

## **INFORMATION TECHNOLOGY POLICY PT BANK SYARIAH INDONESIA, TBK**

### **Introduction**

The Information Technology (IT) Division plays a critical role in ensuring the smooth running of operations and the quality of services delivered to customers. This unit is responsible for designing, implementing, and managing cybersecurity controls across all banking services and applications. Alongside the rapid advancement of banking technologies, new challenges inevitably emerge particularly the growing exposure to risks, including cyber threats. As such, banks are expected to continuously strengthen their maturity in IT management by implementing sound and measurable governance practices.

When governed effectively, IT not only functions as a support system for day-to-day operations but also delivers strategic value, driving business objectives and contributing to the fulfillment of the Bank's vision and mission.

To achieve this, a comprehensive Information Technology Policy is essential. This policy serves as a unifying framework, ensuring all stakeholders share the same understanding of the Bank's direction and principles for IT management. It also provides clear guidance for planning, developing, managing, securing, and monitoring IT systems. By adopting this policy, the Bank seeks to mitigate, manage, and control potential risks while enabling IT to be a strong enabler of business success and long-term sustainability.

### **Legal and Regulatory**

This policy is formulated with reference to:

1. Bank Indonesia Regulation (PBI) No. 23/6/PBI/2021 on Payment Service Providers and its subsequent amendments.
2. OJK Regulation No. 11/POJK.03/2022 (6 July 2022) on the Implementation of Information Technology by Commercial Banks.
3. Bank Indonesia Regulation No. 2 of 2024 (18 April 2024) on Information System Security and Cyber Resilience for Payment System Providers, Money Market and Foreign Exchange Market Participants, and other regulated entities under the supervision of Bank Indonesia.
4. Regulation of Members of the Board of Governors (PADG) No. 24 of 2024 concerning Information System Security and Cyber Resilience for Payment System Operators, Money Market and Foreign Exchange Market Participants, as well as Other Parties Regulated and Supervised by Bank Indonesia.
5. OJK Circular Letter No. 29/SEOJK.03/2022 (27 December 2022) on Cybersecurity and Resilience for Commercial Banks.

## Reference

Information Technology Policy of PT Bank Syariah Indonesia, Tbk, dated 22 July 2024.

## Roles and Responsibilities

The Bank's IT management must be built on solid governance, with a clear division of roles and responsibilities at every organizational level:

1. Board of Commissioners: Provides oversight, evaluation, and direction on IT strategy and governance, including risk management, audit planning and execution, and information security management to ensure availability, confidentiality, and accuracy of information.
2. Board of Directors: Defines IT strategies and policies, supervises IT governance and risk management, ensures resource availability and staff competency development, and safeguards the Bank's interests in third-party contracts.
3. IT Steering Committee: Advises the Board of Directors on IT strategies and policies, ensures project alignment with the Bank's strategic plan, monitors IT investment performance and risks, and supports problem resolution as well as resource adequacy.
4. IT Operating Units: Responsible for the day-to-day management of IT, covering planning, design and development, operations, and monitoring.

## General Provisions on IT Governance

1. IT governance must take into account the Bank's business strategy, size, complexity, role of IT, procurement methods, risks, standards, and legal obligations.
2. The Bank shall conduct regular evaluation, direction, and monitoring of IT strategies while aligning and organizing relevant units.
3. IT solutions must be properly defined, acquired, implemented, and supported through effective operational assistance.
4. IT performance must be monitored against targets, internal controls, and compliance with regulations.
5. IT governance applies to all IT units and users across the Bank.
6. The Bank must map its business processes, organizational structures, policies, information flows, human resources, IT culture, infrastructure, and applications.
7. Governance must ensure synergy across all dimensions of IT management.
8. Policies, standards, and procedures must be applied consistently and sustainably.
9. IT policies and procedures shall be reviewed and updated periodically.
10. The roles and responsibilities of the Board of Commissioners, Board of Directors, and related officials must remain clearly defined.

## **Risk Management Implementation**

Information security is central to safeguarding confidentiality, integrity, and availability of data, while ensuring uninterrupted operations of the Bank. Key obligations include:

1. Ensuring information security is implemented effectively and efficiently.
2. Applying security controls across human resources, processes, technologies, physical facilities, and the IT environment.
3. Protecting all information assets—including staff, technologies, processes, and regulatory compliance—against risks that may compromise confidentiality, integrity, or availability.
4. Basing security measures on comprehensive risk assessments of the Bank’s information assets.
5. Ensuring communication networks meet the principles of confidentiality, integrity, and availability.

## **Cybersecurity Resilience**

1. To strengthen resilience against cyber threats, the Bank must at minimum implement the following processes:
  - a) Identification: Manage and inventory IT assets, monitor vulnerabilities and emerging cyber threats, and conduct regular security testing.
  - b) Protection: Apply comprehensive security controls, perform regular maintenance and updates, manage data, networks, devices, and access rights, collaborate effectively with IT vendors (including cloud providers), and adopt secure coding practices.
  - c) Detection: Establish adequate detection processes, including performance baselines, continuous monitoring of suspicious activities and vulnerabilities, and threat analysis to ensure effective incident handling.
  - d) Response & Recovery: Develop a clear incident response and recovery plan, including a dedicated incident response team, recovery procedures to minimize impact, incident analysis and reporting, and post-incident evaluations for continuous improvement.

Bank must ensures all resilience processes are backed by robust cybersecurity information systems.

## **Cybersecurity Maturity Assessment**

1. The Bank is required to carry out a self-assessment of its cybersecurity maturity level.
2. This assessment must be conducted annually, in alignment with the regulatory cycle.
3. The objective of the assessment is to evaluate the Bank's security posture, identify potential weaknesses, and enhance overall resilience.
4. The assessment may be updated at any time if deemed necessary due to changes in risks or circumstances.
5. The results of the assessment must be formally reported to the Financial Services Authority (OJK).
6. The Bank is also required to perform cybersecurity testing, which should be based on vulnerability analysis and scenario-driven evaluations.
7. To ensure focus and accountability, the Bank must establish a dedicated unit or function specifically tasked with managing cybersecurity and resilience.
8. This cybersecurity function must be independent from IT operations, allowing it to act objectively and effectively in safeguarding the Bank's systems and data.

## **Core Principles of Cybersecurity and Resilience**

1. Clear roles and responsibilities.
2. A comprehensive cybersecurity strategy.
3. Integrated cyber risk management within enterprise risk management.
4. Embedding cybersecurity awareness within organizational culture.
5. Readiness to anticipate and manage cyber incidents.

## **Closing Statement**

This policy reflects BSI's firm commitment to strengthening the security and resilience of its information technology environment. Through its implementation, the Bank aspires to achieve effective cyber resilience capable of anticipating, detecting, and responding to evolving threats.

The policy will be reviewed and updated as necessary, particularly in response to changes in external regulations or internal company policies, and to address any areas not yet fully covered.