Business Continuity and Disaster Recovery Plan

Purpose

The purpose of this Business Continuity and Disaster Recovery Plan is to establish guidelines and procedures for maintaining critical business operations during disruptive events and to ensure the timely recovery of essential functions following a disaster. This plan aims to minimize operational downtime, protect organizational assets, and safeguard the interests of our stakeholders.

Scope

This policy applies to:

- All employees, contractors, and temporary staff
- All departments and business units within the organization
- All critical business processes, systems, and data
- All physical locations and remote work environments
- Third-party vendors and service providers critical to business operations

Definitions

Term	**Definition**
Business Continuity	The capability of an organization to continue the delivery of products or services at acceptable predefined levels following a disruptive incident
Disaster Recovery	The process of restoring systems, data, and infrastructure following a catastrophic event
Recovery Time Objective (RTO)	The targeted duration of time within which a business process must be restored after a disaster to avoid unacceptable consequences
Recovery Point Objective (RPO)	The maximum targeted period in which data might be lost due to a major incident

Term	Definition
Business Impact Analysis (BIA)	A systematic process to determine and evaluate the potential effects of an interruption to critical business operations
Critical Systems	IT systems and applications that are essential for the continuity of key business operations

Policy Section

Roles and Responsibilities

The Business Continuity Management Team (BCMT) shall be responsible for:

- Developing, maintaining, and implementing this plan
- Conducting regular risk assessments and business impact analyses
- Coordinating testing and exercises of the plan
- Reviewing and updating the plan annually or after significant organizational changes

Department heads shall:

- Identify critical processes and resources within their departments
- Participate in business impact analyses and risk assessments
- Ensure their staff are trained on business continuity procedures

All employees shall:

- Familiarize themselves with this plan and their roles during a disruption
- Participate in training and exercises as required
- Report any potential threats or incidents that may impact business continuity

Plan Activation

The BCMT shall determine when to activate this plan based on the severity and potential impact of an incident.

Activation criteria shall include, but are not limited to:

- Prolonged power outages
- Natural disasters
- Cyber attacks
- Pandemic or public health emergencies

- Critical infrastructure failures

The plan shall be activated through a formal declaration by the BCMT, followed by immediate notification to all relevant stakeholders.

Data Backup and Recovery

IT shall implement and maintain a robust data backup system that includes:

- Regular backups of all critical data and systems
- Off-site storage of backup media
- Encryption of backup data in transit and at rest
- Regular testing of data restoration procedures

Backup schedules and retention periods shall be defined based on the criticality of data and regulatory requirements.

Alternate Work Locations

The organization shall maintain alternate work locations or remote work capabilities to ensure business continuity during facility disruptions.

Criteria for selecting and equipping alternate work locations shall include:

- Adequate space and infrastructure to support critical operations
- Secure access to necessary systems and data
- Communication capabilities with stakeholders

Vendor Management

Critical vendors and service providers shall be required to:

- Provide their own business continuity and disaster recovery plans
- Participate in joint testing exercises when appropriate
- Meet specified recovery time and point objectives

The organization shall maintain an up-to-date list of alternative vendors for critical services.

Training and Awareness

All employees shall receive annual training on:

- The contents of this plan
- Their roles and responsibilities during a disruption

- Emergency response procedures

The BCMT shall conduct awareness campaigns to reinforce the importance of business continuity preparedness.

Plan Maintenance

This plan shall be reviewed and updated annually or after significant organizational changes.

All updates to the plan shall be documented and communicated to relevant stakeholders.

The BCMT shall maintain version control of this plan and ensure that only the most current version is in use.

Business Impact Analysis

The Business Impact Analysis (BIA) process shall:

Identify critical business functions and processes Determine the impact of disruptions on these functions over time Establish recovery time objectives (RTOs) and recovery point objectives (RPOs) Identify resource requirements for recovery

The BCMT shall conduct a BIA annually and after significant organizational changes.

Critical Systems and Services

Based on the BIA, the following systems and services have been identified as critical:

Enterprise Resource Planning (ERP) system Customer Relationship Management (CRM) system Email and communication platforms Financial management systems Data storage and backup systems Network infrastructure and security systems

Each critical system shall have a designated owner responsible for its recovery.

Recovery Time Objectives

Recovery Time Objectives (RTOs) for critical systems and services:

System/Service	**RTO**
ERP System	4 hours
CRM System	6 hours

System/Service	RTO
Email and Communication	2 hours
Financial Management Systems	8 hours
Data Storage and Backup	4 hours
Network Infrastructure	2 hours

Recovery Point Objectives

Recovery Point Objectives (RPOs) for critical data:

Data Type	RPO
Financial Data	15 minutes
Customer Data	1 hour
Operational Data	2 hours
Email Data	4 hours

Emergency Response Procedures

Assess the situation and declare an emergency if necessary Notify the BCMT and activate the plan if required Ensure the safety and security of personnel Implement immediate response actions to mitigate damage Activate the crisis communication plan Begin recovery procedures for affected systems and services

Detailed emergency response procedures for specific scenarios (e.g., fire, cyber attack) shall be maintained as appendices to this plan.

Recovery Strategies

IT Systems:

- Utilize redundant systems and failover capabilities
- Implement cloud-based recovery solutions
- Restore from backups in order of criticality

Facilities:

- Activate alternate work locations or remote work protocols
- Implement temporary relocation procedures if necessary

Personnel:

- Cross-train employees for critical functions
- Maintain a pool of pre-screened temporary staff

Data:

- Restore from off-site backups
- Implement data replication and synchronization procedures

Testing and Exercises

Conduct annual full-scale exercises simulating various disaster scenarios Perform quarterly tabletop exercises for specific components of the plan Test backup and recovery procedures monthly Conduct unannounced drills to assess readiness

All tests and exercises shall be documented, and lessons learned shall be incorporated into plan updates.

Communication Plan

Maintain up-to-date contact information for all employees, key stakeholders, and vendors Establish a crisis communication team responsible for internal and external communications Utilize multiple communication channels (e.g., email, SMS, phone) to ensure message delivery Develop pre-approved message templates for various scenarios Establish a process for regular status updates during an incident Designate spokespersons for media communications

The communication plan shall be tested regularly as part of the overall business continuity exercises.Here's the continuation of the policy document with the requested sections:

Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment. The severity of the disciplinary action will be determined based on the nature and impact of the violation. All employees are required to report any suspected violations of this policy to their immediate supervisor or the Information Security team. The organization reserves the right to monitor, audit, and investigate any activities related to this policy to ensure compliance.

Roles and Responsibilities

The Business Continuity Management Team (BCMT) is responsible for developing, maintaining, and implementing this plan, as well as conducting regular risk assessments and business impact analyses. They will coordinate testing and exercises of the plan and review and update it annually or after significant organizational changes. Department heads are tasked with identifying critical processes and resources within their departments, participating in business impact analyses and risk assessments, and ensuring their staff are trained on business continuity procedures. All employees are expected to familiarize themselves with this plan and their roles during a disruption, participate in required training and exercises, and report any potential threats or incidents that may impact business continuity.

Revision History

Version	Date	Author	Changes

Approval

Name	Title	Date	Signature