recovery plan.

Alternate Site

A location, other than normal facility, used to process data and/or conduct critical business functions in the event of a disaster. SIMILAR TERMS: Alternate Location, Alternate Processing Facility, Alternate Office Facility, Alternate Communication Facility, Recovery Center.

Application Recovery

The component of disaster recovery that deals specifically with the recovery of business system software and data, occurs after the processing platform has been restored or replaced. SIMILAR TERMS: Business System Recovery

Assumptions

Basic understanding about unknown emergency situations on which the business continuity plan is based.

Business Continuation

A program covering disaster recovery and business resumption planning as well as prevention. See also disaster recovery planning, continuity of operations planning and business resumption planning.

Business Continuation Planning

The process of documenting prevention measures, disaster recovery, business resumption and restoration plans. SIMILAR TERMS: Business Continuity Planning, Business Resumption Planning, Continuity of Operations Planning and Disaster Recovery Planning.

Business Impact Analysis

The process of analyzing an organization's business and the effect that an emergency may have upon them.

Business Interruption

Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations.

Business Interruption Costs

The costs or unrecoverable lost revenues associated with an interruption in normal business operations.

Business Recovery Critical Path

The order in which recovery processes are executed during a recovery effort. There are major milestones along the path, which are followed regardless of the organization.

Business Resumption Planning

The documenting of procedures and resources to continue time-sensitive business functions at an alternate location. SIMILAR TERMS: Business Continuation Planning, Continuity of Operations Planning.

Business Unit Recovery

The component of a business continuation plan which deals specifically with the relocation of key personnel in the event of a disaster and the provision of essential resources in order to perform their time-sensitive functions.

Checklist Test

A method used to test completed recovery and resumption plans. This test is used to determine if the information such as phone numbers, manuals, equipment, etc. in the plan is accurately documented and current.

Cold Site

An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed in such a facility to duplicate the critical business functions of an organization. Cold-sites have many variations depending on their communication facilities, UPS systems or mobility. SIMILAR TERMS: Shell-site

Command Center

A centrally located facility having adequate phone lines to begin recovery communications. Typically it is a temporary facility used by the management team to begin coordinating the recovery process and used until the alternate sites are functional. Also, referred to as Incident Command Center or Control Site.

Contingency Plan

See Business Continuation

Continuity of Operations Planning

The process of documenting prevention measures, disaster recovery, business resumption and restoration plans. Term used by US Federal Government for Business Continuation Planning. SIMILAR TERMS: Business Continuity Planning, Business Resumption Planning and Disaster Recovery Planning.

Cooperative Hot-Sites

A hot-site owned by a group of organizations available to a group member should a disaster strike. See Hot-Site.

Crate & Ship

A strategy for providing alternate processing capability in a disaster, via a contractual arrangement with an equipment supplier to ship replacement hardware within a specific time period. SIMILAR TERMS: Drop Ship

Crisis

A critical event, which if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation or ability to operate.

Crisis Management

The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

Damage Assessment

The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc. and determining what can be salvaged or restored and what must be replaced.

Data Center Recovery

The component of Disaster Recovery which deals with the restoration, at an alternate location, of data center services and computer processing capabilities. SIMILAR TERMS: Mainframe Recovery.

Dedicated Line

A pre-established point to point communication link between computer terminals and a computer processor, or between distributed processors, that does not require dial-up access.

Declaration Fee

A one-time fee, charged by an Alternate Facility provider, to a customer who declares a disaster. SIMILAR TERMS: Notification Fee. NOTE: Some recovery vendors apply the declaration fee against the first few days of recovery.

Dial Backup

The use of dial-up communication lines as a backup to dedicated lines.

Dial-Up Line

A communication link between computer terminals and a computer processor, which is established on demand by dialing a specific telephone number.

Disaster

Any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time. SIMILAR TERMS: Business Interruption; Outage; Catastrophe; Emergency.

Disaster Prevention

Measures employed to prevent, detect, or contain incidents which, if unchecked, could result in disaster.

Disaster Prevention Checklist

A questionnaire used to assess preventative measures in areas of operations such as overall security, software, data files, data entry reports, microcomputers, and personnel.

Disaster Recovery

The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.

Recovery Time Objective

The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.

Disaster Recovery Plan

The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.

Disaster Recovery Planning

The technological aspect of business continuity planning. The advance planning and preparations that are necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster. SIMILAR TERMS: Contingency planning; business resumption planning; corporate contingency planning; business interruption planning; disaster preparedness.

Distributed Processing

Use of computers at various locations, typically interconnected via communication links for the purpose of data access and/or transfer.

Electronic Vaulting

Transfer of data to an offsite storage facility via a communication link rather than via portable media. Typically used for batch/journaled updates to critical files to supplement full backups taken periodically.

Emergency

A sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property.

Emergency Preparedness

The discipline that ensures an organization, or community's readiness to respond to an emergency in a coordinated, timely, and effective manner.

Emergency Response Procedures

A plan of action to commence immediately to prevent the loss of life and minimize injury and property damage.

Extra Expense Coverage

Insurance coverage for disaster-related expenses, which may be incurred until operations are fully recovered after a disaster.

File Server

The central repository of shared files and applications in a computer network (LAN). SIMILAR TERMS: LAN (Local Area Network)

Forward Recovery

The process of recovering a data base to the point of failure by applying active journal or log data to the current backup files of the data base.

Full Recovery Test

An exercise in which all recovery procedures and strategies are tested (as opposed to a Partial Recovery Test.)

Hot-Site

An alternate facility that has the equipment and resources to recover the business functions affected by the occurrence of a disaster. Hot-sites may vary in type of facilities offered (such as data processing, communication, or any other critical business functions needing duplication). Location and size of the hot-site will be proportional to the equipment and resources needed. SIMILAR TERMS: Backup site; Recovery site; Recovery Center; Alternate processing site.

Human Threats

Possible disruptions in operations resulting from human actions (i.e., unhappy employee, terrorism, etc.).

Internal Hot-Sites

A fully equipped alternate processing site owned and operated by the organization. SIMILAR TERMS: Cooperative Hot-sites

LAN (Local Area Network)

Computing equipment, in close proximity to each other, connected to a server which houses software that can be access by the users. This method does not utilize a public carrier.

LAN Recovery

The component of Disaster Recovery which deals specifically with the replacement of LAN equipment in the event of a disaster, and the restoration of essential data and software.

SIMILAR TERMS: Client/Server Recovery

Leased Line

Usually synonymous with dedicated line.

Line Rerouting

A service offered by many regional telephone companies allowing the computer center to quickly reroute the network of dedicated lines to a backup site.

Line Voltage Regulators

Also known as surge protectors. These protectors/regulators distribute electricity evenly.

Loss

The unrecoverable business resources that are redirected or removed as a result of a disaster. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.

Loss Reduction

The technique of instituting mechanisms to lessen the exposure to a particular risk. Loss reduction is intended to react to an event and limit its effect. Examples of Loss Reduction include sprinkler systems, insurance policies, and evacuation procedures.

MICR Equipment (Magnetic Ink Character Reader)

Equipment used to imprint machine readable code. Generally, financial institutions use this equipment to prepare paper data for processing, encoding (imprinting) items such as routing and transit numbers, account numbers and dollar amounts.

Mobile Hot-Site

A large trailer containing backup equipment and peripheral devices delivered to the scene of the disaster. It is then hooked up to existing communication lines.

Natural Threats

Events caused by nature causing disruptions to an organization.

Node

The name used to designate a part of a network. This may be used to describe one of the links in the network, or a type of link in the network (for example, Host Node or Intercept Node).

STATE OF MINNESOTA
CONTINUITY OF OPERATIONS PLAN
PROTOTYPE

Nonessential Function

Business activities or information which could be interrupted or unavailable indefinitely without significantly jeopardizing critical functions of an organization.

Nonessential Records

Records or documents which, if irretrievably lost or damaged, will not materially impair the organization's ability to conduct business.

Off-Host Processing

A backup mode of operation in which processing can continue throughout a network despite loss of communication with the mainframe computer.

Off-Line Processing

A backup mode of operation in which processing can continue manually or in batch mode if the on-line systems are unavailable.

Off-Site Storage Facility

A secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored.

On-Line Systems

An interactive computer system supporting users over a network of computer terminals.

Operating Software

A type of system software supervising and directing all of the other software components plus the computer hardware. SIMILAR TERMS: Operating System

Parallel Test

A test of recovery procedures in which the objective is to parallel an actual business cycle.

Peripheral Equipment

Devices connected to a computer processor which perform such auxiliary functions as communications, data storage, printing, etc.

Physical Safeguards

Physical measures taken to prevent a disaster, such as fire suppression systems, alarm systems, power backup and conditioning systems, access control systems, etc.

Plan Activation

The time at which all or a portion of the business continuation plan has been put into motion.

Platforms

Hardware or software architecture of a particular model or family of computers (i.e., IBM, Tandem, HP, etc.)

Portable Shell

An environmentally protected and readied structure that can be transported to a disaster site so equipment can be obtained and installed near the original location.

Procedural Safeguards

Procedural measures taken to prevent a disaster, such as safety inspections, fire drills, security awareness programs, records retention programs, etc.

Reciprocal Agreement

An agreement between two organizations with compatible computer configurations allowing either organization to utilize the other's excess processing capacity in the event of a disaster.

Record Retention

Storing historical documentation for a set period of time, usually mandated by state and federal law or the Internal Revenue Service.

Recovery Strategy

The method selected to recover the critical business functions following a disaster. In data processing, some possible alternatives would be manual processing, use of service bureaus, or a backup site (hot or cold-site). A recovery alternative is usually selected following either a Risk Analysis, Business Impact Analysis, or both. *SIMILAR TERMS:* Backup alternative and Recovery Alternative.

Recovery Capability

This defines all of the components necessary to perform recovery. These components can include a plan, an alternate site, change control process, network rerouting and others.

Recovery Point Objective (RPO)

The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data projection strategy is developed.

Recovery Time Objective

The period from the time of disaster declaration to the recovery of the organizations time-sensitive functions.

Remote Site

An alternate processing site that is equipped to provide recovery to a hot-site that is not located in the same geographical location. Also, referred to as local site.

Risk Assessment/Analysis

The process of identifying and minimizing the exposures to certain threats that an organization may experience. *SIMILAR TERMS:* Risk assessment; impact assessment; corporate loss analysis; risk identification; exposure analysis; exposure assessment.

Salvage & Restoration

The process of reclaiming or refurbishing computer hardware, vital records, office facilities, etc. following a disaster.

Salvage Procedures

Specified procedures to be activated if equipment or a facility should suffer any destruction.

Sample Plan

A generic disaster recovery plan that can be tailored to fit a particular organization.

Scope

Predefined areas of operation for which a disaster recovery plan is developed.

Service Bureau (Center)

A data processing utility that provides processing capability, normally for specialized processing, such as payroll.

Shadow File Processing

An approach to data backup in which real-time duplicates of critical files are maintained at a remote processing site. SIMILAR TERMS: Remote Mirroring

Simulation Test

A test of recovery procedures under conditions approximating a specific disaster scenario. This may involve designated units of the organization actually ceasing normal operations while exercising their procedures.

Skills Inventory

A listing of employees which lists their skills that apply to recovery.

Stand-Alone Processing

Processing, typically on a PC or mid-range computer, which does not require any communication link with a mainframe or other processor.

Structured Walk-Through Test

Team members walk through the plan to identify and correct weaknesses.

Technical Threats

A disaster-causing event that may occur regardless of any human elements.

Temporary Operating Procedures

Predetermined procedures which streamline operations while maintaining an acceptable level of control and auditability during a disaster situation. SIMILAR TERMS: User Contingency Procedures

Test Plan

The recovery plans and procedures that are used in a systems test to ensure viability. A test plan is designed to exercise specific action tasks and procedures that would be encountered in a real disaster.

Time-Sensitive Functions

Business activities or information which could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization. SIMILAR TERMS: Critical Functions.

User Contingency Procedures

Manual procedures to be implemented during a computer system outage. SIMILAR TERMS: Temporary Operating Procedures.

Vital Records

Records or documents, for legal, regulatory, or operational reasons, which if damaged or destroyed would impair the organization's ability to conduct business and/or require replacement or recreation at considerable expense. SIMILAR TERMS: Critical Records, Useful Records

Voice Recovery

The restoration of an organization's voice communications system.

WAN –Wide Area Network

Like a LAN, except that parts of a WAN are geographically dispersed, possibly in different cities or even on different continents. Public carriers like the telephone company are included in most WANs; a very large one might have its own satellite stations or microwave towers.

Warm Site

An alternate processing site which is only partially equipped (as compared to Hot Site which is fully equipped).