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