INFORMATION TECHNOLOGY SECURITY

Amid increasing technological complexity and stringent regulatory requirements, Bank Mandiri continues to strengthen its management of data security and protection against cyber threats. The Bank implements various proactive measures such as process automation, the enforcement of strict security policies, periodic system updates, and regular training for all employees. The risk management unit plays a role in identifying and mitigating cyber risks, ensuring compliance with regulations and best practices, while also enhancing employee awareness through various educational platforms. In addition, the Bank conducts capacity planning to maintain service availability and prepares incident handling procedures that are tested periodically. To further strengthen the quality of information security, Bank Mandiri implements a layered IT security strategy in accordance with regulatory requirements and aligned with international standards (ISO 27001) and best practices (NIST Cybersecurity Framework, COBIT Framework, PCI Security Standard), as well as other relevant frameworks. All of these initiatives are integrated into an information security management system that focuses on three main pillars: People, Process, and Technology, ensuring that the Bank remains resilient, innovative, and competitive.

The implementation of strategy and development of a layered information security management system are structured into three main areas, namely People, Process, and Technology, with the following brief explanations:

1. **People**

   Bank Mandiri continues to strengthen the People aspect of information security through security awareness programs and human capital development. Through the security awareness program, the Bank fosters a culture of information security among all employees by conducting annual security awareness certification for all staff members across all levels, both in domestic and overseas offices. The program is complemented by regular security awareness campaigns delivered through newsletters, posters, and phishing drills. Security awareness campaign materials in the form of posters are also shared with all Bank Mandiri partner companies and all entities within the Mandiri Group as a reference for implementing security awareness initiatives within their respective organizations. Several campaign topics that have been conducted include data protection, maintaining data confidentiality, the latest cyber attack trends, methods to identify and avoid phishing, and online transaction security. In addition, security awareness for customers is enhanced through educational programs delivered across the Bank's official channels, such as its website, social media platforms (Instagram, Facebook, Twitter), and other dedicated channels.

   At the same time, Bank Mandiri continuously enhances the competencies of its human resources through training and certification programs for employees, including but not limited to CISSP (Certified Information Systems Security Professional), Offensive Security Certified

Professional (OSCP), and Certified Network Defender (CND). In addition, product-based training is conducted to deepen expertise in the Bank's security systems, as well as training programs for vendor and contractor personnel who support operational activities. Soft skill development is also provided through training programs covering leadership mindset, strategic thinking, creative thinking, design thinking, problem solving, presentation skills, and negotiation skills. All training programs are delivered through both onsite and online (virtual) methods via public platforms to ensure optimal enhancement of capacity and capability.

2. **Process**

Bank Mandiri strengthens the Process aspect in managing information security through the implementation of comprehensive and layered governance mechanisms. The application of the Three Lines of Defense (3LoD) ensures a clear division of roles, starting from the CISO Office Group as the first line, which is responsible for security architecture design, policy development, as well as 24/7 monitoring and incident response operations; SOR IT as the 1.5 line, which conducts testing of the effectiveness of operational controls; the Operational Risk Group as the second line, which establishes the bank-wide risk management framework; and Internal Audit as the third line, which performs independent assurance functions.

Process strengthening is also carried out through the formulation and implementation of Security Policies and Procedures that are periodically reviewed and aligned with regulatory requirements (BI and OJK) as well as international standards such as ISO 27001, the NIST Cybersecurity Framework, CIS Benchmark, and the PCI Security Standard. These information security policies and provisions are also communicated to all entities within the Mandiri Group as references for implementation in strengthening information security governance, taking into account the complexity of systems within each respective entity.

In its cybersecurity operations, Bank Mandiri relies on a Security Operation Center (SOC) that operates 24/7 to conduct monitoring, detection, and mitigation of threats through threat intelligence and threat hunting activities. Incident response capabilities are further strengthened through the Computer Security Incident Response Team (CSIRT), which is registered with BSSN, with incident handling mechanisms covering identification, isolation, eradication, and recovery, in accordance with SEOJK No. 29/SEOJK.03/2022.

Bank Mandiri's strong commitment to monitoring information security is reflected in the direct involvement of the Board of Commissioners and the Board of Directors in this area through the Risk Oversight Committee, Audit Committee, and Integrated Governance Committee, which convene regularly. Agenda items discussed in these committee meetings include the achievement of ESG aspects related to Privacy and Data Security, the effectiveness of layered security systems, and compliance with Mandiri Group's security standards. Updates on cyber resilience across the Mandiri Group, including the fulfilment of Mandiri Group's information security standards, are also discussed, covering control measures implemented to anticipate and safeguard against cyber attacks, which are treated as non-negotiable requirements.

In order to maintain and evaluate cyber resilience and security, as well as to strengthen readiness in incident response processes, Bank Mandiri periodically conducts cyber resilience and security testing in accordance with applicable regulations (SEOJK No. 29/SEOJK.03/2022 on Cyber Resilience and Security for Commercial Banks), including:

1. Penetration Testing: Testing conducted based on vulnerability analysis of devices and applications supporting operational and business activities.
2. Phishing Drill: A simulation of social engineering attacks on employees in the form of phishing emails, aimed at testing employees' readiness to respond to phishing emails securely.
3. Adversarial Attack Simulation Exercise (AASE): A real-life hacker attack simulation conducted by independent consultants to identify potential security gaps within Bank Mandiri's IT operations.
4. Cyber Range Exercise: Cybersecurity testing based on hands-on scenario simulations within an isolated environment, aimed at enhancing technical skills through real-life experience in detecting, analyzing, and responding to cyber threats.

In addition, to anticipate information security risks arising from third parties (supply chain) that collaborate with the Bank, Bank Mandiri regularly conducts vendor security assessments on third-party organizations covering people, process, and technology aspects, in accordance with the scope of their involvement and engagement with Bank Mandiri. These reviews are carried out through several methods, including questionnaires, interviews, and/or site visits.

All of these processes collectively form a robust and measurable information security governance system that is aligned with industry standards and regulatory requirements.

3. **Technology**

Bank Mandiri maximizes the implementation of industry-leading security solutions in safeguarding digital information and assets through the adoption of a layered architecture and best-in-class technologies, including:

a. Applications accessed by customers and employees, such as Multi-Factor Authentication (MFA) and Web Application Firewall (WAF).
b. Network, such as firewalls equipped with Intrusion Prevention System (IPS) and Network Access Control (NAC).
c. Endpoints (personal computers/laptops and servers), such as Endpoint Detection & Response (EDR), antivirus and antimalware, as well as security patches.
d. Access management, such as Identity Access Management (IAM) and Privileged Access Management (PAM), complemented by Privileged Threat Analysis (PTA).
e. Data protection, such as the implementation of encryption and Data Loss Prevention (DLP).

As part of its commitment to continuous improvement, Bank Mandiri consistently enhances its IT security capabilities through strategic investments across all layers of security, further strengthened by the utilization of artificial intelligence (AI) and machine learning technologies.