Business Continuity Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Business continuity ensures that ABC Company can continue to provide services during business disruptions. The emphasis for business continuity is on critical business processes that need to be recovered in the event of a disaster.

Business continuity plans are no longer a luxury, but an essential element of ABC Company’s risk management program. The decision to invest in business continuity is required by legislation, third parties (e.g., insurers), and the realistic view that management must minimize the impact of a disaster on business operations.

# II. Purpose

The purpose of this policy is to protect ABC Company’s Information Resources and its ability to continue business operations in the event of a disaster or component failure. Business continuity requires management to identify risks and install the appropriate mitigating technologies.

An up-to-date business continuity plan creates a competitive advantage out of its ability to respond to rapid changes in its environment. With an effective plan, ABC Company can move from simple recovery to experiencing the benefits associated with the continuing of business operations that are in line with the corporate strategy of facilitating growth and profitability.

# III. Scope

This policy applies to all Staff that are responsible for continuing ABC Company’s business operations.

# IV. Policy

The Chief Security Officer shall ensure:

* The organization has established, and implemented as needed, procedures to restore any loss of sensitive data stored electronically.
* A disaster recovery plan address issues specific to the operating environment.
* A disaster recovery plan addresses the data that is to be restored.
* A copy of the disaster recovery plan is readily accessible at more than one location.
* The organization has established, and implemented as needed, procedures to enable continuation of critical business processes and for protection of sensitive information while operating in the emergency mode.
* The disaster recovery plan balances the need to access the data with the need to protect the data.
* The disaster recovery plan identifies alternate security measures to protect sensitive information.
* The disaster recovery plan includes contact information for all persons that need to be notified in the event of a disaster, as well as roles and responsibilities of staff involved in the restoration process.
* Procedures for periodic testing and revision of contingency plans.
* Those responsible for performing contingency planning tasks understand their responsibilities.
* Staff performs tests of their procedures. The results of each test is documented and retained for audit purposes. The recovery plans are updated as a result of the tests.
* The organization assesses the relative criticality of specific applications and data in support of other contingency plan components.
* A Business Impact Analysis (BIA) formally documents risks and impact to the organization. The disaster recovery plan adequately mitigates business disruption risks.
* The organization has established, and implemented as needed, procedures that allow facility access in support of restoration of lost data under disaster recovery and emergency mode operations. Procedures allow facility access while restoring lost data. Procedures identify personnel that are allowed to re-enter a facility to perform data restoration. Procedures are also addressed in the organization’s disaster recovery plan.
* Procedures for obtaining necessary sensitive information during an emergency. Procedures specify the staff members authorized to access sensitive information during an emergency.

ABC Company shall develop and maintain a comprehensive Business Continuity Plan (Plan). This Plan encompasses both IT contingency planning as well as Company’s corporate office business unit contingency planning. This is not an IT-only undertaking and must cross all business functions and departments.

Company’s risk assessment and Business Impact Analysis (BIA) provide the foundation for business continuity planning. The Business Continuity Plan should cover all essential and critical business activities. The Business Continuity Plan shall consist of:

* Business Resumption Plan – plan to resume business operations including logistics and steps to minimize risks.
* Disaster Recovery Plan - the technical aspect of business continuity planning; the advance planning and preparing necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster.
* Communications Plan – the plan to communicate with employees, vendors, consultants, customers, service providers, and the media with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate.

Business continuity teams shall include a minimum of the following:

* Readiness Team – maintains this Plan and manages business continuity activities
* Emergency Action Operations Team - initiates recovery efforts
* Emergency Action Applications Team - identifies data to be recreated
* Emergency Action Hardware Team - assesses damage, recommends alternatives
* Emergency Action Facilities Team – assesses facilities, repair or new offices
* Emergency Action Administrative Assistance Team

The Business Continuity Plan shall be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed. The Business Continuity Plan shall be tested at least annually and more frequently when changes in business processes or equipment necessitate a test.

The Business Continuity Plan shall be kept up-to-date to take into account changing circumstances. All staff must be made aware of the Business Continuity Plan and their roles.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to Staff responsible for ensuring and restoring business operations.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM03.02, APO09.05, BAI04.05, BAI04.07, DSS01.05, DSS03.05, MEA01.05

GDPR Article 25, 32

HIPAA 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E)

ISO 27001 A.12.3, A.17

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 AU-5, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-9, CP-10

NIST Cybersecurity Framework PR.IP-9, PR.IP-10, DE.DP-2, RS.RP-1, RC.RP-1, RC.CO-1

PCI 12.10