ICT Readiness for Business Continuity Policy & Procedure

DOCUMENT CLASSIFICATION	Internal
VERISON	1.0
DATE	
DOCUMENT AUTHOR	Ayaz Sabir
DOCUMENT OWNER	

REVISION HISTORY

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

DISTRIBUTION LIST

NAME	SUMMARY OF CHANGE

APPROVAL

NAME	POSITION	SIGN

Contents

1. Introduction

This ICT Readiness for Business Continuity Policy outlines the framework for establishing, implementing, maintaining, and continually improving the Information and Communication Technology (ICT) readiness for business continuity within. This policy aligns with the requirements of ISO/IEC 27001:2022, specifically addressing Annex A Control 5.30, which mandates that ICT readiness shall be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.

2. Purpose

The primary purpose of this policy is to ensure the availability, integrity, and confidentiality of critical ICT systems and services that support the organization's essential business functions during and after disruptive events. By proactively preparing our ICT infrastructure, **[organization name]** aims to:

- Minimize the impact of disruptions on critical business operations.
- Ensure timely recovery of ICT services to meet defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Maintain information security during periods of disruption.
- Comply with relevant regulatory, legal, and contractual obligations, including ISO/IEC 27001:2022.
- Enhance overall organizational resilience.

3. Scope

This policy applies to all ICT systems, services, infrastructure, applications, and data that are critical to the continued operation of **[organization name]**business functions. It covers all personnel, including employees, contractors, and third-party service providers, who are involved in the planning, implementation, maintenance, testing, and activation of ICT continuity measures. This includes both on-premises and cloud-based ICT assets.

4. Policy Statement

[organization name]is committed to ensuring the continuous availability and resilience of its critical ICT systems and services to support business continuity. ICT readiness for business continuity will be integrated into the overall Business Continuity Management System (BCMS) and will be regularly reviewed, tested, and updated to adapt to changing business requirements and threat landscapes. This commitment is integral to our Information Security Management System (ISMS) as defined by ISO/IEC 27001:2022.

5. Roles and Responsibilities

Effective ICT readiness for business continuity requires clear roles and responsibilities across various organizational functions. The following outlines key roles and their associated responsibilities:

5.1 Information Security Officer (ISO)

- **Overall Responsibility:** Oversees the ICT readiness for business continuity program, ensuring its alignment with the organization's information security strategy and ISO 27001:2022 requirements.

- **Policy Enforcement:** Ensures adherence to this policy and related procedures.
- **Reporting:** Reports on the effectiveness of the ICT readiness program to top management.

5.2 Business Continuity Management (BCM) Team/Coordinator

- **Overall BCMS:** Manages the overarching Business Continuity Management System (BCMS).
- **BIA Oversight:** Oversees the Business Impact Analysis (BIA) process to identify critical business functions and their associated ICT requirements.
- **Plan Integration:** Ensures ICT continuity plans are integrated with overall business continuity plans.
- **Testing Coordination:** Coordinates testing and exercising business continuity plans, including ICT components.

5.3 ICT Department/IT Operation

- **ICT Continuity Planning:** Develops, implements, and maintains ICT continuity plans and procedures.
- **Infrastructure Resilience:** Ensures the resilience and recoverability of critical ICT infrastructure, systems, and applications.
- **Backup and Recovery:** Manages and tests backup and recovery procedures for all critical data and systems.
- **Disaster Recovery Site Management:** Manages and maintains disaster recovery sites and associated infrastructure
- **Incident Response:** Participates in incident response activities related to ICT disruptions.
- **Technical Testing:** Conducts technical testing of ICT recovery capabilities.

5.4 Data Owners

- **Data Classification:** Classifies data based on its criticality and sensitivity, informing RPOs and RTOs.

- **Recovery Requirements:** Defines recovery requirements for their data and associated ICT services.

5.5 All Employees

- **Awareness:** Understands their role in business continuity and ICT readiness plans.
- **Reporting:** Reports on any potential threats or incidents that could impact ICT systems and business continuity.

6. Business Impact Analysis (BIA) and Risk Assessment

[organization name] will conduct regular Business Impact Analysis (BIA) and risk assessments to identify critical business functions, their dependencies on ICT systems, and the potential impact of disruptions. This forms the foundation for defining ICT continuity requirements and developing effective recovery strategies, aligning with ISO 27001:2022 principles.

6.1 Business Impact Analysis (BIA)

The BIA process will identify and prioritize critical business functions and processes, determining the maximum tolerable period of disruption (MTPD) for each. For each critical function, the BIA will:

- **Identify Critical ICT Dependencies:** Map critical business functions to the underlying ICT systems, applications, infrastructure, and data they rely upon.
- **Determine Recovery Time Objectives (RTOs):** Establish the maximum acceptable downtime for each critical ICT system and service. The RTO defines the target time for restoration after a disruption.

- **Determine Recovery Point Objectives (RPOs):** Define the maximum acceptable data loss for each critical ICT system and service. The RPO specifies the point in time to which data must be recovered.
- **Assessing the Impact of Disruption:** Quantify the financial, operational, reputational, and legal/regulatory impacts of ICT system unavailability over time.

6.1.1 BIA Procedure

The BIA procedure will involve the following steps:

1. **Initiation and Planning:** Define the scope of the BIA, identify key stakeholders, and establish a timeline and resources for the assessment.
2. **Data Collection:** Gather information on business processes, their dependencies, resource requirements (people, technology, facilities, information), and the impact of their disruption. This will involve interviews with departmental heads, process owners, and subject matter experts.
3. **Impact Analysis:** Quantify the potential financial, operational, reputational, and legal/regulatory impacts of disruptions over time. This includes direct losses (e.g., lost revenue, increased expenses) and indirect losses (e.g., damage to brand, regulatory fines).
4. **Dependency Mapping:** Create detailed maps illustrating the interdependence between business processes and critical ICT systems, applications, and data. This helps identify single points of failure.
5. **RTO and RPO Determination:** Based on the impact analysis, define the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each critical business function and its supporting ICT assets. These objectives will be formally approved by relevant business owners and IT management.
6. **Report Generation:** Document the findings of the BIA in a comprehensive report, including identified critical functions, their MTPDs, RTOs, RPOs, and associated impacts.

7. **Review and Approval:** The BIA report will be reviewed by the BCM Team, IT management, and senior leadership, and formally approved.

8. **Regular Review:** The BIA will be reviewed and updated at least annually, or whenever significant changes occur in business processes, ICT infrastructure, or the organizational risk profile.

6.2 Risk Assessment

Comprehensive risk assessments will be conducted to identify, analyze, and evaluate potential threats and vulnerabilities to critical ICT systems and services that could lead to disruptions. This includes:

- **Threat Identification:** Identifying potential threats such as natural disasters, cyberattacks, hardware failures, software errors, human errors, and supply chain disruptions.

- **Vulnerability Identification:** Identifying weaknesses in ICT systems, processes, and controls that could be exploited by threats.

- **Risk Analysis:** Assessing the likelihood of threats exploiting vulnerabilities and the potential impact of such events on critical ICT systems and business functions.

- **Risk Evaluation:** Prioritizing risks based on their assessed likelihood and impact, guiding the development of appropriate risk treatment plans.

6.2.1 Risk Assessment Procedure

The risk assessment procedure for ICT readiness will follow these steps:

1. **Asset Identification:** Identify all critical ICT assets (hardware, software, data, networks, facilities) that support the prioritized business functions identified in the BIA

2. **Threat Identification:** Identify potential threats relevant to the identified ICT assets. This includes natural disasters, technical failures, human errors, and

malicious acts (e.g., cyberattacks, insider threats).

3. **Vulnerability Identification:** Identify weaknesses in the ICT assets, systems, and processes that could be exploited by the identified threats. This may involve security assessments, penetration testing, and review of past incidents.
4. **Risk Analysis:** For each identified risk, assess the likelihood of the threat exploiting the vulnerability and the potential impact on the confidentiality, integrity, and availability of information and ICT services. A qualitative or quantitative risk matrix will be used for this assessment.
5. **Risk Evaluation:** Compare the assessed risk levels against the organization's risk acceptance criteria. Risks exceeding the acceptable threshold will require treatment.
6. **Risk Treatment Identification:** Identify and evaluate appropriate risk treatment options, including applying security controls, transferring the risk (e.g., insurance), avoiding the risk, or accepting the risk (with formal approval).
7. **Risk Treatment Plan Development:** Develop a detailed risk treatment plan outlining the selected controls, responsibilities for implementation, timelines, and required resources. This plan will specifically address controls from ISO 27001:2022 Annex A, including 5.30.
8. **Residual Risk Acceptance:** Formally document and obtain approval for any residual risks that remain after implementing risk treatment measures.
9. **Monitoring and Review:** Continuously monitor identified risks and the effectiveness of implemented controls. The risk assessment will be reviewed at least annually or when significant changes occur.

6.3 Integration with Overall Risk Management

The findings from the BIA and ICT risk assessments will be integrated into the organization's overall Information Security Risk Management process, ensuring that ICT continuity risks are managed consistently with other information security risks as per ISO 27001:2022 Clause 6.1.2.

7. ICT Continuity Strategies and Plans

Based on the outcomes of the BIA and risk assessments, **[organization name]**will develop, implement, and maintain robust ICT continuity strategies and detailed plans to ensure the availability and resilience of critical ICT systems and services. These strategies and plans will be designed to meet the defined RTOs and RPOs.

7.1 Data Backup and Recovery

- **Backup Procedures:** Comprehensive backup procedures will be established and implemented for all critical data and systems. Backups will be performed regularly, stored securely (both on-site and off-site), and protected against unauthorized access or corruption.
- **Recovery Procedures:** Detailed data recovery procedures will be documented and regularly tested to ensure that data can be restored accurately and within the defined RPOs.
- **Data Integrity:** Mechanisms will be in place to verify the integrity and usability of backed-up data.

7.1.1 Data Backup and Recovery Procedures

Detailed procedures for data backup and recovery will include:

1. **Data Identification and Classification:** Identify all critical data assets, classify them based on sensitivity and criticality, and assign appropriate RPOs.
2. **Backup Schedule and Frequency:** Define specific backup schedules (e.g., daily full, hourly incremental) for different data types and systems based on their RPOs
3. **Backup Methods and Technologies:** Specify the backup methods (e.g., disk-to- disk, tape, cloud-based) and technologies (e.g., specific backup software, cloud native backup services) to be used.

4. **Storage Locations:** Define secure storage locations for backups, including off- site and geographically dispersed locations to protect against regional disasters. Encryption of data at rest in backup locations is mandatory.
5. **Retention Periods:** Establish data retention periods for backups in accordance with legal, regulatory, and organizational requirements.
6. **Recovery Procedures:** Document step-by-step procedures for restoring data from backups, including procedures for different scenarios (e.g., single file recovery, full system restores).
7. **Integrity Verification:** Implement regular checks and processes to verify the integrity and usability of backup data (e.g., checksums, test restores).
8. **Access Control:** Implement strict access controls to backup systems and data, ensuring only authorized personnel can access or restore backups.

7.2 System and Application Recovery

- **Redundancy and High Availability:** Critical ICT systems and applications will be designed and implemented with appropriate levels of redundancy and high availability to minimize single points of failure.
- **Disaster Recovery Sites:** For critical systems requiring rapid recovery, disaster recovery sites (e.g., hot, warm, or cold sites) will be established and maintained, complete with necessary infrastructure, hardware, and software.
- **Recovery Procedures:** Detailed recovery procedures for critical systems and applications will be documented, outlining the steps required to restore services at the primary or alternate sites within their defined RTOs.
- **Cloud-based Recovery:** For cloud-based services, recovery strategies will leverage cloud provider capabilities (e.g., multi-region deployments, automated failover, snapshotting) and align with the shared responsibility model.

7.2.1 System and Application Recovery Procedures

Detailed procedures for system and application recovery will include:

1. **Critical System Identification:** Maintain an up-to-date inventory of all critical ICT systems and applications, including their dependencies and RTOs.
2. **Recovery Teams and Roles:** Define clear roles and responsibilities for recovery teams, including technical specialists for each system or application.
3. **Recovery Playbooks/Runbooks:** Develop detailed, step-by-step recovery playbooks for each critical system and application. These playbooks will include:
    - Prerequisites for recovery (e.g., necessary hardware, software licenses, network configurations).
    - Sequence of recovery steps.
    - Configuration details and settings.
    - Dependencies on other systems or services.
    - Verification steps to confirm successful recovery.
    - Contact information for support personnel and vendors.
4. **Alternate Site Activation:** Procedures for activating and transitioning operations to designated disaster recovery sites (e.g., hot, warm, cold sites) or cloud-based recovery environments.
5. **Virtualization and Automation:** Leverage virtualization technologies and automation scripts where it is possible to expedite system and application recovery.
6. **Cloud-Specific Recovery:** For cloud-based applications, procedures will detail the use of cloud provider-specific recovery mechanisms such as multi-AZ/region deployments, automated failover, snapshotting, and infrastructure-as-code for rapid deployment.

7.3 Network and Connectivity Resilience

- **Redundant Connectivity:** Critical network connections will have redundancy (e.g., multiple ISPs, diverse routing) to ensure continuous connectivity.

- **Secure Remote Access:** Secure remote access solutions will be available to enable authorized personnel to manage and operate ICT systems during disruption.

7.3.1 Network and Connectivity Resilience Procedures

Procedures for ensuring network and connectivity resilience will include:

1. **Network Architecture Review:** Regular review of network architecture to identify and eliminate single points of failure.
2. **Redundant Network Paths:** Implementation of redundant network paths, devices, and internet service providers (ISPs) for critical connections.
3. **Failover Mechanisms:** Configuration and testing of automated failover mechanisms for network devices and internet links.
4. **Secure Remote Access:** Establishment and maintenance of secure remote access solutions (e.g., VPNs with MFA) for authorized personnel to manage and access systems during disruptions.
5. **Bandwidth Management:** Ensuring sufficient bandwidth is available for recovery operations and critical business functions during disruption.

7.4 Communication and Command Structure

- **Emergency Communication Plan:** A clear emergency communication plan will be established to facilitate internal and external communication during a disruption. This includes contact lists for key personnel, stakeholders, emergency services, and vendors.

- **Command and Control:** A clear command and control structure will be defined, identifying individuals with authority to make decisions during a crisis, especially those related to information security and ICT recovery.

- **Communication Channels:** Redundant communication channels (e.g., satellite phones, alternative networks) will be available for use if primary channels are unavailable.

7.4.1 Communication and Command Structure Procedure

Procedures for communication and command during a disruption will include:

1. **Incident Management Team (IMT) Activation:** Clear criteria and procedures for activating the IMT and establishing the command center.
2. **Emergency Contact Lists:** Maintenance of up-to-date emergency contact lists for all relevant personnel, stakeholders, vendors, and emergency services, accessible both physically and digitally (off-site).
3. **Communication Protocols:** Defined protocols for internal and external communication during disruption, including pre-approved templates for various scenarios.
4. **Redundant Communication Channels:** Identification and testing of alternative communication channels (e.g., satellite phones, dedicated crisis communication platforms, public service announcements) in case primary channels are unavailable.
5. **Decision-Making Authority:** Clear delegation of decision-making authority for various levels of disruption, ensuring rapid response.

7.5 Resource Availability

- **Personnel:** Identification of key personnel required for ICT recovery, with provisions for their availability and access to necessary resources during a disruption.
- **Equipment and Software:** Ensuring the availability of necessary equipment, software licenses, and spare parts required for recovery operations.
- **Documentation:** All ICT continuity plans, procedures, and relevant technical documentation will be securely stored and readily accessible, including off-site copies.

8. Testing, Review and Maintenance

To ensure the ongoing effectiveness and relevance of ICT continuity plans, **[organization name]** will establish a rigorous program for testing, reviewing, and maintaining these plans. This continuous cycle of improvement is critical for adapting to changes in the ICT environment, business processes, and threat landscape, aligning with ISO 27001:2022 requirements.

8.1 Testing and Exercising

ICT continuity plans will be regularly tested and exercised to validate their effectiveness, identify weaknesses, and ensure that personnel are familiar with their roles and responsibilities. Testing activities will include:

- **Tabletop Exercises:** Discussions-based sessions to walk through scenarios and validate the understanding of roles, responsibilities, and procedures.
- **Simulation Exercises:** Practical exercises that simulate disruption, allowing teams to execute recovery procedures in a controlled environment.
- **Full-Scale Drills:** Comprehensive exercises involving the activation of alternate sites and full recovery of critical ICT systems and services, where feasible.
- **Component Testing:** Regular testing of individual components such as backups, redundant systems, and communication channels.

Testing frequency will be determined by the criticality of the ICT system or service, the complexity of the recovery plan, and regulatory requirements, but will occur at least annually for critical systems. Test results, including identified deficiencies and lessons learned, will be documented and used to improve the plans.

8.1.1 Testing and Exercising Procedures

Detailed procedures for testing and exercising ICT continuity plans will include:

1. **Test Planning:** Develop a detailed test plan for each exercise, outlining objectives, scope, participants, scenarios, success criteria, and a schedule. This plan will be approved by the BCM Team and relevant IT management.
2. **Scenario Development:** Create realistic and challenging scenarios that simulate various types of disruptions (e.g., power outage, cyberattack, natural disaster) to test different aspects of the ICT continuity plan.
3. **Execution:** Conduct the planned tests, ensuring all participants understand their roles and responsibilities. Document all actions taken, observations, and deviations from the plan.
4. **Performance Measurement:** Measure key metrics during testing, such as RTO adherence, RPO achievement, system uptime, data recovery rates, and communication effectiveness.
5. **Post-Test Review (Hot Wash):** Immediately after the test, conduct a debriefing session with all participants to gather initial feedback, identify immediate issues, and acknowledge successes.
6. **Lessons Learned Report:** Prepare a comprehensive lesson learned report, detailing:
    - Test objectives and outcomes.
    - Identified strengths and weaknesses of the plan and procedures.
    - Non-conformities and areas for improvement.
    - Recommendations for corrective actions and enhancements.

    - Action owners and target completion dates.

7. **Corrective Action Implementation:** Implement the recommended corrective actions and verify their effectiveness through follow-up testing or review.
8. **Regularity:** Critical ICT systems and their recovery plans will be tested at least annually, with more frequent testing for highly critical systems or after significant changes.

8.2 Review and Update

ICT continuity plans and this policy will be formally reviewed at least annually, or whenever significant changes occur, such as:

- Changes in business processes or organizational structure.
- Changes in critical ICT systems, applications, or infrastructure.
- Changes in the threat landscape or risk profile.
- Lessons learned from incidents or testing activities.
- Changes in legal, regulatory, or contractual requirements.

Reviews will ensure that RTOs and RPOs remain appropriate, recovery strategies are still viable, and all documentation is current and accurate.

8.2.1 Review and Update Procedure

Procedures for reviewing and updating ICT continuity plans and this policy will include:

1) **Scheduled Reviews:** Conduct formal reviews of the policy and all associated ICT continuity plans at least annually, or as specified by the BCM Team.
2) **Triggered Reviews:** Initiate reviews whenever significant changes occur, such as:
    - Changes in business process or organizational structure.

- Major changes to critical ICT systems, applications or infrastructure.
- Significant changes in the threat landscape or risk profile.
- Lessons learned from actual incidents or testing activities.
- Changes in legal, regulatory, or contractual requirements.

3) **Stakeholder involvement:** Ensure that relevant stakeholders, including business owners, IT management, information security and legal/compliance are involved in the review process.
4) **Documentation Update:** All changes and updates to the policy, plans and procedures will be formally documented, version controlled and communicated to relevant personnel.

8.3 Maintenance

Ongoing maintenance activities will ensure that the ICT environment and supporting documentation remain aligned with the continuity plans:

- **Configuration Management:** Ensuring that changes to ICT configurations are reflected in continuity plans.
- **Documentation Updates:** Keeping all plans, procedures, contact lists, and technical documentation up to date.
- **Software and Hardware Refresh:** Ensuring that recovery capabilities are compatible with current software versions and hardware.
- **Supplier Agreements:** Regularly reviewing and updating agreements with third-party suppliers of ICT services to ensure their continuity capabilities align with organizational requirements.

9. Training and Awareness

[organization name] is committed to ensuring that all relevant personnel are adequately trained and aware of their roles and responsibilities in supporting ICT readiness for business continuity. This commitment aligns with the ISO 27001:2022 requirement for competence and awareness.

9.1 Training Program

A comprehensive training program will be established and maintained for all personnel involved in ICT continuity planning, implementation, and response. Training will be tailored to specific roles and responsibilities and will include:

- **Initial Training:** For new employees and those assigned new roles related to ICT continuity.
- **Refresher Training:** Regular training sessions to reinforce knowledge and update personnel on changes to plans or procedures.
- **Specialized Training:** For technical teams responsible for specific recovery tasks, covering detailed recovery procedures, tools, and technologies.

9.2 Awareness program

An ongoing awareness program will be implemented to ensure that all employees understand the importance of business continuity and their general role in supporting it. This includes:

- **Policy Awareness:** Ensuring all employees are aware of this policy and its implications.
- **Reporting Procedures:** Educating employees on how to report potential threats, incidents, or disruptions that could impact ICT systems.
- **Communication Protocols:** Familiarizing employees with emergency communication channels and procedures.

9.3 Documentation of Training

All training activities, including attendance records, training materials, and assessment results, will be documented and maintained. This provides evidence of competence and compliance with training requirements.

10. Compliance and Audit

[organization name] is committed to ensuring that its ICT Readiness for Business Continuity program is compliant with all applicable laws, regulations, contractual obligations, and internal policies, including ISO/IEC 27001:2022. Regular audits will be conducted to verify compliance and effectiveness.

10.1 Legal, Regulatory and Contractual Requirements

- **Identification:** All relevant legal, regulatory, and contractual requirements pertaining to business continuity and ICT readiness will be identified, documented, and regularly reviewed.
- **Compliance:** The ICT Readiness for Business Continuity program will be designed and implemented to meet these identified requirements. Any changes in these requirements will trigger a review and update of the policy and associated procedures.

10.2 Internal and External Audits

- **Internal Audits:** The ICT Readiness for Business Continuity program will be subject to regular internal audits as part of the overall ISMS internal audit program. These audits will assess compliance with this policy, related procedures, and ISO 27001:2022 requirements.
- **External Audits:** The organization will cooperate with external auditors for ISO 27001 certification or other compliance audits, providing necessary documentation and evidence related to ICT readiness for business continuity.
- **Audit Findings:** Findings from both internal and external audits will be documented as non-conformities, and corrective actions will be promptly identified, implemented, and verified for effectiveness.

10.3 Management Review

- **Review Input:** The performance of the ICT Readiness for Business Continuity program, including audit results, test outcomes, incident reports, and compliance status, will be presented as input to the management review of the ISMS.
- **Decision Making:** Top management will review this information to ensure the continuing suitability, adequacy, and effectiveness of the program, and make decisions regarding resource allocation and improvements.

11. Continuous improvement

[organization name] is committed to the continual improvement of its ICT Readiness for Business Continuity program. This commitment aligns with the ISO 27001:2022 requirement for continual improvement of the Information Security Management System (ISMS).

11.1 Performance Monitoring and Measurement

- **Metrics:** Key performance indicators (KPIs) and metrics will be established to measure the effectiveness of ICT continuity controls and the overall program. These metrics may include:
  - RTO and RPO achievement rates during tests and actual incidents.
  - Number of identified single points of failure and their remediation status.
  - Timeliness of backup and recovery operations.
  - Effectiveness of communication during disruptions.
  - Number of personnel trained and their understanding of procedures.

- **Reporting:** Performance metrics will be regularly collected, analyzed, and reported to relevant management committees to support data-driven decision-making and demonstrate the value of the ICT readiness program.

11.2 Non-Conformity and Corrective Action

- **Identification:** Any non-conformities (e.g., failed tests, incidents, audit findings, policy deviations) related to ICT readiness for business continuity will be identified and documented.
- **Root Cause Analysis:** A systematic root cause analysis will be conducted for significant non-conformities to understand the underlying reasons for their occurrence.
- **Corrective Actions:** Appropriate corrective actions will be determined, implemented, and verified for effectiveness to prevent recurrence of non-conformities.

11.3 Preventive Action

- **Proactive Measures:** Based on trends from performance monitoring, risk assessments, and lessons learned, proactive measures will be identified and implemented to prevent potential non-conformities or improve the overall resilience of ICT systems.

11.4 Technology and Best Practice Review

- **Emerging Technologies:** The ICT Department will continuously monitor emerging technologies, tools, and best practices in business continuity and disaster recovery to identify opportunities for enhancing the program.
- **Industry Standards:** Adherence to relevant industry standards and guidelines (e.g., NIST, BCI) will be periodically reviewed to ensure the program remains aligned with leading practices.

12. References

- ISO/IEC 27001:2022 – Control A.17.1.1: Planning information security continuity
- Internal Document: BIA Register, IT Asset List, BCP Plan
- ISO 22301:2019 – Business Continuity Management