SCB X

SCB X Group

Information and Cybersecurity Policy

www.scbx.com

DISCLAIMER
This document is a public, summarized version of the SCBX Group's internal Information and Cybersecurity Policy.
It is intended to provide a high-level overview of the Group's cybersecurity principles and governance framework.
Certain operation details and internal governance mechanisms have been intentionally excluded to align with public disclosure standards.


Our Sustainability Mission
OPPORTUNITIES
FOR EVERYONE,
POSSIBILITIES
EVERYDAY

TABLE OF CONTENTS

SCBX GROUP INFORMATION AND CYBERSECURITY POLICY

1. BACKGROUND AND RATIONALE

Given the fast-paced development of technology and tools, and the fact that organizations become even more dependent on the use of such technology and tools in their day-to-day operations, maintaining high level of cyber security maturity play a significant role in ensuring organizational resiliency and sustainability. Emerging technologies like artificial intelligence (AI), robotics, machine learning and Internet of things (IoT), are all tightly connected. As such, risks and threats related to information and cybersecurity must be properly assessed, monitored and managed to align with the changing environment when implementing new technology.

With our ambition to become The Most Admired Regional Financial Technology Group, SCBX Public Company Limited (The "Company" or "SCBX Group") realizes that information, either in physical or electronic form, and the supporting business applications, IT processes, databases and underlying infrastructure are important assets to the business and must be suitably protected from unintentional incidents as well as deliberate attacks. Information and cybersecurity risk refers to SCBX Group's likelihood to incur losses due to a cyber-attack or data breach. Hence, SCBX Group has put in place a robust information and cybersecurity framework for directors, management, and staff to incorporate information and cybersecurity risk as part of the decision-making process, to foster strong risk culture and to implement an efficient information and cybersecurity risk management system and process consistently throughout SCBX Group.

2. SCOPE

This policy applies to SCBX Group for which SCBX has management control. This includes, but is not limited to, business units, board members, permanent staff, contractors, and third parties that exchange data, provide, or consume a service or technology as part of a contract. This policy has retrospective effect.

This policy shall cover all assets belonging to SCBX Group, whether at the SCBX Group's premises or at IT third party locations. It includes information assets, software assets, physical assets, and services.

3. POLICY REVIEW

The Information and Cybersecurity (ICS) Policy is approved by SCBX Board of Directors (BOD) and shall be reviewed annually or when there are major changes to maintain relevance and effectiveness. In case that changes to the policy do not involve changes in the guiding principles or they are insignificant, the policy shall be proposed to the Risk Management Committee (RMC) for endorsement and Risk Oversight Committee (ROC) for approval and then report to the SCBX BOD for acknowledgement. In case there is significant change to this policy, it shall be proposed to the RMC and ROC for endorsement, before proposing to the SCBX BOD for approval.

Policies and standards shall be reviewed periodically to ensure its continuous improvement, relevance, effectiveness, and alignment with the organization's evolving threat landscape and any emerging technologies. Any necessary updates or modifications to the policy and standards should be made based on lessons learned, changes in technology, industry best practices, and emerging threat trends. Employees and relevant stakeholders shall be notified of any policy and standards changes, and awareness and training programs should be conducted to ensure adherence and understanding.

4. COMPLIANCE

To ensure the continuous and systematic execution of Information and cybersecurity within the SCBX Group, authorized officers, those required to comply with this policy, any individual who violates any provisions of this policy, either by intention, negligence, deliberate fraud, without or beyond authority, regardless of whether such violation has caused damage to SCBX Group, will be regarded as committing an offense against code of conduct and will be subject to any disciplinary action imposed by SCBX Group.

All employees shall fully cooperate with internal and external authorities in the event of an investigation. Any direct and indirect violations or failure to comply with this policy by management and staff will be subject to disciplinary action in accordance with SCBX Group regulations.

5. MANAGEMENT APPROACH

SCBX Group shall utilize the ICS policy and standards from SCBX Group as a foundational framework to establish information security objectives, guidelines, and requirements. Additional controls may be added if necessary to meet regulatory requirements or risk appetite, compliance obligations, or unique needs within SCBX Group. Any additions to the baseline controls must be approved by the company's own relevant committees. If for any reason, this policy cannot be fully adopted by the SCBX Group, a complete risk and impact assessment with compensation action must be formally reported to the Policy Owner. This ensures that SCBX Group maintains a robust information security posture while remaining adaptable to specific requirements and maintaining compliance with industry standards.
SCBX Group shall comply with relevant laws, regulations, industry standards, and contractual obligations pertaining to information and cyber security. A framework to ensure compliance with regulatory requirements with respect to information and cyber security, as well as compliance with SCBX Group internal policies and requirements for security, safety, and ethical conduct shall be established and documented.

To uphold the required Information and Cybersecurity, the policy provides guidance that all employees in each business function are accountable to

- Report risks, issues, and incidents with significant impacts in a timely manner determined by their risk level.
- Identify, assess, manage, mitigate, and monitor technological risks (which include information and cybersecurity risks) relevant to owned business processes and activities.
- Comply with applicable laws, rules, regulations, policies, and standards related to technology risks areas, and
- Act and report risks may affect employee performance or report incidents involving technology risk management to supervisors.

5.1 Security Assessment and Strategy

The purpose of Security Assessments and Strategy is to establish a framework for conducting regular assessments to evaluate the security controls within SCBX Group. These assessments will help identify risks and areas for improvement as well as align security strategies with the overall goals and direction of SCBX.

- All Subsidiaries shall participate in regular security assessments performed by Cyber-COE to evaluate the security controls implemented across the organization. The assessments cover various aspects of SCBX Group Reference Security Capability, including but not limited to, GRC, Digital Identity, Infrastructure and Endpoint Security, Application Security, Data Security and Cyber Defense.
- SCBX Group shall align its security strategy with the overall goals and direction of the SCBX Group. The security strategy shall consider the findings, recommendations, and roadmap from the annual security assessments to address identified vulnerabilities, risks, and areas for improvement.
- Regular reviews of the security strategy shall be conducted to ensure its continued alignment with the evolving threat landscape, the changing needs of the organization, and the progress made in implementing remediation recommendations. The results of the security assessments shall be documented and reported to relevant stakeholders, including management and governance body.
- Action plans shall be developed based on the recommendations and roadmap provided by the assessments, with assigned responsibilities and timelines for implementation. Progress on the implementation of action plans shall be monitored and reported to ensure timely and effective resolution of identified issues.

5. 2 Risk Management

For upkeeping and ensuring of risk being properly managed, a systematic approach to identify, assess, and mitigate information security and cyber risks across the organization shall be established and documented.

5. 3 Operations Security

SCBX Group shall conduct day-to-day IT/Cybersecurity operations in a controlled and secure manner, adhering to the defined policies and alignment with established security practices.

The Operations procedures shall be documented and maintained by all technology support functions and its effectiveness must be tracked, reviewed, and updated at least annually or upon the occurrence of a major change in the system to safeguard data against new threats posed by advances in technology, software, and attack methods.

5.4 Outsourcing

SCBX Group subsidiaries outsources or external IT Third party systems must be operated in accordance with this policy.

(1) Outsourced providers must establish measures to safeguard sensitive data and uphold integrity and confidentiality.
(2) System owners must ensure that outsourced service providers or external IT third parties have their own data protection policies or must fully comply this policy and its associated.
(3) Should outsourced service providers or external IT third party does not agree to comply with any portion of this policy or its associated standards, an exception must be requested. If the exception is not approved, the IT third party may not be used.

5. 5 Information and Cyber Security Awareness, Education and Training

SCBX Group shall leverage and incorporate the Cyber COE Security awareness and training service to enhance and promote security awareness and provide training programs to educate employees about their roles and responsibilities in maintaining information and cyber security.

- All employees and contractors shall receive appropriate awareness education and training and regular updates in policies and standards, as relevant for their job function. An information security awareness program should aim to make employees and, where relevant, contractors aware of their responsibilities for information and cyber security.
- An information security awareness program should be established in line with this policy and relevant standards. The awareness program should include several awareness-raising activities such as campaigns (e.g., an “information security day”) and issuing booklets or newsletters.
- The awareness program should be planned to take into consideration the employees’ roles, and, where relevant, the expectation of the awareness of contractors. The activities in the awareness program should be scheduled over time so that the activities are repeated and cover new employees and contractors. The awareness program should also be updated regularly so it stays in line with the policies and standards and should be built on lessons learnt from security incidents.

5. 6 Cyber Resilience

SCBX Group shall develop and implement comprehensive plans and strategies to ensure the continuous availability, recovery, and resilience of critical systems and data in the face of disruptive events, including cyber-attacks and other disasters. This includes proactive and reactive measures such as risk assessments, backup and recovery procedures, incident response planning, and testing to maintain the organization's ability to operate effectively during and after adverse events, while also minimizing the impact of cyber threats.

5.7 Data Security

The policy also outlines necessary measures and guidelines to effectively manage data access, prevent unauthorized disclosure or alteration, and support our commitment to safeguarding all data utilized, generated, or stored within the organization.

(1) Data Classification: SCBX Group shall identify and classify data to ensure that all data has the appropriate level of classification, and apply suitable safeguards based on classifications.
(2) Data Handling and Control: SCBX Group shall apply a comprehensive set of controls to ensure the proper management and security of data across various classifications.
(3) Data Transfer: Data transmitted to a remote location, or administrative functions conducted by personnel from outside SCBX Group must be done using an approved transmission protocol.
(4) Data Storage: The use of personal media storage to store SCBX Group data is strictly prohibited. Only approved data storage is permitted.
(5) Encryption: Regular review of the effectiveness of data encryption methods and key management to ensure that they remain resilient against evolving threats should be established and documented as well as tracked for any risk assessment and mitigation.

5.8 Cyber Defense

Cyber defense outlines the organization's approach to protecting its systems, networks, and data from cyber threats. It encompasses a comprehensive set of capabilities and strategies designed to detect, prevent, respond to, and recover from cybersecurity incidents.

(1)Vulnerability Management: A regular Vulnerability Assessment (VA) should be established, documented, and followed to identify and manage security vulnerabilities in a timely manner.
(2)Threat Intelligence: The organization shall establish a threat modelling process to identify potential threats and vulnerabilities relevant to its systems, networks, and assets.
(3)Threat Prevention: The organization shall implement a comprehensive threat prevention strategy to safeguard its systems, networks, and data.
(4)Monitoring and Detection: As part of ensuring and upholding of SCBX Group security posture, security monitoring and surveillance should be determined to detect unusual events or threats continuously that have an impact on the security of critical systems. An appropriate monitoring system should be in place to identify unusual attack mechanisms and detect compromise of SCBX Group systems.
(5)Threat Hunting: SCBX Group shall implement Threat Hunting strategy to proactively detect and respond to advanced threats.
(6)Incident Management: SCBX Group shall implement Incident Management Strategy to effectively detect, respond to, analyze, and report security incidents.
Active Defense: SCBX Group shall implement a comprehensive Active Defense strategy to proactively engage and disrupt adversaries, protect critical assets, and strengthen its overall cybersecurity posture.

SCB X

www.scbx.com