Nebraska Public Service Commission

Public Safety Answering Point
Continuity of Operations
Planning Guide

July 2021

OVERVIEW

This Continuity of Operations (COOP) Planning Guide is intended to serve as an outline to assist Nebraska 911 Public Safety Answering Point (PSAP) and Emergency Communications Center (ECC) managers in the preparation of a COOP plan. PSAP/ECC managers/911 agencies are encouraged to use this outline to develop a more detailed and specific COOP plan that meets the needs and circumstances of their agencies and jurisdictions.

This guide was developed in conformance with COOP planning methodologies promulgated by the Federal Emergency Management Agency (FEMA), the National Fire Protection Association (NFPA), and the National Emergency Number Association (NENA).

Instructional text appears in various sections of this guide in ***italicized blue*** font. Those instructions should be deleted once the plan has been completed. Additional COOP planning guidance is available online at the following websites:

FEMA: Federal Continuity Directive 1 *Federal Executive Branch National Continuity Program and Requirements*, January 17, 2017

https://www.fema.gov/sites/default/files/2020-07/January2017FCD1.pdf

FEMA: Federal Continuity Directive 2 *Federal Executive Branch Mission Essential Functions and Candidate Mission Essential Functions Identification and Submission Process*, June 13, 2017

https://www.fema.gov/sites/default/files/2020-07/fema_federal-continuity-directive-2_061317.pdf

NFPA 1600: *Standard on Continuity, Emergency, and Crisis Management*, 2019

https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600

NENA-INF-017.3-2018: *NENA Communications Center/PSAP Disaster and Contingency Plans Model Recommendation*

https://www.nena.org/resource/resmgr/standards/nena-inf-017.3-2018_disaster.pdf

PSAP CONTINUITY OF OPERATIONS (COOP) PLAN

for

[Insert Agency Name]

[Insert Date]

SENSITIVE SECURITY INFORMATION

Public safety communication systems are classified as Critical Infrastructure. This PSAP Continuity of Operations (COOP) Plan and all attached subsections incorporated herein are deemed confidential.

FOREWORD

The nation's emergency services and public safety organizations have been designated as a *critical infrastructure sector* by the Department of Homeland Security (DHS).[1] Public Safety Telecommunicators (PSTs) as "911 center employees" are classified as "*essential critical infrastructure workers*" by the DHS Critical Infrastructure and Cybersecurity Agency (CISA).[2] Individuals serving in a public safety position in law enforcement, fire/rescue, emergency medical services (EMS), and emergency management are designated as *essential critical infrastructure workers.*[2] The work performed by PSTs is critical to the health and safety of the community and must continue during disruptive events.

[INSERT AGENCY NAME] has adopted this Continuity of Operations (COOP) Plan to ensure the capability to support employees, system users, emergency responders, local and regional emergency management agencies, and the public during emergencies. Key objectives to be accomplished by the adoption of this COOP Plan include:

- Minimize disruption to normal service levels
- Mitigate the extent of disruptive events and damage
- Minimize fiscal impacts of disruptive events
- Prepare personnel to implement emergency procedures
- Establish an alternate method to continue service delivery
- Provide for the rapid and efficient restoration of services

Resilience is defined as *the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions ...* [it] *includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents*.[3] This COOP Plan presents a continuity strategy that is intended to assure the resilience and operational capacity of [INSERT AGENCY NAME].

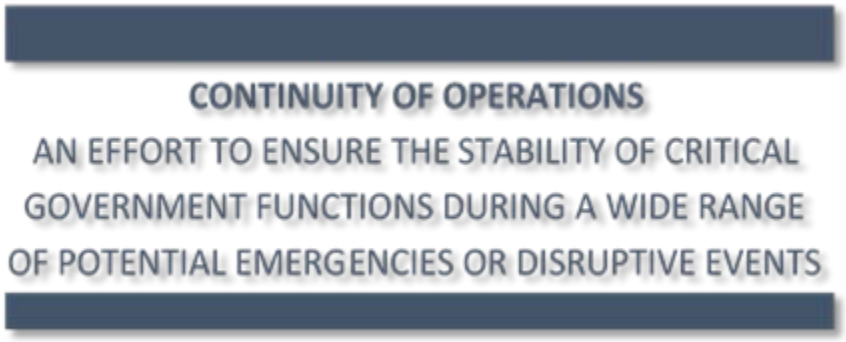
[1] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection
[2] Memorandum on Identification of Essential Critical Infrastructure Workers during COVID-19 Response. (CISA), March 19, 2020
[3] "Presidential Policy Directive – Critical Infrastructure Security and Resilience." The White House President Barack Obama. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

TABLE OF CONTENTS

SIGNATURE PAGE

This *PSAP Continuity of Operations Plan for [INSERT AGENCY NAME]* is approved by the authorized signatories below and is implemented as of the latest signatory date. This plan supersedes all previous plans.

_____	_____
[Insert official name]	Date
_____	_____
[Insert official name]	Date



1. INTRODUCTION

1.1 Purpose

The [INSERT AGENCY NAME] serves a population of [INSERT POPULATION] by managing 911 and public safety communications for the following agencies:

- [INSERT AGENCIES SUPPORTED]
-

The [INSERT AGENCY NAME] coordinates service delivery with local telephone companies and wireless service providers. The statewide Next Generation 911 (NG911) service provider is Lumen, and the regional network provider is [INSERT PROVIDER NAME]. The PSAP is served by the following wireline service providers [LIST WIRELINE SERVICE PROVIDERS], the following wireless carriers [INSERT WIRELESS SERVICE PROVIDERS], and Voice over Internet Protocol (VoIP) providers [INSERT LIST OF VoIP PROVIDERS].

The purpose of this COOP Plan is to establish a strategy to assure the resilience and operational capacity of the [INSERT AGENCY NAME]. The capability to prepare for, respond to, and recover from emergencies affecting [INSERT AGENCY NAME] operations is dependent upon the proficiency and well-being of its employees and the clarity of its leadership.

This COOP Plan outlines the steps necessary for [INSERT AGENCY NAME] to maintain a baseline operational capacity in its core functions during a localized or region-wide event that disrupts normal operations. It encompasses all phases of the continuity management process including activities to accomplish within four distinct yet overlapping phases:

Prevention – Activities that are implemented before an emergency occurs to avert or minimize the probability of occurrence and the related potential impact of a given hazard.

Preparedness – Activities that are intended to enhance the capacity of an organization to protect itself from the effects of emergency events. Preparedness activities include developing response plans, maintaining situational awareness, acquiring protective equipment, training staff, and conducting drills and exercises.

Response – Activities that are initiated to address the immediate effects of an emergency through the application of procedures and emergency resources. These activities are intended to protect lives and property and meet short-term human needs.

Recovery – Activities that involve both short- and long-term actions that are intended to restore the operational capacity to a pre-disaster condition.

1.2 Authorities

The [INSERT AGENCY NAME] 911 system is managed in accordance with various state regulations, professional standards, and practices promulgated by professional organizations including:

Legal Authorities

- The Nebraska Emergency Management Act, Neb. Rev. Stat. §§ 81-829.36 to 81-829.75
- 911 Service System Act, Act, Neb. Rev. Stat. §§ 86-1001 to 86-1029.03
- Emergency Telephone Communications Systems Act, Neb. Rev. Stat. §§ 86-420 to 86-441.01
- Enhanced Wireless 911 Services Act, Neb. Rev. Stat. §§ 86-442 to 86-470
- [INSERT AGENCY NAME] Interlocal Agreement for E911 Public Safety Answering Point Services

2. SITUATION

[INSERT COUNTY/REGION] is susceptible to a wide range of natural and technological hazards and human-induced threats. The [INSERT AGENCY NAME] leadership is responsible for assuring the resilience and operational capability of the agency regardless of emergency or disaster circumstances. The [INSERT AGENCY NAME] is an integral component of the region's public safety infrastructure that may best be described as a system of systems.

2.1 Risk Identification and Vulnerability Assessment

A risk is a probable threat to an organization that has the potential to cause harm. Vulnerability may best be described as an exposure to risk and its associated consequences. Risk management is the *process of identifying, analyzing, and communicating risk, and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken*.[4] Organizations seek to manage risk by implementing controls to mitigate risk and minimize the disruption of normal operations.

2.2 Hazards and Threats

A natural hazard is defined as a *source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena*.[5] [INSERT COUNTY NAME HERE] is susceptible to a range of natural hazards including severe thunderstorms, tornados, flooding, winter storms, and pandemic disease.

Technological hazards are those that result from interactions with the manmade environment such as transportation systems, utilities, communication systems, nuclear power generation, and hazardous materials releases.

Human-induced threats involve intentional acts such as violence, attacks on critical infrastructure, terrorism, civil unrest, and cybersecurity attacks.

Communication facilities are susceptible to localized or site-based incidents that can disrupt the operation of departments. These include extended power outages, utility system failures, fires, information technology (IT) network outages, and telecommunication system failures. The PSAP must be prepared to implement continuity procedures to maintain operational capacity regardless of the initiating incident. The following table presents hazards and threats that may impact public safety communication facilities across Nebraska.

[4] *DHS Risk Lexicon*. Department of Homeland Security (September 2010), page 30. https://www.cisa.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf

[5] Ibid., page 21.

Hazards and Threats		
Natural Hazards	**Technical Hazards**	**Man-Made Threats**
Severe Thunderstorms/Lightning	Communication Network Outage	Cybersecurity Incident
Tornado	Computer System Failure	Civil Unrest/Protest
Flooding	Energy Utility Failure	Property Damage/Destruction
Winter Storm/Blizzard	Water Utility Failure	Workplace Violence
Earthquake/Subsidence	Hazardous Material Release	Sabotage
Extreme Heat	Facility Structure Fire	Theft
Pandemic Disease	Cooper Nuclear Station EPZ*	Terrorism (CBRNE**)
Agriculture Disease	Dam Failure	Enemy Military Attack
Wildfire		
* *Emergency Planning Zone (EPZ) Nemaha and Richardson Counties*		
** *Chemical, Biological, Radiological, Nuclear, Explosive*		

Table X – [INSERT PSAP NAME] Hazards and Threats Matrix

Hazard or Threat	Probability of Occurrence	Estimated Impact Upon Health & Safety			Estimated Impact Upon Operations		
		Limited	*Moderate*	*Major*	*Limited*	*Moderate*	*Major*
Natural Hazards							
Severe Thunderstorm							
Tornado							
Winter Storm							
Extreme Heat							
Flooding							
Earthquake							
Pandemic Disease							
Agriculture Disease							
Technological Hazards							
Energy Utility Failure							
Water Utility Failure							
Computer Network Outage							
Communication Network Failure							
Structural Fire							
Hazardous Materials Release (Fixed site)							
Hazardous Materials Release (Transit)							
Cooper Nuclear Station EPZ							
Human-induced Hazards							

Hazard or Threat	Probability of Occurrence	Estimated Impact Upon Health & Safety			Estimated Impact Upon Operations		
		Limited	*Moderate*	*Major*	*Limited*	*Moderate*	*Major*
Workplace Violence							
Cybersecurity (data/infrastructure)							
Civil Unrest/Protest							
Terrorism (CBRNE)							
Property							
Workplace Violence							
Sabotage							
Theft							
Terrorism							
Enemy Military Attack							

3. CONCEPT OF OPERATIONS

3.1 General

This COOP Plan is intended to promote the continuation of services during a disruptive incident or large-scale emergency. The objectives of the COOP Plan include:

- Preserving the public's confidence in the local 911 system
- Protecting the health and safety of agency personnel and visitors
- Enhancing organizational and operational resilience to hazards and threats
- Minimizing the impact on the operational capacity of the PSAP
- Implementing the rapid restoration of essential functions and technology systems

During a continuity event or emergency, PSAP personnel will function within the normal organizational structure and chain of command. Personnel also may be invited to participate in or coordinate with operations of local and regional emergency operations centers (EOCs) during a disaster.

3.2 Mission Essential Functions

Certain services must be continued regardless of emergency circumstances. These essential services are supported by discreet tasks that are identified as mission essential functions (MEFs). A MEF is a function or task that must be continued throughout or resumed immediately after a disruptive event to maintain mission-critical services. During a disruptive event, each MEF will be assigned to the primary or an alternate staff member in accordance with the staffing succession procedures. The following table presents the most critical MEFs that must continue during an emergency.

[Prioritize and insert mission essential functions into the following table]

Priority	Mission Essential Function
1	
2	
3	

Priority	Mission Essential Function
4	
5	
6	
7	
8	
9	
10	

3.3 Mission Essential Workforce

Essential workforce positions are those that are responsible for supporting MEFs or are assigned a critical response role during an emergency incident. Personnel may be required to work extended shifts to assure coverage of positions.

[INSERT ORGANIZATION CHART]

3.3.1 Orders of Succession

The [INSERT AGENCY NAME] must maintain an essential level of staffing during a disruptive event or emergency incident. The PSAP will utilize an emergency staffing methodology for all critical and essential positions. Each key position within the [INSERT AGENCY NAME] is staffed by an individual on a full-time basis. Some individual staff members may be unavailable during an emergency. Alternate positions must be identified that will assume the duties of each key position. Two alternate personnel should be designated to replace the incumbent in each critical position. Those serving in an alternate capacity must be properly trained and prepared to support alternate roles and tasks.

It is critical that the [INSERT AGENCY NAME]'s MEFs are maintained. This may require employees to be assigned work of a lower or higher-level classification due to a high level of absences. Supervisors will track the shifts, and level of work performed during an incident. Records must be kept on the time that each employee works in each position as well as all overtime and any other receipts for items purchased during the event for Federal Emergency Management Agency (FEMA) grant reimbursement.

[Please use the following tables to identify positions within the PSAP that are essential to maintain operations. List alternative positions that will fill the position in the absence of the incumbent. List key MEFs that are assigned to the position and any legal authorities to be delegated to the person temporarily filling the position (e.g., hiring, budget, purchasing, etc.). The table can be copied, and additional positions inserted as needed. Note: All positions should be listed by title and not the names of individuals serving in those positions.]

[Insert Position Title]
Alternate 1:
Alternate 2:
Essential Tasks to Perform:
Authority to be Delegated:

[Insert Position Title]
Alternate 1:
Alternate 2:
Essential Tasks to Perform:

Authority to be Delegated:

[Insert Position Title]
Alternate 1:
Alternate 2:
Essential Tasks to Perform:
Authority to be Delegated:

[Insert Position Title]
Alternate 1:
Alternate 2:
Essential Tasks to Perform:
Authority to be Delegated:

3.4 Essential Systems and Software Applications

PSAP operations are heavily dependent upon a variety of technology systems. Efficient dispatch services utilize electronic systems including 911 call-handling equipment (CHE), computer-aided dispatch (CAD), records management system (RMS), logging/recording system, geographic information system (GIS), and others. A disruptive event may render these systems inoperable or inaccessible. Hardware and software applications must be documented to support recovery operations.

[Use the following tables to document the computer hardware, software applications, data, and records that are essential to PSAP operations. Please ask your IT support for assistance in completing and maintaining this section]

Essential Hardware				
Equipment Description	Manufacturer	Model No.	Serial No.	Vendor Support Contact Info.

Application Inventory			
Manufacturer/Vendor	Application Name	Version#	Application Interfaces/Dependencies*
*Data requirements, interfaces, processing relationships, etc. Identify application dependencies—i.e., what related processes must be available for each application to function properly?			

Essential Records and Data			
Record Type	Data Type	Offsite Backup	Backup Frequency

Essential Records and Data			

IT Vendor Contacts		
Hardware or Application	Vendor Name	Point(s) of Contact
		Name: Phone: Email:
		Name: Phone: Email:
		Name: Phone: Email:
		Name: Phone: Email:

It is important to capture the circuit identification (ID) numbers of each carrier that provides telecommunications services for the PSAP including 911 trunks and administrative lines. A table is provided below to document circuit IDs and carrier contact information for trouble reporting.

Vendor Contacts				
Carrier	**Circuit ID**	**Point(s) of Contact**	**Phone Number**	**Account Number**

3.4.1 Failover/Rollover Operations

For essential systems or software, it is important to plan and identify failover/rollover operational scenarios and identify how 911 operations will continue. This involves identifying:

- Possible scenarios
- Level of risk (high, moderate, low)
- Location of operations
- Call routing protocol
- Operational protocol
- Any important notes or details supporting the scenario

[Use the following table to document the applicable failover/rollover operational scenarios in the PSAP. An example is included in italics, if not applicable, please delete it. Refer to Appendix A for a blank form.]

Failover/Rollover Operations					
Scenario	**Risk**	**Location of Operations**	**Call Routing Protocol**	**Operational Protocols**	**Notes**
High Volume of 911 Calls	*Low*	*PSTs remain in place*	*Overflow calls are rerouted to [INSERT PSAP NAME]*	*Callers are transferred back to the PSAP via an administrative line for dispatch*	

3.5 Alternative Work Site

A continuity event such as a fire or tornado may render the communications facility inaccessible or unusable. Such an event will require the transfer of operations and relocation of personnel to an alternate worksite (AWS). The PSAP manager, or their designee, is responsible for determining if the facility is safe to access and equipment suitable for use.

The PSAP staff must be prepared to transfer operations to an alternate or backup worksite. A PSAP requires an AWS that supports immediate activation with limited preparation efforts. An AWS could be a backup PSAP, a mobile command unit, the support of another regional PSAP, or some staff working from home. As events progress from a moderate to a major event, the AWS may change.

A memorandum of understanding (MOU) or interlocal agreement is required when transferring 911 calls to an alternate PSAP. Legal agreements must be reviewed regularly and kept up to date.

3.5.1 Designated AWS

The designated AWS is located at: ***[Insert name and address of AWS]***

[Insert map(s) to each AWS. Highlight primary and alternate routes from the primary PSAP to the AWS]

3.5.2 AWS Activation

The [INSERT AGENCY NAME] manager/director, or their designated alternates, are authorized to activate the AWS. This includes notifying the official in charge of the site and arranging for the transport or delivery of equipment and supplies. Contact the following representatives of the AWS to request site activation:

Primary AWS	
Facility Name:	
Facility Address:	
Contact Name:	Contact Name:
Telephone:	Telephone:
Telephone:	Telephone:
Email:	Email:
Other:	Other:

3.5.3 Devolution of Operations

Operational control is transferred to an AWS through a process known as devolution. This involves the transfer of control (i.e., direction and control, operations) from the primary worksite to the AWS. Key personnel must arrive at the AWS and, when ready, assume control and initiate operations. Personnel should be prepared to relocate to the appropriate AWS to resume operations.

Equipment and supplies may need to be moved to the AWS. If possible, a cache of materials should be maintained at the AWS for immediate use. Emergency procurement of equipment and supplies may be required to replace items that are damaged, missing, or inaccessible. The PSAP manager will maintain a list of qualified vendors and manage emergency procurement activities.

Equipment and Supplies to Transport to AWS	

3.5.4 Vital Records and Databases

Vital records are those records that must be preserved, protected, and available for use by [INSERT AGENCY NAME] and public safety agencies during or immediately following a continuity event. Examples include local hard drives, shared network drives, and/or external devices, an offsite data facility, or a cloud-based solution. A sample layout is below.

Vital Records ---Site Inventory

Vital Records Maintained at Location			
Record Type	**Data Type**	**Offsite-Back-up Location**	**Backup Frequency**

4. INCIDENT MANAGEMENT

Most continuity events are of short duration with limited impact on the organization. However, significant events may require the activation of this COOP Plan and the implementation of an incident management team. The PSAP will continue to operate using the normal organizational structure until an alternate command and control structure is implemented.

4.1 COOP Plan Activation

The PSAP manager or their designee are authorized to activate this COOP Plan in response to an incident or emergency event.

4.2 Incident Management Team

The Incident Management Team (IMT) concept is used to coordinate the response to an emergency event that disrupts normal operations. The members of the IMT will be selected from PSAP staff members based upon their roles and technical expertise.

The [INSERT AGENCY NAME] will utilize its normal organizational structure to manage the response to short-term continuity events. Complex or long-term incidents will require the IMT to use the National Incident Management System (NIMS) methodology. All PSAP staff members are required to complete NIMS training and participate in exercises to test their ability to operate using the NIMS methodology.

4.3 Incident Action Plan

The Incident Action Plan (IAP) is a tool to aid in managing the response to a disruptive incident. The IAP is used to capture information that is relevant to the incident, including incident type, location(s) impacted by the incident, situation summary, operational period, incident objectives, IMT members and roles, external resources, and management approval. The IAP was formatted for use by individuals who do not frequently operate under the NIMS methodology. Digital and printed versions of the IAP form (blank) should be maintained and accessible during an emergency. Refer to Appendix B for instructions on completing the IAP.

4.4 Crisis Communications

The PSAP manager/director is responsible for coordinating information during an emergency that disrupts 911 service. The PSAP internal communications procedures utilize a combination of voice, text, and email to communicate with staff. The crisis communications procedures address the following:

- Staff notification and communication procedures
- Coordination with partner agencies
- Coordination with PSAP manager and senior officials

- Coordination with contractors and vendors
- Coordination with Nebraska Public Service Commission
- Public information and media relations

PSAP Communications Contact List				
Department/Official/Vendor or Media	**Contact Name**	**Phone**	**Email**	**Backup Frequency**

[Insert Employee Phone Tree]

4.5 Personnel Safety and Accountability

A continuity event can affect the health and safety of [INSERT AGENCY NAME] staff. When a disruptive event occurs, personnel may be working in the facility, at home, or traveling outside of the area. The PSAP supervisor must account for all employees during and after the occurrence of a continuity event. The emergency notification process will involve documenting the employee's location, status of their health and safety, and availability to report for work.

The PSAP will use a dedicated non-published telephone number to aid in monitoring personnel status. Staff members will use the number to report their status and receive instructions and assignments. Personnel assigned to monitor the phone will maintain a log of staff contacts and document the status of each employee. An emergency contact list for personnel will be maintained separately from this plan in digital and print formats. The contact list must be updated monthly.

5. RECOVERY AND RECONSTITUTION

Post-incident recovery involves evaluating the status of PSAP resources following a disruptive incident and reorganizing to secure resources to maintain operational capacity. Reconstitution is the process of resuming normal operations at the primary work site, AWS, or temporary/permanent replacement facility.

Recovery and reconstitution activities will be implemented to restore the operational capacity of the PSAP. The organization will be prepared to support recovery on two levels. The first level, continuity of operations, involves the human and physical resources that are necessary to provide services to partner agencies. The second level, disaster recovery, involves the recovery of IT equipment, systems, applications, and networks. The recovery process involves establishing and prioritizing short-term and long-term objectives.

Examples of short-term recovery objectives include:

- Provide for the needs and well-being of PSAP staff
- Continue operations at the AWS
- Restore essential systems and services
- Recover data
- Assess damages to the facility and assets
- Activate vendor support agreements
- Communicate with stakeholders

Examples of long-term recovery objectives include:

- Replace equipment
- Recruit and hire permanent staff
- Restoration of the primary PSAP facility
- Establish long-term operations at an interim worksite

6. COOP TRAINING

The PSAP staff will receive training and will be tested in the use of the COOP Plan annually.

6.1 Training

The [INSERT AGENCY NAME] staff must be trained in the use of this COOP Plan. Initial and annual training is intended to strengthen capabilities that are needed to respond to and recover from a continuity event. Topics for training include:

- Threat monitoring, alerting, and warnings
- Emergency response procedures
- Crisis communications procedures and processes
- Establishing alternate PSAP and devolution procedures
- Reconstitution operations procedures

6.2 Exercises

Organizations use preparedness exercises to test and validate procedures and planning assumptions, test new equipment, and refine personnel capabilities. The PSAP will utilize exercises to assess continuity capabilities. Exercise should be conducted in coordination with partner agencies and the local office of emergency management.

6.3 After-Action Reporting

Training and real-world events represent opportunities for organizations to implement plans and assess response capabilities. Drills, exercises, and responses to actual emergency events should be documented using an after-action report/improvement plan (AAR/IP) format. This schedule and list require frequent updates and may be used as a separate document.

Staff Training/Exercise Schedule			
Date	**Topic**	**Location**	**Attendee**

7. PLAN ADMINISTRATION AND MAINTENANCE

7.1 Distribution and Access

This COOP Plan contains sensitive security information that will be restricted from public access. The distribution plan must be approved by the [INSERT AGENCY Name] manager/director. Distribution of this COOP Plan is limited to essential personnel and authorized representatives of partner agencies and contractors. Copies of this COOP Plan will be maintained at the facility and offsite in print and digital format.

7.2 Maintenance

The [INSERT AGENCY NAME} manager/director] is responsible for assuring that this COOP Plan is maintained and tested annually. The COOP Plan will be reviewed and updated no later than [INSERT DATE] of each year. The review process should include an assessment of changes in hazards, threats, personnel assignments, facilities, hardware, and other resources.

7.3 Records and Reports

Records related to the activation of this COOP Plan must be maintained in compliance with state law and [INSERT AGENCY NAME] record-retention policies. Documentation of disaster-related expenses will be needed to support cost recovery requests. Examples of preparedness and incident-related reports include:

- Disaster and Continuity Plan
- Exercise and actual event AAR/IP
- Personnel and payroll records
- Purchase orders, receipts, and contracts
- Reports of injuries and workers' compensation documents
- Other administrative data and reports related to incidents

APPENDIX A – FAILOVER OPERATIONS WORKSHEET

Failover Operations Worksheet					
Scenario	**Impact Level**	**Location of Operations**	**Call Routing Protocol**	**Operational Protocols**	**Notes**

APPENDIX B – INCIDENT ACTION PLAN

1. IAP Purpose

The IAP document is intended for use during an emergency incident. The IAP contains information regarding the nature of the incident, response strategy for managing the incident, staff assignments, and objectives to achieve during a prescribed operational period.

Blank copies of the IAP document should be readily available to staff in digital and print formats. The following section presents the IAP form and an explanation of its preparation and use.

CONTINUITY OF INCIDENT ACTION PLAN

1. Incident Type	2. Prepared By	3. Date	4. Time
5. Incident Location (s)			
6. Operation Period Date: From_____ To_____ Time: From_____ To_____			
7. Situation Summary and Priorities			
8. Hazards and Safety Measures			
9. Incident Objectives			
Objectives	Strategy and Resources Required	Assigned To	

10. Incident Management Team (IMT) Members and Assignments		
Name	Position/IMT Role	Contact Information
		Phone: Email:
		Phone: Email:
		Phone: Email:
		Phone: Email:
		Phone: Email:
11. External Resources		
Contractor/Vendor Name	Services Provided	Contact
		Phone: Email:
		Phone: Email:
		Phone: Email:
		Phone: Email:
12. Attachments		
13. Approved By:	14. Date:	Time:

2. Continuity IAP Instructions

Purpose
The IAP is a tool to aid the organization in managing the response to a disruptive incident. The IAP is used to capture incident type, location or locations impacted by the incident, situation summary, operational period, incident objectives, IMT members and roles, external resources, and approvals.

Preparation
The IAP is typically completed by the individual assigned to lead the organization's response and recovery efforts. Information entered on the form should be concise and clearly described. The IAP is reviewed and approved by a senior representative such as the Incident Commander, Public Safety Director, 911 Director, or Emergency Management Director.

Distribution
The IAP should be distributed to all individuals involved in leading incident response and recovery efforts. The priorities and objectives should be presented during briefings to the IMT. Copies of each completed IAP will be retained for use in the incident documentation and post-incident review(s).

Incident Priorities
The initial stages of a disruptive incident may be chaotic and confusing. It may be difficult to identify the extent of disruptions and damages due to a lack of situational awareness. The IAP is intended to provide individuals responsible for managing the incident response with coordinating information needed to establish actionable priorities and objectives.

Initial priorities will begin with broad and generic language due to the lack of specific information. Examples of initial priorities may include:

- Establish the IMT
- Account for the health and safety status of all personnel
- Determine the status of partner agencies
- Identify the extent of disruption to normal operations
- Determine the level of damage to facilities
- Restore essential services
- Recall off-duty personnel to support response efforts

Priorities will progress to include more specific actions such as:

- Establish defined operational periods
- Restore electrical service
- Request emergency assistance from contractors and vendors
- Conduct damage assessment of the primary facility

Incident Objectives

Incident objectives provide direction and help focus the IMT's actions throughout the response and recovery phases of the incident. Incident objectives are more immediate than priorities and represent a target to be attained during the operational period. Objectives provide a means to measure progress achieved during an operational period. The characteristics of effective incident objectives should reflect the ***SMART*** concept. Incident objects should be:

Specific. Contain specific direction regarding the five W's – who, what, when, where, and why. The objective should specify a timeframe in which it should be accomplished.

Measurable. Include metrics that describe observable actions and outcomes.

Achievable. Be within the control, influence, and realistic application of available resources.

Relevant. Be related to the mission of the organization and related to goals and strategic intent.

Time-bound. Include a reasonable timeframe for completion.

The following table is a guide that describes the information that should be entered into each section of the IAP

Item No.	Section Title	Instructions
1.	Incident Type	Enter the type of incident that has occurred (i.e., flood, fire, power outage, etc.).
2.	Prepared By	Enter the name of the person completing the IAP.
3.	Date	Enter the date the IAP was prepared.
4.	Time	Enter the time the IAP was prepared.
5.	Incident Location(s)	Enter the location (or locations) that are affected by the incident, including addresses.
6.	Operational Period	Enter the time that the IAP covers. The typical operational period is 8–12 hours.
7.	Situation Summary and Priorities	Enter a summary of the current conditions that exist at the beginning of the operational period. The summary should include the priorities for the operational period.
8.	Hazards and Safety Measures	Enter the hazards that currently exist, and precautions being taken to protect personnel.
9.	Incident Objectives A. Objectives B. Strategy and Resources Required C. Assigned To	A. Enter each objective that has been defined for the operational period. Objectives should clearly reflect the SMART concept. B. Describe the strategy and resources necessary to achieve the objective. C. Enter the name of the individual responsible for leading the efforts to attain the objective.
10.	Incident Management Team (IMT) Members and Assignments Name Position/IMT Role Contact Information	Enter the name, position/role, and contact information for members of the IMT.
11.	External Resources Contractor/Vendor Name Services Provided Contact	Enter the name of contractor or vendor organizations supporting the operational period. Enter the services being provided and contact information for vendor representatives.
12.	Attachments	List any additional documents that are attached to the IAP.
13.	Approved By	Enter the name of the person reviewing and approving the IAP.
14.	Date and Time	Enter the date and time that the IAP was approved.

3. Incident Task List

The information presented in the following tables is an example of the use and development of an Incident Task list. These tasks list should be modified to meet the needs of each PSAP. The list below is an example used by a Nebraska county that shared this information for use in the document:

The listed task items are intended to be used as objectives in the IAP.

Incident Task List	
Stage I: Short-term Activation (Day 1 at AWS) **Goal: Attain operational status within [12] hours**	
Task	Completed
Notify department personnel that the COOP Plan has been activated and devolution/relocation procedures are being implemented (include IT or appropriate departments that manage network and equipment at AWS)	
Contact the AWS representative to confirm that the site is available to support the relocation of department personnel and coordinate site access	
Determine which members of the Continuity Team are to report immediately and who is on call	
Contact Continuity Team and advise them of their status (report or on-call)	
Convene at the designated AWS per Continuity Management Team (CMT) instructions	
At AWS—coordinate with the CMT for specific seat assignments	
Verify availability of necessary office supplies (e.g., paper, envelopes, pens, pencils, forms, paperclips, stapler, staples, etc.)	
Verify access to items on the Equipment list using recovery time objective priority order	
Verify access to computer systems and software on the Computer Programs List using recovery time objective priority order	
Verify access to items on the Vital Records List using recovery time objective priority order. Coordinate retrieval of offsite, as required	
Review Communications Contact list and make necessary contacts, as required, to alert them of the situation and/or solicit support. (Notify the EOC or EMA that department operations have been initiated at the AWS. Notify officials, media contacts, vendors, etc.)	
Advise CMT of the Office's recovery status	
Brief department staff regarding site operation procedures	
Begin performing functions/processes on the Function/Process list using recovery time objective priority order	
Determine work schedules and staffing needs for the remainder of the week	
Contact employees currently on-call and advise them of their status and work schedule	

Provide scheduled situation updates to the appropriate point of contact at the EOC	
Provide situation updates to staff working at the AWS at regular intervals	
Track hours, overtime, and receipts for items purchased	

Incident Task List	
Stage II: Long-term Activation (Up to 30 days at AWS)	
Task	Completed
Continue to monitor the Function/Process list to add functions, as staff and time allows	
Advise CMT of the Office's resumption of process and staffing status	
Continue to review Communications Contact list and make necessary calls, as required to advise, or coordinate	
Determine and set up workspace for additional staffing using Minimum Operating Requirements as a guide	
Order and replenish equipment and supplies, as required and coordinate with CMT	
Track hours, overtime and receipts for items purchased	
Assist with clean up and/or salvage operations (refer to Vital Records and Equipment tables for target salvage items	
Determine inventory of usable equipment, documents, and materials	
Assist with determining losses for insurance carriers, if required, coordinate with Management Team	
Provide briefing to entire office staff	
Prepare and present briefing for Customers, Vendors, and Suppliers, as required	
Assist with developing long-term recovery strategy/reconstitution activities	
Monitor workforce stress caused by the relocation	

Incident Task List	
Stage III: Extended Relocation:	
Task	Completed
Assess the need to relocate department operations to another location (i.e., leased space or other governmental jurisdiction)	
Negotiate and execute a commercial lease or an interlocal agreement for the extended use space not owned by the County	

4. After-Action Report

Introduction	
After Action Report (AAR) Overview	
Incident Overview:	
Duration:	
Focus *(Check appropriate area(s)**:* ☐ Prevention ☐ Response ☐ Recovery ☐ Other	***Activity/Scenario*** *(Check appropriate area(s):* ☐ Fire ☐ Severe Weather ☐ Hazardous Material Release ☐ Bomb Threat ☐ Medical Emergency ☐ Power Outage ☐ Evacuation ☐ Lockdown ☐ Special Event ☐ Exercise/Drill ☐ Other

Location:	
Participating Organizations:	
Strengths:	
Areas of Improvement:	
Recommendations:	
Conclusion and Next Steps:	

The following table is a guide that describes the information that should be entered into each section of the AAR

Item No.	Section Title	Instructions
1.	Introduction	Include a brief synopsis of the incident and as much as possible include a sequence of events (if available)
2.	After Action Report Overview	Include a compilation of information from the different departments and staff who participated in the response and the purpose of the AAR
3.	Incident Overview	Insert incident/exercise details in this section
4.	Duration	Insert incident/exercise /event time
5.	Focus	Select the type of incident and the focus of the event
6.	Activity/Scenario	Select the reason for the incident
7.	Location	Enter the incident/exercise/event location in this section
8.	Participating Organizations	Insert organization names in this section
9.	Strengths	List the strengths of the incident/event response and activities in this section
10.	Areas of Improvement	List the opportunities for improvement of the incident/event response and activities in this section
11.	Recommendations	List recommendations for next steps for future improvement and response
12.	Conclusion and Next Steps	Insert a conclusion and next steps for incident/event response in this section