Information Security Policy Summary

Seylan Bank PLC.

This version of the Information Security Policy summary is suitable for sharing with external suppliers and third parties, providing them with a clear understanding of Seylan Bank's security expectations and practices.

Classification | Public

This document is issued under the authority of the Information Security Council. Duplication and distribution of this document without an authorized release strictly prohibited.

Every person in custody of this document has the responsibility for ensuring its confidentiality. The Document owner will also ensure that the document continually updates with amendments that may be issued from time to time. Any loss or mutilation of the document must be reported promptly to CISO.

This version of the Information Security Policy summary is suitable for sharing with external suppliers and third parties, providing them with a clear understanding of Seylan Bank's security expectations and practices.

Document Control

1.	Document Title	Information Security Policy Summary
2.	Date of Release	09/05/2024
4.	Version No.	Ver 1
5.	Document Owner	Seylan Bank PLC
6.	Document Author(s)	CISO

Document Approvers

Version No.	Approver	Approved Date
V 1	Information Security Committee	

Document Change Approvals

Version No.	Description of Amendment	Amendment done by

This version of the Information Security Policy summary is suitable for sharing with external suppliers and third parties, providing them with a clear understanding of Seylan Bank's security expectations and practices.

Table of Contents

This version of the Information Security Policy summary is suitable for sharing with external suppliers and third parties, providing them with a clear understanding of Seylan Bank's security expectations and practices.

1. Introduction

The Information Security Policy (ISP) of Seylan Bank PLC aims to protect its information assets against breaches of confidentiality, integrity failures, and availability interruptions. The policy provides management direction and support to ensure protection and appropriate use of Seylan's information assets in compliance with standards, laws, and regulations.

2. Scope

The ISP applies to all information assets of Seylan Bank PLC. Information assets include software, physical assets, paper documents, services, personnel, and electronic data. The policy covers all employees and suppliers associated with Seylan.

3. Policy Objectives

The key objectives of the ISP are:

- Protecting the confidentiality, integrity, and availability of information.
- Ensuring compliance with legal, regulatory, and contractual obligations.
- Supporting business operations by managing information security risks.
- Promoting a culture of information security within the organization.

4. Asset Management

- **Responsibility**: Employees and suppliers are responsible for the proper handling of assets.
- **Asset Register**: An up-to-date register of all assets is maintained.
- **Classification and Labelling**: Information is classified based on sensitivity and labelled accordingly.
- **Acceptable Use**: Clear guidelines on acceptable use of assets.

5. Physical and Environmental Security

- **Controls**: Physical security measures to protect against unauthorized access and environmental hazards.
- **Entry Controls**: Controlled access to secure areas.
- **Visitor Management**: Procedures for managing visitors to secure areas.
- **Equipment Security**: Measures to protect equipment from theft, damage, and environmental hazards.

6. Operations Security

- **Procedures**: Documented operational procedures to ensure security.
- **Change Management**: Processes for managing changes to systems and infrastructure.
- **Patch Management**: Regular updates and patches to software.
- **Separation of Duties**: Segregation of roles and responsibilities to reduce risk.

7. Communications Security

- **Network Controls**: Security measures for network infrastructure.
- **Firewall and Intranet Security**: Protection against external and internal threats.
- **Media Handling**: Secure handling and disposal of media.

8. Access Control

- **User Access Management**: Procedures for managing user access to information systems.
- **User Responsibilities**: Guidelines for users to protect access credentials.
- **Network Access Control**: Measures to control access to the network.

9. Systems Acquisition, Development, and Maintenance

- **Security Requirements**: Incorporating security requirements into new systems and updates.
- **Application Security**: Ensuring secure development and maintenance of applications.
- **Vulnerability Management**: Identifying and mitigating vulnerabilities.

10. Supplier Relationships

- **Supplier Management**: Processes for managing relationships with suppliers.
- **Risk Management**: Identifying and managing risks related to supplier access to information.
- **Due Diligence**: Ensuring suppliers comply with security requirements.

11. Cryptography

- **Use of Cryptography**: Guidelines for using cryptographic controls to protect information.

This version of the Information Security Policy summary is suitable for sharing with external suppliers and third parties, providing them with a clear understanding of Seylan Bank's security expectations and practices.

- **Key Management**: Procedures for managing cryptographic keys.

12. Business Continuity Management

- **Planning**: Ensuring information security continuity in business continuity plans.
- **Implementation and Review**: Regular testing and review of continuity plans.

13. Compliance

- **Legal Compliance**: Adherence to legal, regulatory, and contractual requirements.
- **Intellectual Property**: Protecting intellectual property rights.
- **Fraud Management**: Measures to prevent and manage fraud.

14. Information Systems Audit

- **Audit Controls**: Regular audits to ensure compliance with security policies.
- **Protection of Audit Tools**: Securing tools and data used in audits.

This version of the Information Security Policy summary is suitable for sharing with external suppliers and third parties, providing them with a clear understanding of Seylan Bank's security expectations and practices.