

Security Guidelines for the Electricity Sector Continuity of Business Processes

NERC	Guideline
Guideline Title: Continuity of Business Processes	Version: 1.0
Revision Date:	Effective Date: June 14, 2002

Purpose:

In the event of an incident, business continuity plans help reduce the impact of significant market or system interruptions and ensure prompt resumption of business and 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 company.

Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, 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.

Guideline Statement:

This guideline recommends “best practices” for the electricity infrastructure in the area of “Continuity of Business Processes” for facilities and functions considered critical.

Table of Contents:

Guideline Detail:

While companies in the electricity sector traditionally have extensive plans in place for the restoration of service in response to natural disasters such as

Security Guidelines for the Electricity Sector Continuity of Business Processes

earthquakes, floods, and other weather-related emergencies, they also need to ensure they have business recovery plans in place in the event a disaster impacts their strategic business locations — fire or evacuation due to an industrial accident.

As a matter of general principle, many companies in the electricity sector that own or operate critical facilities have plans for relocating critical operations such as their Grid Control Center, Data Center, Customer Call Center, and other key operating facilities. It is good practice to locate alternate facilities for these functions sufficiently distant from the primary location to ensure rapid continuity of operations.

Alternate facilities do not have to mirror the primary facility but they should be able to maintain critical operations at some minimal level until the primary facility is restored.

In addition, the company should consider its vulnerabilities and its need to recover key financial, information technology, and business systems, which are typically located in, or close to, the company headquarters facility. Examples include the following:

- Accounts Payable and Receivable
- Payroll
- Financial Transactions
- Acquisition of Services and Materials
- Delivery Services
- Energy Trading and Settlement
- Stock Transfer and Investor Record Management
- Banking
- Other key financial support functions such as Tax, Insurance etc.

Each company should consider developing a business recovery plan that identifies the key functions that may need to be relocated, an alternate work location for each critical function, and the resources needed to ensure their continued operation at a minimum acceptable level.

Security Guidelines for the Electricity Sector Continuity of Business Processes

The following are important considerations when siting alternate locations:

- Facilities should be outside the immediate area to ensure that the location will not be impacted to the same degree as the primary.
- Facilities should be accessible to personnel or transportation arrangements should be available 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.)
- Facilities should be controlled by the company either through ownership or other arrangements to ensure they will be available during an emergency.
- Facilities should support key infrastructure requirements, particularly voice and data networks, key operating systems, and file storage.
- Facilities where supporting resources can be stored for retrieval.

Business Recovery Plans typically address the following process elements:

- A designated person or department to develop, maintain, and test the business recovery plan.
- Specific emergency plans for individual critical functions that supplement the overall business recovery plan.
- Protocols for the activation of the business recovery plan including facility preparation, systems activation, and relocation of personnel.
- An annual test of the business recovery plan, a review of lessons learned, and revision of the plan as required.
- Training for key personnel to ensure that they are aware of the business recovery plan requirements. An annual exercise provides an excellent opportunity for such training.

Exceptions:

Security Guidelines for the Electricity Sector Continuity of Business Processes

Certified Products/Tools:

Related Documents:

- Security Guidelines for the Electricity Sector: Guideline Overview
- Security Guidelines for the Electricity Sector:
 - Vulnerability and Threat Assessment
 - Threat Response
 - Emergency Plans
 - Communications
 - Physical Security
 - Cyber Security
 - Employment Background Screening
 - Protecting Potentially Sensitive Information
- *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001, <http://www.nerc.com>
- *Threat Alert Levels and Physical Response Guidelines*, NERC, November 2001, <http://www.nerc.com>
- *Threat Alert Levels and Cyber Response Guidelines*, NERC, March 2002, <http://www.nerc.com>

Revision History:

Date	Version Number	Reason/Comments