# Contingency Planning Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### **S**ecurity boundary under scope

1. [List of applicable systems]

### References

1. ISO 22301:<https://www.iso.org/standard/75106.html>
2. NIST SP 800-34:<https://www.nist.gov/privacy-framework/nist-sp-800-34>
3. ISO/IEC 27001:2022: A.5.29, A.5.30, A.7.5, A.7.11, A.7.12, A.8.13
4. NIST 800-53 rev. 5: CP-1, CP-2, CP-2(1), CP-3, CP-4, CP-4(1), CP-6, CP-6(1), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-8, CP-8(2), CP-9, CP-9(8), MA-6, PE-11
5. CIS v8: 11.1, 11.2, 11.3, 11.4, 11.5, 17.6
6. PCI DSS 4.0: 9.4.1.1, 9.4.1.2, 12.10.1
7. AIPCA SOC 2 TSC: A1.2, A1.3, CC7.4, CC7.5, CC9.1

## Document ownership

<(Choose from)>

* 1. Policy Owner:
     1. [Owner name] ([Owner email]), [Owner title]
  2. Information Security Officer:
     1. [Information officer name], ([Information officer email]), [Information officer title]
  3. System Owner(s):
     1. [System owner name], ([System owner email]), [System owner title]
  4. Process and Operational Owner(s)
     1. [process owner], ([process owner email]), [process owner title]
  5. System Administrator(s):
     1. [System admin name], ([System admin email]), [System admin title]
  6. Required Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. Information Security Team
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT
  7. Optional Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. Information Security Team
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT

## Purpose

The purpose of the Contingency Planning Policy is to ensure the continuous availability, integrity, and confidentiality of the organization's critical data and systems. This policy aims to provide a comprehensive framework for the backup and recovery of data, supporting business continuity, incident response, and disaster recovery efforts. By implementing this policy, the organization aims to minimize data loss, ensure rapid recovery from disruptions, and maintain compliance with legal and regulatory requirements.

## Scope

This policy applies to all data and information systems within the organization, including but not limited to databases, file systems, applications, and network infrastructure. It covers the processes and procedures for data backup, retention, encryption, and recovery. This policy is applicable to all employees, contractors, and third-party service providers involved in the handling, storage, and protection of organizational data. The scope includes:

* 1. **Data Backup**: Frequency, scope, and procedures for regular data backups.
  2. **Data Handling in Backups**: Retention periods, encryption requirements, and integrity checks.
  3. **Support for Business Continuity and Disaster Recovery**: Integration with business continuity and disaster recovery plans.
  4. **Redundant Systems and Alternative Processing Sites**: Requirements for redundant systems and alternative sites.
  5. **Telecommunication and Power**: Redundancy measures for telecommunication and power supply.
  6. **Testing and Validation**: Regular testing and validation of backup and recovery processes.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], **[owner title]** | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | **Executive Team** | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | **Executive Team** | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], **[Information officer title]** | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner],  **Operational owner title]** |  |
| Information Systems Administrators | **System Administrators** | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], **[HR title]** | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users | **End Users** | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | **[provider type]** | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
  2. Management has reviewed and approved this policy.
  3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
  4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
  2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. Backup: The process of creating a copy of data to ensure that it can be recovered in the event of primary data failure or loss.
  2. Incremental Backup: A type of backup that only copies data that has changed since the last backup operation, reducing storage requirements and backup time.
  3. Full Backup: A comprehensive backup method that copies all selected data, regardless of whether it has changed since the last backup.
  4. Archive Backup: A backup that is preserved for an extended period, typically for compliance, historical, or long-term data retention purposes.
  5. Data Retention: Policies and processes related to how long backup data is stored before it is deleted or archived.
  6. Data Encryption: The process of converting data into a code to prevent unauthorized access, ensuring data confidentiality during storage and transmission.
  7. Business Continuity Plan (BCP): A strategy outlining how a business will continue operating during an unplanned disruption in service.
  8. Incident Response: The approach taken by an organization to prepare for, detect, contain, and recover from a data breach or cyberattack.
  9. Disaster Recovery Plan (DRP): A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
  10. Redundant Systems: Additional or duplicate systems that are available to take over operations if the primary systems fail.
  11. Alternative Processing Site: A secondary location where business operations can be resumed in the event that the primary site is compromised.
  12. Telecommunication Redundancy: The implementation of multiple, independent communication paths to ensure continuous connectivity if one path fails.
  13. Uninterruptible Power Supply (UPS): A device that provides emergency power to a load when the input power source fails.
  14. Backup Generator: A standby electrical system that provides power in the event of a main power outage.
  15. Simulation Drill: An exercise that tests the effectiveness of backup, recovery, and business continuity plans by simulating a disruption.
  16. Data Integrity: The accuracy and consistency of stored data, ensuring it remains unchanged during transfer, storage, and retrieval.
  17. Data Recovery: The process of restoring data from a backup to its original or functional state following data loss or corruption.
  18. Recovery Point Objective (RPO): The maximum acceptable amount of data loss measured in time, defining the interval of time that might pass during a disruption before the amount of data lost during that period exceeds the maximum allowable threshold.
  19. Recovery Time Objective (RTO): The targeted duration of time within which a business process must be restored after a disruption to avoid unacceptable consequences.

## Policy

#### Backup of Data

* + 1. The [responsible party] shall ensure that all critical data is backed up on a regular basis. This includes:
       1. Daily incremental backups.
       2. Weekly full backups.
       3. Monthly archive backups.
    2. The backup process shall cover all essential business data, including databases, file systems, and application data to ensure comprehensive data recovery capabilities.

#### Data Handling in Backups

* + 1. The [responsible party] is required to retain backups for a period of seven years to comply with legal, regulatory, and business requirements.
    2. All backup data must be encrypted using industry-standard encryption techniques both in transit and at rest to protect against unauthorized access.
    3. Backup data shall be verified for integrity and completeness through regular checksum validation processes.

#### Support for Business Continuity, Incident Response, and Disaster Response Plans

* + 1. The [responsible party] shall integrate backup processes with the organization's Business Continuity Plan to ensure rapid recovery of critical operations.
    2. Backups must be readily accessible to support incident response efforts, enabling the restoration of affected systems and data.
    3. The backup strategy must align with the Disaster Recovery Plan (DRP), ensuring that backup data can be used to restore systems in case of a catastrophic event.

#### Redundant and/or Alternative Processing

* + 1. The [responsible party] is required to maintain redundant systems and backup sites to ensure continuous availability of critical services in case of primary system failure.
    2. An alternative processing site must be established and maintained to take over operations if the primary site becomes unavailable.

#### Telecommunication and Power

* + 1. The [responsible party] shall implement redundant telecommunication links to ensure uninterrupted data transfer and communication capabilities during backup operations.
    2. Critical backup systems and sites must have uninterruptible power supplies (UPS) and backup generators to prevent data loss during power outages.

#### Testing of Backups and Redundant Systems

* + 1. The [responsible party] is required to perform annual testing of backup and restore procedures to ensure data can be accurately and completely restored.
    2. Periodic simulation drills must be conducted to test the effectiveness of redundant systems and alternative processing sites in supporting business continuity and disaster recovery.
    3. All backup and recovery tests must be documented, and the results reviewed to identify and address any weaknesses in the backup strategy.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
  2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
  3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
     1. Policies
     2. Procedures
     3. Standards
     4. Documentation
     5. Regulations
     6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
  2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
     1. The Information Security Officer
     2. Officer of the [Organization name] Leadership Team
  3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |