SOUTHBANK INC.

IT Policy and Guidelines

Document Revision History:

Version	Date	Author	Description of Changes
Version 1.1	September 2021	Norman Armian	Initial Draft
Version 1.2	April 20, 2025	Norman Armian	This is a streamlined version that incorporates the IT minimum applicability standards, vendor accreditation process, and general IT governance oversight.

TABLE OF CONTENTS

1. Introduction

- **1.1 Purpose of the Policy**
- **1.2 Scope and Coverage**
- **1.3 Regulatory and Standards References**
- **1.4 Compliance and Enforcement**

2. Minimum IT Security Requirements

- **2.1 Purpose and Importance**
- **2.2 Potential Risks**
- **2.3 Implementation Guidelines**
- **2.3.1 Network Firewall**
- **2.3.2 VPN Router (Branch and HO Connectivity)**
- **2.3.3 Endpoint Protection**
- **2.3.4 Updated Operating Systems**
- **2.3.5 Network Segmentation**
- **2.3.6 Wi-Fi Access**
- **2.4 Regulatory References (BSP Circular 808, ISO/IEC 27002:2022)**

3. IT Operations and Vendor Management

- **3.1 Purpose and Importance**
- **3.2 Potential Risks**
- **3.3 Policy Details**
- **3.3.1 IT Vendor Accreditation**
- **3.3.2 Servicing for Contractors/External Personnel**
- **3.3.3 Access to Data Center / Controlled Areas**
- **3.3.4 Use and Access of Storage Devices**
- **3.3.5 Equipment Life-Cycle Management**
- **3.3.6 Data Backup**
- **3.4 Regulatory References**

4. Internet Use Policy

- **4.1 Purpose and Importance**
- **4.2 Potential Risks**
- **4.3 Policy Details**

5. Wi-Fi Access Policy

- **5.1 Purpose and Importance**
- **5.2 Potential Risks**
- **5.3 Policy Details**
- **5.4 Regulatory References**

6. Compulsory System and Cybersecurity Training

- **6.1 Purpose and Importance**
- **6.2 Potential Risks**
- **6.3 Training Requirements**
- **6.4 Regulatory References**

7. Work-Related Tools and Software Applications Policy

- **7.1 Purpose and Importance**
- **7.2 Potential Risks**
- **7.3 Policy Details**

8. Official Communication Channels Policy

- **8.1 Purpose and Importance**
- **8.2 Potential Risks**
- **8.3 Policy Details**

9. User Responsibilities

- **9.1 Purpose and Importance**
- **9.2 Potential Risks**
- **9.3 Policy Details**
- **9.3.1 Password Complexities and Security**
- **9.3.2 Physical Security**
- **9.3.3 Incident Reporting**
- **9.3.4 Password Sharing Prohibition**
- **9.3.5 Confidentiality Obligations**
- **9.3.6 Unauthorized File Transfer Restrictions**
- **9.3.7 Memorandum of Understanding (MOU)**
- **9.4 Regulatory References**

10. Policy Review and Updates

- **10.1 Review Cycle**
- **10.2 Change Management**
- **10.3 Communication of Updates**

INTRODUCTION

This policy governs the secure and appropriate use of all the bank's IT services, with a special focus on the SBPay application. The objective is to protect the bank's information assets, ensure the confidentiality, integrity, and availability of our IT infrastructure, and comply with all relevant Bangko Sentral ng Pilipinas (BSP) regulations and international IT security standards.

The purpose of this policy is to provide a clear framework for all employees and authorized users regarding their responsibilities when using the bank's IT services. Observance of this policy is mandatory. Failure to comply can result in disciplinary action, including termination, and may lead to legal consequences.

1. MINIMUM IT SECURITY REQUIREMENTS

Purpose and Importance: Implementing minimum security requirements is the foundation of a comprehensive cybersecurity posture. A multi-layered defense strategy, including firewalls, endpoint protection, and network segmentation, helps to protect the bank's systems from a wide range of cyber threats. These controls are critical for preventing unauthorized access, data breaches, and service interruptions.

Potential Risks: Without these security measures, the bank is exposed to significant risks such as unauthorized access (exploiting vulnerabilities), malware and ransomware attacks (leading to system downtime and data loss), and regulatory penalties for non-compliance.

Implementation Strategy:

1. **Network Firewall**: Inspects and controls all incoming and outgoing network traffic.
2. **VPN Router:** Provides secure, encrypted connections for all remote and branch offices.
3. **Endpoint Protection:** All bank-owned devices must have up-to-date antivirus and endpoint detection and response (EDR) solutions.
4. **Updated Operating Systems:** All systems and software must be regularly patched.
5. **Network Segmentation:** Core banking systems must be isolated on a separate, segmented network.
6. **Wi-Fi Access:** A secure Wi-Fi network with a registration process must be implemented to segment bank users from guests.

References: This aligns with BSP Circular No. 808, Series of 2013, which mandates a comprehensive IT risk management program, and ISO/IEC 27002:2022, which provides guidance on network security management.

2. IT OPERATIONS AND VENDOR MANAGEMENT

Purpose and Importance: This section ensures all IT-related work, including that performed by external parties, is conducted securely. It also establishes standards for asset management and data protection.

Potential Risks: Failure to manage vendors and control physical access can lead to unauthorized data access, system vulnerabilities, poor service or after-sales support, and operational disruptions.

Policy Details:

1. **IT Vendor Accreditation:** All third-party IT service providers must undergo the bank's accreditation process to ensure compliance with established security standards. For detailed guidelines, *please refer to SouthBank Inc. – IT Vendor Accreditation Policy v1*.

2. **Physical Servicing of Contractors/External Personnel:** Third-party personnel or service providers are required to submit work details or a formal notice to the IT Unit for review, approval, and sign-off by the concerned officers before the scheduled service delivery date

3. **Access to Data Center / Controlled Areas:** Access is restricted to authorized personnel and must be controlled using, at minimum, a locking mechanism such as biometric systems, physical locks, or other equivalent security tools.

4. **Use and Access of Storage Devices:** The use of personal or unapproved external storage devices is prohibited.

5. **Equipment Life-Cycle Management**: A standard lifespan of three (3) years is set for main working facilities. Equipment must be replaced or disposed of after a maximum of five (5) years. Special cases are considered for end-of-life support.

6. **Data Backup:** Data backups must be performed a minimum of once a day. Backups must be kept in a defined on-site or off-site storage location. Logs and necessary documentation are kept for record-keeping purposes. *Please refer to the Backup_logsheet 2025.*

References: These measures are consistent with BSP Circular No. 808, Series of 2013, which mandates strong third-party risk management and physical security and backup procedures.

3. INTERNET USE POLICY

Purpose and Importance: Regulating internet access is important for minimizing the risk of malware infections, phishing attacks, and data exfiltration.

Potential Risks: Unrestricted internet use can lead to unproductivity, malware infections, data breaches, bandwidth misuse, and legal liabilities for the bank.

Policy Details:

1. Internet access is a privilege, not a right.

2. All internet access requests must be submitted through the designated IT Service Request Form (ITSRF) and approved by the respective department head.

3. Access will be granted based on business needs and the user's role to be defined during the employee onboarding procedure.

4. Access to high-risk websites or sites that are not work-related or cause service disruptions (such as streaming services, online gaming) is strictly prohibited.

5. For websites deemed important while it is restricted, the concerned user can request whitelisting through the IT ticketing facility.

4. WI-FI ACCESS POLICY

Purpose and Importance: Controlling Wi-Fi access is essential for managing the security of both bank-owned and personal devices (BYOD) that connect to the network.

Potential Risks: Uncontrolled Wi-Fi access may result in unauthorized network entry, bandwidth disruption, data breaches, and malware infections from unsecured devices.

Policy Details:

1. Only authorized and approved devices can connect to the bank's Wi-Fi network. This shall be filed or requested in the IT Service Request Form (ITSRF).

2. All devices, including BYOD, must be registered with the IT Department. Each employee may register up to two devices, limited to those with direct relevance to their work responsibilities.

3. Registered devices are subject to security checks, including the installation of bank-mandated security software. A list of these software can be available upon request from the IT Unit, approval of the Unit Head to maybe required for those sensitive by nature.

4. For guest users, they may be allowed depending on the purpose, but come with a voucher facility with limited time access.

References: This aligns with global IT standards for Network Access Control (NAC) as defined in ISO/IEC 27002:2022, which specifically addresses the security of network services, including Wi-Fi, by requiring access control policies to ensure only authorized users and devices can connect.

5. COMPULSORY SYSTEM AND CYBERSECURITY TRAINING

Purpose and Importance: Employees are often the first line of defense against cyber threats. Regular training and awareness programs are critical for educating staff on common threats.

Potential Risks: Without regular training, employees are more likely to fall victim to phishing and social engineering attacks, leading to data breaches and financial losses.

Policy Details:

1. All new employees must undergo mandatory cybersecurity training as part of their onboarding process.

2. Existing employees must attend an annual cybersecurity awareness training session.

3. Training will cover topics such as (but not limited to) phishing identification, password hygiene, safe use of IT services, and incident reporting.

4. Employees may be required to enroll and pass the online training (e-learning) facility provided by the bank on certain topics using our SBOnline Academy Facility.

References: This aligns with BSP Circular No. 808, Series of 2013, which requires a cybersecurity awareness program for all personnel.

6. WORK-RELATED TOOLS AND SOFTWARE APPLICATIONS POLICY

Purpose and Importance: Centralizing software installation and configuration to the IT Unit is crucial for maintaining a secure and stable IT environment.

Potential Risks: Unauthorized software installations can introduce malware, create system vulnerabilities, lead to licensing violations, and cause system instability.

Policy Details:

1. Only authorized IT personnel are permitted to install, configure, or remove software.

2. All software or hardware installation requests must be submitted through the bank's ticketing facility and must be duly approved.

3. Employees are strictly prohibited from downloading or installing any software from unapproved sources.

7. OFFICIAL COMMUNICATION CHANNELS POLICY

Purpose and Importance: This policy mandates the use of official, registered communication channels for all work-related correspondence, ensuring all communications are secure and traceable.

Potential Risks: Using unofficial channels can lead to exposure of confidential information, make the Bank vulnerable to social engineering attacks, and hinder legal and compliance auditing.

Policy Details:

1. All employees must exclusively use their official, Bank-provided registered email addresses or officially known email addresses for all business-related communications.

2. The use of personal email accounts or unauthorized third-party messaging applications for bank information is strictly prohibited.

3. All employees are expected to access, read, and confirm email communications sent from official email channels of the bank.

8. USER RESPONSIBILITIES

Purpose and Importance: Users are the first line of defense in cybersecurity. Defining clear responsibilities for secure behavior empowers employees to protect themselves and the Bank's information assets.

Potential Risks: Failure to follow these responsibilities can lead to compromised accounts, data breaches, and system failures.

Policy Details:

1. **Password Complexities:** Users must create and use strong passwords.
2. **Password Security:** Users shall not store passwords in browsers or on notes visible to other users.
3. **Physical Security:** Users must lock their computers when not in use.
4. **Incident Reporting:** Users must immediately report any IT issue or unusual activity to the IT Unit.
5. **Password Sharing:** Password sharing is strictly prohibited.
6. **Confidentiality:** All employees must keep Bank information confidential.
7. **Unauthorized File Transfer:** The unauthorized sending of Bank files to personal emails is prohibited.
8. **MOU:** All users must sign a Memorandum of Understanding (MOU) acknowledging their understanding and agreement to the use of the Bank's IT facilities. Refer to **Employee x SouthBank - IT Policy MOU.**

References: These responsibilities are essential for compliance with the Data Privacy Act of 2012 (RA No. 10173) and align with BSP Circular No. 982, Series of 2017, and BSP Circular No. 808, Series of 2013, which emphasize the importance of data protection and incident reporting.

9. GENERAL IT OVERSIGHT AND MANAGEMENT PROCESS

9.1 PURPOSE

This document establishes the governance, oversight, and management process for the use of any IT Services. It defines the roles and responsibilities of governing bodies, decision-making processes, and project approval workflows to ensure alignment with regulatory requirements, business objectives, and risk management practices.

9.2 GOVERNANCE STRUCTURE

9.2.1 Board of Directors (BOD)

Composition: Elected members of the Bank's Board, including independent directors as required by regulatory standards.

Function:

- Provide ultimate oversight and accountability for the IT Systems and Facility.
- Approve strategic initiatives, policies, and significant investments.
- Ensure compliance with regulatory requirements and industry best practices.
- Review and endorse major system enhancements and change requests with long-term impact.

9.2.2 IT STEERING COMMITTEE

Composition: Elected 3 BOD Members, CTO, IT personnel, compliance officer, business unit representatives.

Function:

- Review, evaluate, and recommend IT initiatives, including special IT-related projects.
- Assess feasibility, cost, and risk of proposed changes.
- Monitor IT performance and cybersecurity posture of critical IT systems or facilities.
- Endorse projects for BOD approval.

9.2.3 EXECUTIVE COMMITTEE (EXCOM)

Composition: Senior Management and selected heads of business units.

Function:

- Provide executive direction and alignment with business strategy.
- Review project proposals, critical changes, and major system enhancements before IT Steering Committee or BOD elevation.
- Decide on urgent and operationally critical matters affecting critical IT systems or facilities.

Updates, enhancements, and change requests that are deemed material to the Bank's operations and business direction shall be discussed and endorsed at this level unless it will fall under the standard support procedures.

9.2.4 DIGITAL BANKING UNIT (DIGI) AND STRATEGIC PARTNERS

Composition: CTO and other key IT personnel, Subject Matter Experts (SME), support personnel, project managers, Tech Lead, and strategic technology partners/vendors.

Function:

- Coordinate day-to-day system operations, support, enhancements, and integrations.
- Conduct regular meetings with partners to track updates, regulatory requirements, and new features.
- Prepare impact assessments and proposals for higher-level review.
- Ensure smooth collaboration between the Bank and external vendors or service providers.

9.3 PROJECT GOVERNANCE AND APPROVAL FRAMEWORK

Projects and system enhancements follow a structured process to ensure alignment with strategic direction, risk management, and compliance requirements.

9.2.2 Requisition Procedure

- Requests may be initiated by business units, the DIGI Unit, or internal/external regulatory directives.
- Communication channels:
    a) Official email submission with supporting details, or
    b) Presentation during scheduled committee meetings.
- Request must include justification, expected benefits, and alignment with business/operational goals.

9.3.2 Needs Analysis and Risk Assessment

A structured analysis will be conducted to evaluate necessity, risks, and impacts.

The Needs Analysis/Risk Assessment template should contain the following:

ITEM/REQUIREMENT	IMPACT ASSESSMENT (HIGH/MED/LOW)	MONITORING METHOD	CONTROL MEASURES	RESPONSIBLE UNIT	REMARKS
Example: Vendor API Integration	High regulatory compliance requirement	Monthly compliance monitoring	Automated reporting, monitoring and validation	DIGI / Compliance	Mandatory by BSP Circulars
Example: Vendor Service Level Agreement	Medium – potential operational impact	Quarterly vendor audit	SLA enforcement, redundancy setup	DIGI / IT	Requires IT Steering review

Areas of Concern:

- Oversight – Governance, reporting, and committee accountability.
- Regulatory – BSP, AMLA, Data Privacy Act, and other compliance obligations.
- Third-Party – Vendor management, outsourcing risks, SLA performance.
- Operational – Impact on service continuity, scalability, and end-user experience.
- Security – Cybersecurity posture, fraud prevention, access controls.
- Financial – Cost, ROI, budget approval, and resource allocation.

9.3.3 SUBMISSION OF CONCEPT PAPER / PROJECT PROPOSAL

To formalize IT development requests, all initiatives must be supported by a Concept Paper or Project Proposal along with the need analysis. This requirement ensures that the project's objectives, scope, and resource needs are clearly defined, while also promoting alignment with the bank's strategic goals. The submission fosters proper evaluation, transparency, and accountability, and encourages coordination among all departments and stakeholders involved in the development process.

For reference, please refer to the following outline below:

Concept Paper Outline:

1. Project Title
2. Project Proponent / Initiating Unit
3. Background and Rationale
    - Problem/need statement
    - Regulatory or business driver
4. Objectives
    - Strategic alignment with bank goals
    - Customer/operational benefits
5. Scope
    - Inclusions/exclusions
    - Dependencies (systems, vendors)
6. Impact Assessment
    - Operational, financial, regulatory, and security impact (refer to template)
7. Risk Assessment Summary
    - Key risks and mitigation measures (refer to template)
8. Estimated Cost and Resources
    - Budget allocation and funding source
    - Human resource requirements
9. Timeline
    - Phases and milestones
10. Recommendation/Next Steps

9.3.4 DECISION AND ENDORSEMENT

Decisions are documented through Minutes of Meeting (MoM) and formally endorsed across levels:

1. Project Stakeholder / Initiator
2. Involved Unit or Departments
3. EXCOM
4. IT Steering Committee
5. Board of Directors (final approval for major projects)

9.3.5 BUSINESS REQUIREMENTS DOCUMENT (BRD) CREATION

The BRD will serve as the foundation for development and testing. It must include:

- Documentation of requirements and scope.
- System analysis and design.
- Team composition and roles.
- Timelines and milestones.
- Resources (financial, human, technological).
- Regulatory and compliance considerations.

9.4 TESTING AND ASSESSMENT

- UAT (User Acceptance Testing) and QA (Quality Assurance) will be conducted.
- Security and regulatory compliance testing is mandatory.
- Results and deviations must be documented and remediated before rollout.

9.5 SIGN-OFF AND PROJECT CLOSURE

- Formal sign-off from the project team, proponents, and the IT Committee.
- Project turnover / Production Stage.
- Post-implementation review and lessons learned documentation.
- Closure memorandum recorded in MoM.

9.6 RECORDS AND DOCUMENTATION

All submissions, evaluations, approvals, MoMs, BRDs, and closure reports must be:

- Properly archived in the Bank's official document management system.
- Accessible for regulatory review and internal audit.
- Retained in compliance with record-keeping policies.

9. POLICY REVIEW AND UPDATES

This IT Policy will be reviewed at least annually, or as needed, in response to changes in technology and regulatory requirements. Any updates or revisions will be communicated to all relevant stakeholders or concerned personnel or unit heads.