

# Security Guidelines for the Electricity Sector: Continuity of Operations

<b>Effective Date: TBD Pending BOT Approval</b>	<b>Version: 2.0</b>
	<b>Approved by Board of Trustees: May 2007</b>

## Preamble

This guideline reviews the concepts an electricity sector organization should consider when developing continuity of operation plans for critical facilities and functions. Each organization shall decide on the scope of facilities and functions included based on the risk it can accept and the practices it deems appropriate.

## Introduction

This Continuity of Operations Guideline is to provide North American electricity sector organizations with the concepts they should consider when developing operational continuity plans. Such plans are one means of preparing the organization to ready itself for natural or man-made incidents, prevent or mitigate an incidents impact, and to assure response and recovery efforts are coordinated and effective. Detail on what constitutes a critical facility or function are not provided in this guideline. Critical facilities and functions should be identified by the impact analysis and risk assessments each organization will develop to support its operational continuity plans. The guideline is a framework identifying the concepts and steps associated with an effective operational continuity plan.

## Purpose

In the event a major natural disaster or man-made incident creates an interruption in normal operations, an operational continuity plan will reduce the impact and ensure prompt resumption of operations.

## Applicability

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual organization.

In developing its operational continuity plan, each electricity sector organization should consider defining and identifying those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility or function through redundancies may make some facilities or functions less critical than others.

From an industry-wide perspective, a critical facility or function may be defined as any facility, function, or combination thereof that, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

# Continuity of Operations Security Guideline

## Version 2.0: Effective July 1, 2007

### Guideline Statement

This guideline describes steps electricity sector organizations should consider in developing plans that will ensure continuity of operations during and after an incident or crisis.

### Table of Terms

In this guideline, reference is made to the following unique terms when designing and implementing a continuity of operations plan. The definitions for these unique terms are:

**Alternate Worksite<sup>1</sup>** — A work location, other than the primary location, to be used when the primary location is not accessible.

**Business Continuity<sup>1</sup>** — A comprehensive managed effort to prioritize key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to the challenges that surface during and after a crisis.

**Business Continuity Plan<sup>1</sup>** — An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the continuity of operations through personnel training, plan testing, and maintenance.

**Crisis<sup>1</sup>** — Any global, regional, or local natural or human-caused event or business interruption that runs the risk of (1) escalating in intensity, (2) adversely impacting shareholder value or the organization's financial position, (3) causing harm to people or damage to property or the environment, (4) falling under close media or government scrutiny, (5) interfering with normal operations and wasting significant management time and/or financial resources, (6) adversely affecting employee morale, or (7) jeopardizing the organization's reputation, products, or officers, and therefore negatively impacting its future.

**Crisis Management Team<sup>1</sup>** — A group directed by senior management or its representatives to lead incident/event response comprised of personnel from such functions as human resources, information technology facilities, security, legal, communications/media relations, manufacturing, warehousing, and other business critical support functions.

**Critical Function<sup>1</sup>** — Business activity or process that cannot be interrupted or unavailable for several business days without having a significant negative impact on the organization.

**Disaster<sup>1</sup>** — An unanticipated incident or event, including natural catastrophes, technological accidents, or human-caused events, causing widespread destruction, loss, or

## Continuity of Operations Security Guideline Version 2.0: Effective July 1, 2007

distress to an organization that may result in significant property damage, multiple injuries, or deaths.

**Disaster Recovery**<sup>1</sup> — Immediate intervention taken by an organization to minimize further losses brought on by a disaster and to begin the process of recovery, including activities and programs designed to restore critical business functions and return the organization to an acceptable condition.

**Disturbance**<sup>2</sup> — An unplanned event that produces an abnormal system condition or any perturbation to the electric system.

**Emergency**<sup>1</sup> — An unforeseen incident or event that happens unexpectedly and demands immediate action and intervention to minimize potential losses to people, property, or profitability.

**Mitigation Strategies**<sup>1</sup> — Implementation of measures to lessen or eliminate the occurrence or impact of a crisis.

**Pandemic**<sup>3</sup> — An epidemic outbreak of an infectious disease that spreads worldwide, or at least across a large region. The worldwide outbreak of a disease in humans in numbers clearly in excess of normal.

**Prevention**<sup>1</sup> — Plans and processes that will allow an organization to avoid, preclude, or limit the impact of a crisis occurring. The tasks included in prevention should include compliance with corporate policy, mitigation strategies, and behavior and programs to support avoidance and deterrence and detection.

**Readiness**<sup>1</sup> — The first step of a business continuity plan that addresses assigning accountability for the plan, conducting a risk assessment and a business impact analysis, agreeing on strategies to meet the needs identified in the risk assessment and business impact analysis, and forming Crisis Management and any other appropriate response teams.

**Recovery/Resumption**<sup>1</sup> — Plans and processes to bring an organization out of a crisis that resulted in an interruption. Recovery/resumption steps should include damage and impact assessments, prioritization of critical processes to be resumed, and the return to normal operations or to reconstitute operations to a new condition.

**Response**<sup>1</sup> — Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as provide services to the surviving population. Response steps should include potential crisis recognition, notification, situation assessment, and crisis declaration, plan execution, communications, and resource management.

# Continuity of Operations Security Guideline

## Version 2.0: Effective July 1, 2007

**Risk Assessment**<sup>1</sup> — Process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization's operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.

### Guideline Detail

Electric utility organizations historically have extensive plans in place for the restoration of service to customers in response to natural disasters such as earthquakes, floods, and other weather-related emergencies. Business practices and critical assets should have their own business recovery plans in place in the event a natural disaster (flood, earthquake, fire, pandemic, etc.) or a man-made crisis (vandalism, sabotage, terrorism, etc.) impacts strategic business facilities or functions.

Some steps to consider when either beginning or reassessing a Continuity of Operations program should include:

### Readiness

- Conduct a Readiness Evaluation and assign responsibilities
- Conduct a Business Impact Analysis
- Conduct a company-wide Risk Assessment
- Determine the maximum tolerable downtime of critical applications
- Use the data from the tools listed above to develop a Disaster Recovery Strategy to ensure maximum tolerable downtimes for critical applications and/or services are not exceeded
- Identify the Disaster/Crisis Management Team and define:
  - What constitutes a disaster and a crisis
  - Who and how a disaster /crisis are declared
  - Authorities to put a response plan into action

### Prevention

- Compliance with an organizations business policies
- Identification of mitigation strategies
- Avoidance, deterrence and detection of threats and risks
- Pre-positioning of recovery assets
- Staff response training and exercises

### Response

- Declare the Disaster/Crisis and mobilize the Disaster/Crisis Management Team
- Execute established plans
- Communicate/coordinate response efforts

# Continuity of Operations Security Guideline

## Version 2.0: Effective July 1, 2007

### Recovery

- Damage impact and assessment
- Process for resuming critical and remaining functions
- Disaster/Crisis Management Team continues managing the disaster incident/crisis
- Execute established plans
- Communicate/coordinate response efforts

Developing recovery strategies for critical applications as well as critical functions or facilities is a prudent step in the planning process. Many companies in the electricity sector that own or operate critical facilities have plans for relocating critical operations such as their Transmission Control Center, Data Center, Customer Call Center, and other key business operating facilities. Another good practice is to locate these critical functions at alternate facilities that are distant from the primary location to ensure continuity of operations.

Alternate facilities do not have to mirror the primary facility but they should be able to maintain critical operations at a predetermined minimal level until the primary facility is restored. The following are important considerations when selecting alternate locations, these facilities should be:

- ...outside the immediate area to ensure that the location will not be impacted to the same degree as the primary.
- ...accessible to personnel or transportation arrangements to ensure that personnel can get to the alternate facility within the timeframe required to assure continuity of critical operations. (Personnel should be provided with driving directions to the site.)
- ...controlled by the company either through ownership or other arrangements to ensure they will be available during an emergency.
- ...supported by key infrastructure requirements, particularly voice and data networks, key operating systems, and file storage.
- ...capable of storing supporting resources for retrieval when needed.

Business Recovery Plans typically address the following process elements:

- ...are coordinated by a designated person or department to develop, maintain, and test the business recovery plan.
- ...provide for training on the specific emergency plans for individual critical functions that supplement the overall business recovery plan.
- ...are kept up to date on the protocols for the activation of the business recovery plan including facility preparation, systems activation, and relocation of personnel.
- ...are exercised annually on the implementation of the business recovery plan, a review of lessons learned, and revision of the plan as required.

## Continuity of Operations Security Guideline Version 2.0: Effective July 1, 2007

- ...include trained personnel that have been tested annually on their performance of the business recovery plan requirements.

### Related Documents

American Red Cross; *Preparing Your Business for the Unthinkable*; Washington, D.C.; <http://www.redcross.org/services/disaster/beprepared/unthinkable2.pdf>

ASIS, International; *Business Continuity Guideline*; June 2006; <http://www.asisonline.org/guidelines/guidelines.htm>

Federal Emergency Management Administration (FEMA); *Emergency Management Guide for Business and Industry*; FEMA Document 141, October 1993; Washington, D.C.; <http://www.fema.gov/pdf/business/guide/bizindst.pdf>

Federal Emergency Management Administration (FEMA), *Standard Checklist Criteria for Business Recovery*; October 1993; Washington, D.C., <http://www.fema.gov/business/bc3.shtm>.  
See also, *Purpose of Standard Checklist Criteria for Business Recovery*; <http://www.fema.gov/business/bc.shtm>

National Fire Prevention Association (NFPA); *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2004 Edition*; <http://www.nfpa.org/assets/files/PDF/NFPA1600.pdf>

NERC; Standard CIP-009-1; Cyber Security – Recovery Plans for Critical Cyber Assets; Effective June 1, 2006  
[http://www.nerc.com/~filez/standards/Reliability\\_Standards.html#Critical\\_Infrastructure\\_Protection](http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection)

NERC; Security Guidelines for the Electricity Sector; <http://esisac.com/library.htm>:

- Guideline Overview
- Vulnerability and Threat Assessment
- Threat Response
- Emergency Plans
- Communications
- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information
- Threat Alert Levels and Physical Response Guidelines
- Threat Alert Levels and Cyber Response Guidelines
- An Approach to Action for the Electricity Sector

# Continuity of Operations Security Guideline

## Version 2.0: Effective July 1, 2007

National Strategy for Pandemic Influenza; The White House, U.S. Government; Homeland Security Council; November 2005; <http://www.whitehouse.gov/homeland/nspi.pdf>

Electricity Sector – Influenza Pandemic – Planning, Preparation, and Response Reference Guide; North American Electric Reliability Council; Princeton, NJ; <http://esisac.com/publicdocs/Influenza%20Pandemic%20Reference%20Guide.pdf>

### Revision History

Effective Date	Version Number	Reason/Comments
6/14/2002	1.0	Initial Version – <i>Continuity of Business Processes Security Guideline</i>
7/1/2007	2.0	Title and content revised to <i>Continuity of Business Operations Security Guideline</i> . Extensive updates and edits to make the text current and to incorporate the 2006 CIPC approved format for all guidelines.

NOTE: This Continuity of Operations Security Guideline will remain in effect until it is either changed or rescinded by NERC. The guideline will be reviewed:

- ...following any significant change in the Electricity Sector that warrants review and updating of this guideline, or
- ...three years following the guideline’s Effective Date.

### Endnotes

1. “Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery,” Copyright (c) 2004 by ASIS International. Used by permission. The complete guideline is available from ASIS International, 1625 Prince Street, Alexandria, Virginia 22314  
<http://www.asisonline.org/guidelines/guidelines.htm>.

2. “Glossary of Terms Used in Reliability Standards;” NERC; May 2, 2006;  
[ftp://www.nerc.com/pub/sys/all\\_updl/standards/rs/Glossary\\_02May06.pdf](ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Glossary_02May06.pdf)

3. Definition summarized from numerous sources. The central definition is that obtained from the US Center for Disease Control: “Pandemic: The worldwide outbreak of a disease in humans in numbers clearly in excess of normal.”  
<http://www.pandemicflu.gov/glossary/#P>