Bank Internal IT Policy

1. Introduction This policy outlines the framework for managing ICT and security risks in compliance with the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04). It aims to ensure the confidentiality, integrity, and availability of the bank's ICT systems and data.

2. Scope This policy applies to all ICT systems, services, processes, and staff within the bank, including third-party providers and contractors.

3. Governance and Strategy

- **Management Body Responsibilities:** The management body is accountable for the ICT strategy, ensuring its alignment with the business strategy. It should establish an internal control framework for ICT and security risks, set clear roles and responsibilities, and ensure adequate resources and training.
- **ICT Strategy:** The ICT strategy should define:
    - The evolution of ICT to support the business strategy.
    - Key dependencies on third parties.
    - Information security objectives focusing on systems, services, staff, and processes.
- **Action Plans:** Establish action plans to achieve ICT strategy objectives, review them periodically, and communicate them to relevant staff.

4. Risk Management Framework

- **Risk Identification and Assessment:** Identify and classify business functions, processes, and information assets. Conduct annual risk assessments and update them upon significant changes.
    - **Mapping:** Maintain updated mappings of business functions, processes, and information assets.
    - **Classification:** Classify assets based on confidentiality, integrity, and availability.
- **Risk Mitigation:** Define and implement measures to mitigate ICT and security risks. Continuously monitor and improve the framework based on lessons learned.
    - **Documentation:** Document the risk management framework and review it annually.
    - **Reporting:** Report risk assessment results and updates to the management body regularly.

5. Information Security

- **Information Security Policy:** Develop a policy defining high-level principles to protect data confidentiality, integrity, and availability. This policy should include:
    - Roles and responsibilities of information security management.
    - Requirements for staff and contractors regarding information security.
    - Protection measures for critical assets, resources, and sensitive data.

- **Logical Security:** Implement procedures for identity and access management, including:
    - Need-to-know, least privilege, and segregation of duties.
    - User accountability and activity logging.
    - Access management and recertification.
    - Robust authentication methods.
- **Physical Security:** Define measures to protect premises, data centers, and sensitive areas from unauthorized access and environmental hazards.
    - **Access Control:** Restrict physical access to authorized individuals and review access rights regularly.
    - **Environmental Protection:** Implement measures to protect against environmental hazards.
- **Security Monitoring:** Establish procedures to detect and respond to security incidents, including continuous monitoring of internal and external factors.
    - **Detection and Reporting:** Implement capabilities for detecting and reporting intrusions and breaches.
    - **Threat Monitoring:** Regularly review threats and vulnerabilities.
- **Information Security Reviews:** Conduct regular security reviews, assessments, and testing to identify vulnerabilities.
    - **Testing Framework:** Implement a testing framework for security measures, including vulnerability scans, penetration tests, and other assessments.

6. ICT Operations Management

- **ICT Operations:** Document and implement processes for operating, monitoring, and controlling ICT systems. Maintain an up-to-date ICT asset inventory.
    - **Asset Inventory:** Detail configuration and interdependencies of ICT assets.
    - **Lifecycle Management:** Monitor and manage the lifecycle of ICT assets, ensuring they meet business and risk management requirements.
    - **Backup and Restoration:** Define and implement backup and restoration procedures, ensuring secure storage and regular testing.
- **Incident and Problem Management:** Establish processes to monitor and log ICT incidents and problems.
    - **Incident Response:** Implement procedures to identify, track, and mitigate incidents.
    - **Problem Management:** Identify root causes of incidents and update security measures accordingly.

7. Business Continuity Management

- **Business Impact Analysis (BIA):** Conduct BIAs to assess potential impacts of severe business disruptions.
    - **Criticality Assessment:** Consider the criticality of business functions, processes, and assets.
    - **Redundancy:** Design ICT systems with redundancy for critical components.
- **Continuity Planning:** Develop and document business continuity plans (BCPs) based on BIAs.

    - **Recovery Objectives:** Define recovery time and point objectives (RTOs and RPOs).
    - **Scenario Planning:** Consider a range of scenarios, including cyber-attacks.
- **Response and Recovery Plans:** Develop response and recovery plans to ensure availability and continuity of critical systems and services.
    - **Short-Term and Long-Term Recovery:** Address both short-term and long-term recovery options.
    - **Third-Party Continuity:** Implement measures to mitigate failures of key third-party providers.
- **Testing and Maintenance:** Test BCPs at least annually and update them based on test results, threat intelligence, and lessons learned.
    - **Scenario Testing:** Include severe but plausible scenarios in tests.
    - **Documentation:** Document test results and address deficiencies.

8. Compliance and Reporting

- **Audit and Reporting:** Perform periodic audits of ICT governance, systems, and processes.
    - **Independent Audits:** Ensure audits are conducted by independent auditors with relevant expertise.
    - **Audit Plan:** Approve and regularly update the audit plan, reflecting inherent ICT and security risks.
    - **Follow-Up:** Establish a follow-up process for critical audit findings.
- **Regulatory Compliance:** Ensure compliance with relevant EU and national regulations.
    - **Notifications:** Submit compliance notifications as required and report changes in compliance status.

9. Training and Awareness

- **Training Program:** Implement a training program for all staff and contractors to ensure awareness of ICT and security risks and responsibilities.
    - **Frequency:** Provide training at least annually.
    - **Content:** Cover security policies, procedures, and how to address information security-related risks.