Business Continuity Policy Template

Document Control Information

- **Document Title:** Business Continuity Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Business Continuity Policy establishes [ORGANIZATION NAME]'s approach to ensuring the continuity of critical business functions during and after disruptive incidents in accordance with ISO 27001:2022 requirements. It provides a framework for developing, implementing, and maintaining effective business continuity plans to minimize the impact of disruptions and ensure timely recovery.

1.2 Scope

This policy applies to: - All business functions, processes, and services of [ORGANIZATION NAME] - All information systems and technology infrastructure supporting critical business functions - All facilities and physical locations where the organization operates - All employees, contractors, consultants, and third parties involved in business operations - All situations that could disrupt normal business operations

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Identifying and protecting critical business functions and supporting resources - Developing and maintaining effective business continuity plans - Minimizing the impact of disruptive incidents on operations, stakeholders, and reputation - Ensuring timely and orderly recovery of business operations following disruptions - Complying with legal, regulatory, and contractual business continuity requirements - Continuously improving business continuity capabilities through regular testing and review

2. Business Continuity Management Framework

2.1 Governance Structure

- A Business Continuity Management (BCM) program shall be established
- Executive management shall provide leadership and commitment to the BCM program
- A Business Continuity Manager/Coordinator shall be appointed
- Business continuity roles and responsibilities shall be defined and documented
- A Business Continuity Steering Committee shall oversee the BCM program
- Business unit representatives shall be appointed as Business Continuity Coordinators

2.2 Business Continuity Lifecycle

The BCM program shall follow a continuous lifecycle approach: 1. Program Management 2. Business Impact Analysis and Risk Assessment 3. Business Continuity Strategy Development 4. Business Continuity Plan Development 5. Testing and Exercises 6. Training and Awareness 7. Maintenance and Review 8. Continuous Improvement

2.3 Integration with Other Management Systems

The BCM program shall be integrated with: - Information Security Management System - Risk Management Framework - Incident Management System - Crisis Management Framework - Disaster Recovery Program - Emergency Response Procedures

3. Business Impact Analysis and Risk Assessment

3.1 Business Impact Analysis (BIA)

- A BIA shall be conducted to identify critical business functions
- The BIA shall determine:
  - Maximum Tolerable Period of Disruption (MTPD)
  - Recovery Time Objectives (RTO)
  - Recovery Point Objectives (RPO)
  - Minimum resource requirements for critical functions
  - Dependencies between functions, systems, and third parties
- The BIA shall be reviewed annually and after significant organizational changes

3.2 Risk Assessment

- Business continuity risks shall be identified and assessed
- Risk assessment shall consider:
    - Threats that could cause business disruption
    - Vulnerabilities that could be exploited
    - Potential impact on business operations
    - Likelihood of occurrence
    - Existing controls and their effectiveness
- Risk assessment results shall inform business continuity strategies
- Risk assessments shall be reviewed annually and after significant changes

3.3 Criticality Classification

Business functions shall be classified based on criticality: - **Critical**: Functions that must be recovered immediately (within hours) - **Essential**: Functions that must be recovered within 24-72 hours - **Important**: Functions that must be recovered within one week - **Non-critical**: Functions that can be delayed for more than one week

4. Business Continuity Strategies

4.1 Strategy Development

- Business continuity strategies shall be developed for:
    - People and skills
    - Premises and work environment
    - Technology and systems
    - Information and data
    - Suppliers and third-party services
    - Stakeholder communications
- Strategies shall be aligned with RTOs and RPOs
- Multiple strategy options shall be considered
- Cost-benefit analysis shall be conducted for strategy options
- Selected strategies shall be documented and approved

4.2 Resource Requirements

- Resource requirements for implementing strategies shall be identified
- Resources shall include:
    - Personnel with required skills
    - Alternative work locations
    - IT systems and infrastructure
    - Data backup and recovery capabilities

  - Equipment and supplies
  - Documentation and records
  - Financial resources
- Resource gaps shall be addressed through appropriate actions

4.3 Technology Recovery

- Technology recovery strategies shall be developed for:
  - Critical IT systems and applications
  - Networks and telecommunications
  - Data centers and infrastructure
  - End-user computing devices
  - Data backup and restoration
- Technology recovery strategies shall be aligned with business RTOs and RPOs
- Technology dependencies shall be identified and addressed
- Recovery capabilities shall be tested regularly

5. Business Continuity Plans

5.1 Plan Development

- Business continuity plans shall be developed for critical business functions
- Plans shall be based on approved strategies
- Plans shall be documented in a clear, concise, and accessible format
- Plans shall include:
  - Scope and objectives
  - Roles and responsibilities
  - Activation criteria and procedures
  - Emergency response procedures
  - Communication procedures
  - Recovery procedures
  - Return to normal operations
- Plans shall be approved by relevant management

5.2 Plan Components

5.2.1 Crisis Management Plan

- Procedures for managing crisis situations
- Crisis management team structure and responsibilities
- Decision-making authority and escalation procedures
- Crisis communication protocols
- Stakeholder management

5.2.2 Emergency Response Plan

- Procedures for immediate response to incidents
- Life safety and evacuation procedures
- Emergency contacts and notification procedures
- Damage assessment procedures
- Coordination with external emergency services

5.2.3 Business Recovery Plan

- Procedures for recovering critical business functions
- Alternative processing arrangements
- Resource requirements and allocation
- Recovery tasks, responsibilities, and timeframes
- Dependencies and prerequisites for recovery

5.2.4 IT Disaster Recovery Plan

- Procedures for recovering IT systems and infrastructure
- System recovery priorities and sequences
- Technical recovery procedures
- Data restoration procedures
- Testing and verification procedures

5.3 Plan Documentation

- Plans shall be documented in a standardized format
- Plans shall be clear, concise, and actionable
- Plans shall be accessible during disruptions
- Multiple formats and locations shall be used for plan storage
- Plans shall be protected from unauthorized access
- Plans shall be version controlled

6. Testing and Exercises

6.1 Exercise Program

- A business continuity exercise program shall be established
- Exercises shall be conducted regularly according to a schedule
- Different types of exercises shall be included:
    - Desktop/tabletop exercises
    - Functional exercises
    - Technical tests

    - Full-scale simulations
- Exercise objectives shall be clearly defined
- Exercise scenarios shall be realistic and relevant

6.2 Exercise Planning and Execution

- Exercises shall be properly planned and documented
- Exercise participants shall be briefed on objectives and expectations
- Exercises shall be conducted with minimal disruption to normal operations
- Observers shall be appointed to evaluate exercises
- Exercise results shall be documented and reported

6.3 Post-Exercise Activities

- Debriefing sessions shall be conducted after exercises
- Exercise performance shall be evaluated against objectives
- Strengths and weaknesses shall be identified
- Improvement opportunities shall be documented
- Corrective actions shall be implemented
- Business continuity plans shall be updated based on exercise results

7. Training and Awareness

7.1 Training Program

- Business continuity training shall be provided to:
    - Business continuity team members
    - Crisis management team members
    - Recovery team members
    - General staff
- Training shall be appropriate to roles and responsibilities
- Training shall be provided at onboarding and refreshed regularly
- Training effectiveness shall be evaluated
- Training records shall be maintained

7.2 Awareness Program

- Business continuity awareness shall be promoted throughout the organization
- Awareness activities shall include:
    - Communications from senior management
    - Intranet resources and newsletters
    - Posters and visual reminders
    - Awareness sessions and briefings

    - Participation in exercises
- Awareness materials shall be updated regularly
- Awareness effectiveness shall be measured

8. Maintenance and Review

8.1 Plan Maintenance

- Business continuity plans shall be reviewed and updated:
    - At least annually
    - After significant organizational changes
    - After major incidents or exercises
    - When new threats or vulnerabilities are identified
- Changes to plans shall follow change management procedures
- Plan versions shall be controlled and documented
- Obsolete plans shall be archived or destroyed

8.2 Program Review

- The BCM program shall be reviewed regularly
- Reviews shall assess:
    - Program effectiveness and maturity
    - Compliance with policy and standards
    - Achievement of program objectives
    - Resource adequacy
    - Integration with other management systems
- Review results shall be reported to senior management
- Improvement opportunities shall be identified and implemented

9. Incident Response and Activation

9.1 Incident Detection and Assessment

- Procedures shall be established for detecting and assessing incidents
- Criteria shall be defined for activating business continuity plans
- Incidents shall be classified based on severity and potential impact
- Assessment shall consider:
    - Nature and extent of the disruption
    - Affected functions and locations
    - Estimated duration of the disruption
    - Available resources for response and recovery

9.2 Plan Activation

- Authority for plan activation shall be clearly defined
- Activation procedures shall be documented and communicated
- Notification procedures shall ensure timely communication to:
    - Business continuity teams
    - Senior management
    - Affected staff
    - Key stakeholders
- Activation decisions shall be documented

9.3 Response and Recovery Operations

- Response and recovery shall follow established plans
- Operations shall be coordinated through defined command structures
- Regular situation updates shall be provided
- Resource allocation shall be managed effectively
- Progress shall be monitored against recovery objectives
- Decisions and actions shall be documented

10. Communication

10.1 Internal Communication

- Communication procedures shall be established for disruptions
- Multiple communication methods shall be available
- Communication shall be clear, timely, and appropriate
- Regular updates shall be provided to staff
- Feedback mechanisms shall be established
- Communication effectiveness shall be monitored

10.2 External Communication

- Procedures shall be established for communicating with external stakeholders
- External communications shall be approved by authorized personnel
- Consistent messages shall be provided across all channels
- Media inquiries shall be handled according to procedures
- Regulatory notification requirements shall be fulfilled
- Customer and supplier communications shall be prioritized

11. Compliance and Reporting

11.1 Compliance Requirements

- Business continuity activities shall comply with:
    - Legal and regulatory requirements
    - Contractual obligations
    - Industry standards and best practices
    - Organizational policies and standards
- Compliance shall be regularly assessed
- Non-compliance shall be addressed through corrective actions

11.2 Performance Measurement

- Key performance indicators (KPIs) shall be established for the BCM program
- Performance shall be measured and reported regularly
- KPIs shall include:
    - Plan development and maintenance
    - Exercise completion and results
    - Training and awareness effectiveness
    - Incident response performance
    - Recovery time achievement
- Performance trends shall be analyzed

11.3 Management Reporting

- Regular reports shall be provided to senior management
- Reports shall include:
    - Program status and progress
    - Exercise results and lessons learned
    - Incident response performance
    - Risk assessment updates
    - Resource requirements and constraints
    - Improvement recommendations
- Management shall review reports and provide direction

12. Roles and Responsibilities

12.1 Executive Management

- Approve the Business Continuity Policy
- Provide leadership and commitment to business continuity
- Ensure adequate resources for the BCM program

- Review program performance and provide direction
- Participate in crisis management

12.2 Business Continuity Manager/Coordinator

- Develop and maintain the BCM program
- Coordinate business continuity activities
- Facilitate BIA and risk assessment
- Support plan development and maintenance
- Coordinate exercises and training
- Report on program performance

12.3 Business Unit Managers

- Identify critical functions in their areas
- Participate in BIA and risk assessment
- Develop and maintain business continuity plans
- Ensure staff awareness and training
- Participate in exercises
- Implement business continuity strategies

12.4 IT Department

- Develop and maintain IT disaster recovery plans
- Implement technology recovery strategies
- Ensure data backup and recovery capabilities
- Participate in exercises and testing
- Provide technical expertise during recovery
- Maintain IT infrastructure resilience

12.5 All Staff

- Be aware of business continuity procedures
- Participate in training and exercises
- Report incidents that could disrupt operations
- Follow instructions during disruptions
- Provide feedback on business continuity activities

13. Related Documents

- Information Security Policy
- Risk Management Policy
- Incident Management Policy

- Crisis Management Plan
- IT Disaster Recovery Plan
- Emergency Response Procedures
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

14. Approval

This Business Continuity Policy is approved by:

Name: ________________________ Position: ______________________ Date: _________________________ Signature: _____________________