INFORMATION **TECHNOLOGY SECURITY**

The development of digital era and technology adoption makes the customers' transactions easier and more convenient. However, services digitalization also carries the threat of information security risks including theft, loss, manipulation and misuse of data, disclosure of sensitive information and damage or destruction of unlawfully information that can threaten the confidentiality, integrity, and availability of information.

To maintain information security, Bank Mandiri has developed and implemented an IT security strategy that complies with regulations (BI & OJK), in line with international standards (ISO 27001) & best practices (NIST Cybersecurity Framework, COBIT Framework, PCI Security Standard). The information security management system strategy is divided into three main areas, namely People, Process, and Technology as follows:

1. **People**
   a. **Security Awareness**
      The Security Awareness Program is carried out to foster awareness on information security in daily behavior which ultimately becomes the Bank's culture. Bank Mandiri conducts security awareness certification every year to all levels of employees in domestic and overseas offices. Routine security awareness campaign programs are also carried out in various media, namely newsletters (monthly), posters (quarterly), podcasts (quarterly), and phishing drills (quarterly). Some of the topics of security awareness campaigns include data security protection, maintaining data confidentiality, the latest cyber-attack trends, how to identify and avoid phishing, and online transaction security.

      Moreover, Bank Mandiri continues to increase customer security awareness with educational programs through various official Bank channels such as websites, social media (Instagram, Facebook, Twitter), and YouTube.

Campaign Security Awareness for Customer

b. Human Resource Development (HR)

Strengthening the people aspect is carried out by continuous skills development (capacity and capability) on human resources. Bank Mandiri provides training & certification to regularly develop soft skills and hard skills to all employees, and vendors/ contractors.

1. Training & certification for employees: CISM (Certified Information Security Manager), CISSP (Certified Information Systems Security Professional), CRISC (Certified in Risk and Information Systems Control), ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, CISA (Certified Information Systems Auditor), CEH (Certified Ethical Hacker), CHFI (Computer Hacking Forensic Investigator), and product-based knowledge training to deepening and expertise on the Bank security system.
2. Training for vendors/contractors: Internal training for vendor employees who work for operational support.

Soft skill development is provided through training such as leadership mindset, strategic thinking, creative thinking, design thinking, problem solving, presentation skill, and negotiation skill.

Training & certification is provided through various methods, both onsite and online (virtual) training through public platforms.

2. Process

a. Three Lines of Defense (3LoD)

Bank Mandiri has implemented a risk management mechanism consisting of three levels of defense:

- 1st line of defense - CISO Office Group, responsible for bank information security through three main functions, namely:
  - Design, designing security architecture and security requirements that are embedded from the beginning of development, implementation to system/ application operations.
  - Services, developing, reviewing and disseminating standard procedures, awareness programs and risk management. IT also implements security controls in the IT planning and development process.
  - Operations, conducting 24/7 monitoring, detecting attack threat anomalies and handling information security incidents which include identification, protection, detection, response and recovery of cyber security incidents.

INFORMATION TECHNOLOGY SECURITY

- 2nd line of defense - Operational Risk Group, responsible for developing the bank-wide operational risk management framework.

- 3rd line of defense – Internal Audit, responsible for carrying out assurance functions on operational activities in accordance with internal and regulatory regulations.

b. Security Policy & Procedure

Bank Mandiri already has a structure of information security policies and procedures based on regulations and International Standards such as POJK No. 11/POJK.03/2022 on the Implementation of Information Technology by Commercial Banks), ISO 27001 (Information Security Management System) and other best practices. These policies and procedures are regularly reviewed to be relevant and up-to-date with international standards & best practices, as well as technological developments. These policies and procedures are also a reference for the Company's Subsidiaries.

c. Security Operation Center (SOC)

Bank Mandiri implements optimal best-in-class security devices according to the function and application of layered architecture to secure the Bank's systems and data, as well as identify and block security event anomalies at each layer, namely:

1. Applications accessed by customers, for example: Securing transactions with a PIN.
2. Network, example: Firewall equipped with Intrusion Prevention System (IPS).
3. Endpoint (PC/Laptop), example: Antimalware.
4. Server (Branch Server & Data Center), example: Antimalware.

In dealing with the threat of cyber-attacks, Bank Mandiri has the capability to detect and handle cyber-attacks through the Security Operation Center (SOC) which operates for 7x24 hours. SOC together with related work units are registered as Bank Mandiri Computer Security Incident Response Team (CSIRT) registered with the State Cyber and Encryption Agency (BSSN) to collaborate, facilitate coordination, and share information if there is a cyber incident. In responding and handling cyber incidents, Bank Mandiri CSIRT implements an incident response plan consisting of the following stages:

- Identification: includes the process of detecting and receiving cyber incident reports.
- Handling & escalation: includes the process of cyber incident analysis, isolation/containment of affected systems, follow-up destruction/ eradication to stop cyber incidents, and recovery to restore the entire system to normal work as before.

These stages are carried out in conjunction with periodic escalation and reporting to relevant stakeholders & regulators.

CSIRT conducts regular testing and simulation of cyber incidents to train the readiness of organizations and employees to respond to incidents. Every cyber event and incident is managed consistently, effectively and measurably.

SOC proactively follows up on information on the development of cyberattacks from the reputable Threat Intelligence Service. In addition, Bank Mandiri also builds internal capabilities to conduct threat hunting in providing online protection for brands & websites from threats such as phishing, online scams, unauthorized access and counterfeit.

d. Cyber Security Forum

Bank Mandiri's seriousness in monitoring information security is expressed by the direct involvement of the Board of Commissioners and Directors in this topic through the Risk Oversight Committee, Audit Committee and Integrated Governance Committee which are carried out regularly. The agenda of discussion at the committee meeting included reporting on ESG initiatives in