

Business Continuity and Disaster Recovery

# Overview/ Purpose

Since disasters happen so rarely, many organizations fail to plan in advance their immediate response to a disaster, referred to as a Disaster Recovery Plan, or the resumption and continuation of their operations after a disaster, called Business Continuity Planning. It is important to realize that having a Disaster Recovery/Contingency Plan in the event of a disaster gives a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended disruption in or delay of service should be considered. The Disaster Recovery Plan should be part of the overall Business Continuity Plan.

This policy defines the requirement for a baseline Disaster Recovery Plan to be developed and implemented by <**Utility Name**> that will describe the process to recover IT systems, applications and data from any type of disaster that causes a disruption to business processes or access to critical data and IT services. Additionally, this policy defines a requirement for a Business Continuity plan, which provides guidance for the resumption of normal operations following a disaster.

# Scope

This policy is directed to the **<person or group responsible for the policy>** who are accountable for ensuring that the Business Continuity/Disaster Recovery Plans are developed, tested and kept up-to-date. The purpose of this policy is solely to state the requirement to have Business Continuity/Disaster Recovery Plans; it does not define the specific contents of these plans, or the process for their development.

# Policy

## General Requirements

The following contingency plans, which comprise the overall Business Continuity/Disaster Recovery Plans, must be created to include, at a minimum:

* + 1. Emergency Response Plan: The level of emergency, the process of recovery and how business continues during the emergency are defined.
    2. Chain of Command: Define the order of responsibility when normal staff is unavailable to perform duties.
    3. Data Study: Detail the data stored on the systems, criticality, and level of confidentiality. This should follow the *Data Classification* policy and the *Data Assets Inventory*.
    4. Criticality of Service List: List all the services provided in their order of importance.
    5. Explain the order of recovery in both short-term and long-term timeframes.
    6. Data Backup and Restoration Plan: Detail what data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered. This should follow the *Backup and Recovery* policy.
    7. Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
    8. Mass Media Management: Define the accountability for corporate spokesperson and development of messages for communications to public and consumers.

## Table Top Exercise Requirements

After creating the plans, it is important to practice them to the extent possible. Management, including key staff, should set aside time to test the Disaster Recovery and Business Continuity Plans. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences. The Plans are revised and updated to reflect outcomes of the table top exercises.

## Review Schedule

At a minimum, the plans should be reviewed and updated on an annual basis.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* Adapted from “Cyber Security Policy Framework”  
  (<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)   
  Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.
* Adapted from “Disaster Recovery Plan Policy  
  <http://www.sans.org/security-resources/policies/general/pdf/disaster-recovery-plan-policy>

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **CFO** | **All Employees** |

*Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<I**nsert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |