|  |  |
| --- | --- |
| Title | Business Continuity and Disaster Recovery Policy |
| Version | 0.1 (Internal Review) |
| Scope | ACME Technical and Management Teams |
| Date Approved |  |

# Purpose

This policy outlines ACME's approach to managing business continuity and disaster recovery for critical processes and services to:

* Effectively manage any incident that may cause a business disruption to ACME.
* Provide continuity of critical business processes and services managed by ACME.
* Minimize the potential impact that any business disruption would have on ACME and its reputation.

# Definitions

BIA - Business Impact Analysis (BIA) predicts the consequences of disrupting a business function and process and gathers information needed to develop recovery strategies.

BCP - Business Continuity Planning is concerned with keeping business operations running, perhaps in another location or using alternative tools and processes following a disruption.

DRP - Disaster Recovery Planning is concerned with restoring normal business operations after a disaster.

RTO - RTO refers to the maximum amount of time that a business process, system, or application can be down or unavailable after a disruption or disaster before it starts to cause significant damage to the business. It’s essentially the deadline for getting things back up and running to avoid serious consequences.

RPO - RPO represents the maximum amount of data that your business can afford to lose during a disruption or disaster, measured in time. It answers the question, "How much data can we lose and still operate effectively?" The RPO helps determine how frequently data backups should be made.

Tier - A "Tier" is a classification level assigned to systems, applications, or business processes based on their criticality to the organization and the potential impact on the business in the event of their failure or unavailability. Tiers are used to prioritize recovery efforts and resources during a disaster or business disruption. The classification helps to ensure that the most critical systems are recovered first to minimize business impact. ACME recognizes the following tiers of systems within its environment:

|  |  |  |
| --- | --- | --- |
| Tier | Definition | RTO/RPO |
| Tier 1 | Systems or processes that are essential to the core operations of the business. Their failure would cause an immediate and severe impact on the organization, potentially leading to significant financial loss, legal or regulatory penalties, or damage to the organization's reputation. | RTO = 1 hours  RPO = 1 hours |
| Tier 2 | Systems or processes that are very important to the business but can tolerate a short period of downtime without causing severe disruption. While their failure would be problematic, it would not have the same immediate impact as Tier 1 systems. | RTO = 4 hours  RPO = 4 hours |
| Tier 3 | Systems or processes that are important to the business but can withstand longer periods of downtime with manageable impact. These systems are necessary for day-to-day operations but do not directly support mission-critical functions. | RTO = 24 hours  RPO = 24 hours |

# Policy

Business Impact Analysis (BIA)

* ACME shall maintain a Business Impact Analysis (BIA) Process, which will be exercised periodically based on material changes to essential business technologies.
* The BIA process will quantify the impact of business process unavailability, expressed in terms of Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO). The output of this activity should be used to determine business continuity priorities and requirements. At a minimum, the following should be considered in the business impact analysis exercise:
* The BIA will determine which systems are essential to a given business process.
* Systems will inherit its ‘Tier’ from the most critical business process it supports. For instance, if a database server ‘mssql01’ supports business process ‘a’, which is a Tier 3 process, and business process ‘b’, which, is a Tier 1 process, ‘mssql01’ will be classified as a ‘Tier 1’ system.
* The BIA will include a ‘System Risk Analysis’ to evaluate cyber and operational risks, producing a risk score for each system categorized as Tier 3 or lower.
* The BIA will map the minimum acceptable standards for each category of risk mitigation strategy on a per-tier basis. For example, determining that implementing ‘highly available systems’ is a requirement for a system integral to a Tier 1 business process.
* Systems within a given tier, that have risk scores that indicate a failure to meet the requirements of that tier will be put on a remediation plan.

Business Continuity Planning (BCP)

* ACME shall maintain a Business Continuity (BCP) that is informed by the BIA.
* ACME will exercise backup validation exercises according to a yearly calendar that systematically verify that the RPO and RTO of critical business processes are, in fact, attainable.
* The BCP will address disruptions affecting day-to-day operations without compromising infrastructure integrity.
* Contracts with essential third-party suppliers will be assessed based on their impact on ACME' BCP with an eye toward ensuring they meet our dependency requirements.
* All management personnel and employees shall be made aware of the business continuity plans and their roles and responsibilities in achieving the defined continuity objectives.
* ACME will conduct a ‘tabletop exercise’ yearly to ensure that all stakeholders in the process understand their roles and are prepared to fill them.
* The business continuity plan shall be reviewed periodically to ensure it remains relevant.
* The BCP will include communication strategies that include both employees and third parties.
* The BCP will include recovery strategies that address the entire product lifecycle of our essential products and services.
* The BCP will include requirements for periodic exercise of the plan to validate expected outcomes.

Disaster Recovery Planning (DRP)

* ACME shall maintain a Disaster Recovery Plan (DRP) that is informed by the BIA.
* The DRP covers significant events affecting major parts of our operations, infrastructure, or data. Examples include natural disasters, major cyber-attacks, or significant hardware failures. The DRP focuses on the recovery and restoration of IT systems, applications, and data to ensure the organization can continue its critical operations. The activation of the DRP signifies a situation beyond normal contingencies and requires a coordinated and extensive response to restore services.
* Contracts with essential third-party suppliers will be assessed based on their impact on ACME's DRP with an eye toward ensuring they meet our dependency requirements.
* All management personnel and employees shall be made aware of the DRP and their roles and responsibilities in achieving the defined recovery objectives.
* The DRP shall be reviewed periodically to ensure it remains relevant.
* The DRP will include communication strategies that include both employees and third parties.
* The DRP will include recovery strategies that address the entire product lifecycle of our essential products and services.
* The DRP will include requirements for periodic exercise of the plan to validate expected outcomes.