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

BUMN
livin' by mandiri
hidup itu banyak warna,
kalo banyak kena tipu itu, apes!
Penipu
yuk waspada sama telepon tipu-tipu >>
livin'

BUMN
mandiri
ada-ada aja cara penipu
buat nguras tabungan kamu!
Waspada dengan file APK/Apk palsu
Telepon dari penipu
Menang undian halu
Sosmed tipu-tipu
Ingat! selalu jaga data rahasia kamu yaa
livin'

BUMN
livin' by mandiri
awas modus baru
+628123456789
jangan ketipu aplikasi bodong
yang bisa bikin rekening kosong melompong
livin'
<<< SWIPE

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 the quarterly Privacy & Data Security aspect, multi-layer defense mechanism, and fulfillment of Mandiri Group's security requirements.

e. **Cybersecurity Testing**
To maintain and evaluate resilience and cybersecurity, Bank Mandiri periodically conducts resilience and cybersecurity tests in accordance with applicable regulations, as follows:

1. Based on vulnerability analysis, Bank Mandiri conducts penetration testing for every new application development and periodically for internet-facing and/or very critical applications at least once a year. Penetration testing is carried out by external independent parties certified by international penetration tester standards.

2. Bank Mandiri conducted scenario-based testing through activities:
   a. Table-top Exercise (Cybersecurity Drill)
   This testing activity is based on discussions where each personnel from across work units gathers and discusses handling and countermeasures in the event of a cyber incident in accordance with their respective duties. This testing activity is carried out by involving relevant work units, including IT units, risk management units, business continuity units, customer care units, and corporate secretary units. Examples of scenarios that have been tested include: ransomware attacks, illegal hacking, unauthorized access, data leakage, e-mail threats, and others.

   Bank Mandiri collaborates with reputable international consultants (external independent parties) in the preparation of scenarios and the implementation of table-top exercise activities to adopt the latest cyber-attack trends and best practices for testing implementation.

   b. Social Engineering Exercise (Phishing Drill)
   The testing activity was by simulating a social engineering (phishing) attack via email asking employees to divulge sensitive information such as passwords. This testing activity is carried out using a phishing drill tool that can automatically send a simulated phishing e-mail to all employees. This activity aims to assist employees in identifying and reporting if they receive phishing emails in a near-real experience.

   c. Adversarial Attack Simulation Exercise (AASE)
   Testing activities by simulating real-life attacks by reputable international consultants (external independent parties) who use the latest and customized tactics, techniques, and procedures of cyberattacks in the real world by targeting aspects of people, process, technology to test cyber resilience. This testing activity is carried out at least in collaboration with reputable international consultants (external independent parties) in the preparation of scenarios and the implementation of AASE activities to adopt the latest cyber-attack tactics, techniques, and procedures as well as best practices for conducting tests. Examples of scenarios that have been tested include: Getting unauthorized access, theft of application source code from the code repository, disabling defense systems, and theft of confidential data from the Data Center.

INFORMATION TECHNOLOGY SECURITY

The results of the resilience and cybersecurity tests are reported to the Board of Directors and regulators in accordance with relevant regulations.

f. **Third Party Security Review**
Bank Mandiri is aware of the risk of information security threats from third parties (supply chain) in collaboration with Bank Mandiri. As such, Bank Mandiri routinely conducts information security reviews implemented by third party organizations (people, process, technology) in accordance with the scope of their interests and involvement with Bank Mandiri. This review is carried out through several methods such as filling out questionnaires, interviews, and/or site visits.

Furthermore, to measure and evaluate the optimization of the information security process, Bank Mandiri conducted a series of assessment activities by the dependent external assessor, namely the State Cyber and Encryption Agency (BSSN) related:

a. **Cyber Security Maturity (CSM) assessment** with maturity level 5 – "**Optimal**" (highest score). CSM Assessment is an instrument from BSSN to assess the level of cybersecurity maturity of an organization, including the assessment of the maturity of management and protection of personal data confidentiality (data privacy).

b. **Measurement of Incident Handling Maturity Level (TMPI)** with the result of maturity level 5 – "**Optimise**" (highest value). TMPI is a tool to map the level of organizational readiness in responding to and recovering cybersecurity incidents, including detecting and responding if there is an incident of personal data leakage due to system security gaps.

3. **Technology**
Bank Mandiri conducts multi-layer defense mechanism starting from securing applications, networks, and systems that use best-in-class technology and are always up-to-date on technological developments relevant to the latest cybersecurity trends. Bank Mandiri actively secures technology from various sides, including:

a. **Information Security Architecture**
The Bank continuously improves capabilities through investment in every layer of IT security, namely endpoint security, network security, application security, data security and IT infrastructure security. Furthermore, Bank Mandiri also builds anomalous network & account activity detection capabilities by utilizing AI and machine learning technology.

b. **Endpoint Security**
In supporting endpoint security from all inherent vulnerabilities, Bank Mandiri implements Virtual Private Network, Network Access Control (NAC), antivirus/antimalware, Endpoint Detection Response (EDR), disk encryption, Multi Factor Authentication (MFA) and others.

c. **Network Security**
The use of layered and redundant tools to make the internal network more resilient, Bank Mandiri implements an Intrusion Prevention System, Anti-DDoS, Antispam, Virtual Patch and Web Application Firewall. Security devices are placed in the Data Center & Disaster Recovery Center, to maintain service availability and readiness for business continuity (Business Continuity Plan).

d. **Application Security**
Bank Mandiri has adopted the Agile Development method to support business needs quickly. Both methods are equipped with testing stages that use Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) techniques. In addition, source code management also includes security source code review.

Bank Mandiri also has digital forensic capabilities that support the security incident investigation process to support post-incident recovery, improve security posture and prevent similar incidents.

e. **Data Security**
The implementation of Bank and customer data/information security has been implemented at every stage in the data lifecycle, namely when Data-in-Use, Data-in-Transit and Data-at-Rest. The use of Data Loss Prevention (DLP) tools can prevent data leakage both intentional and unintentional, and provide security for personal data.

f. **Infrastructure Security**
Bank Mandiri carries out maintenance of IT infrastructure security devices by paying attention to the expiration period (technology obsolescence) of the system used. In addition, security measurement and strengthening activities are carried out periodically through vulnerability assessment (VA), patching hardening, and penetration testing. Similarly, security in terms of managing access rights and provisioning user IDs is carried out centrally through Identity Management. Meanwhile, the management of access rights with the highest authority (power user) is carried out using Privileged Access Management (PAM) which is equipped with the Privileged Threat Analytics (PTA) feature to detect and notify the rules that have been defined.

INFORMATION SECURITY MANAGEMENT IMPLEMENTATION IN 2023

Bank Mandiri realizes the important role of resilience and cybersecurity in supporting the digitization of Bank services to customers. As a continuous improvement measure in increasing customer trust and the Bank's reputation, Bank Mandiri implements regulation-based information security management, international standards & best practices. This is shown by several certifications and accreditation achievements, including:

- ISO 27001:2013 (Information Security Management System) certification for:
  a) Provision of application development and IT operation related to Livin' by Mandiri
  b) Security Operation Centre to manage cyber security threats in banking systems & cyber operations
  c) Provision of Infrastructure and Operational Data Center and Disaster Recovery Center
- ISO 17025:2017 Accreditation for CISO Office Group Digital Forensics Laboratory granted by the National Accreditation Committee (KAN)

ISO 27001:2013 and ISO 17025:2017 Certification

CERTIFICATE

PT Bank Mandiri (Persero) Tbk

ISO/IEC 27001 : 2013

bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

...making excellence a habit.™

CERTIFICATE

PT Bank Mandiri (Persero) Tbk - IT Infrastructure Group

ISO/IEC 27001 : 2013

SERTIFIKAT AKREDITASI

Laboratorium Forensik Digital PT Bank Mandiri (Persero) Tbk

PLAZA MANDIRI, lantai 29, CISO Office Group, Jl. Jenderal Gatot Subroto Kav. 36-38, DKI Jakarta