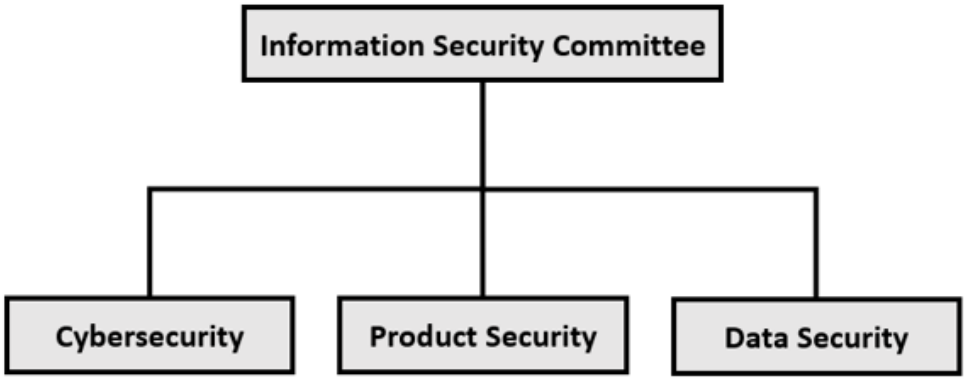
Information Security Risk Management Policy

• Information Security Risk Management Structure

MediaTek Inc. ("**MediaTek**") establishes Information Security Committee (the "**Committee**") in order to manage information security risks. The chairperson of the Committee is the executive vice president. The Committee is accountable for reviewing the execution of cybersecurity, product security, and data security regularly and reporting the result of information security safety checks to the Board of Directors periodically. The Committee convenes at least once every six months and holds additional meetings at all times depending on the needs of information security risk management. The chairperson of the Committee also reports to the Board of Directors once a year.

- Cybersecurity: Cybersecurity management, planning, supervision, and implementation are included.
- Product Security: Planning and implementation of product security framework, industry compliance, procedure formulation, education and training, threat modeling, testing regulations, vulnerability management, etc. are included.
- Data Security: Drafting, implementation, and discussion of intellectual property information management practices are included.



- ## Information Security Strategy

1. To effectively implement information security management, MediaTek shall establish and implement an Information Security Management System (hereinafter referred to as the "**ISMS**")[1] following ISO/IEC 27001 standards and requirements and shall create control mechanisms under the National Institute of Standards and Technology Cybersecurity Framework (hereinafter referred to as the "**NIST CSF**") to integrate the information security control mechanism into the daily operation process.

2. MediaTek shall ensure the confidentiality, integrity, and availability of its information to decrease the risk of any unauthorized use, damage, or leakage of information and shall ensure all internal information security management rules comply with the requirements of information security related laws, regulations, and policies.

3. To maintain customers' confidence in product security, MediaTek shall establish effective control measures to ensure that products are free from security or privacy vulnerabilities, including but not limited to security requirements and architecture analysis, threat analysis, code scanning, security incident response, and vulnerability management.

4. MediaTek shall adopt a defense-in-depth strategy to set up safeguards proactively before any incident happens and shall take essential emergency actions upon the occurrence of incidents to minimize the potential damages resulting from such incidents and improve MediaTek's information security resilience.

5. To enhance the understanding and knowledge of MediaTek's personnel toward information security, MediaTek shall promote the concept that "everyone shall be accountable for information security" through employee training programs.

- ## Information Security Requirement for Suppliers

MediaTek requests all suppliers of MediaTek to comply with the information security policies of MediaTek and sign necessary information security contracts and confidentiality agreements with MediaTek before cooperation.

[1] MediaTek operates an Information Security Management System which complies with the requirements of ISO27001 and achieved ISO27001 certification in 2022 (Effective Date: 2022/12/6-2025/10/31).

- ## Information Security Control Mechanisms

  MediaTek shall refer to NIST CSF to formulate information security defense and control mechanisms.

Identify	MediaTek develops risk management strategies that meet daily operations by inspecting environments, key sources, and services, including formulating information security regulations and establishing the asset management system.
Protect	MediaTek formulates and implements defensive measures to strengthen the key sources and services, including Identity Access Management ("**IAM**"), anti-virus software, endpoint protection, and system patch management.
Detect	MediaTek establishes the real-time detection and warning mechanism for incidents, including the email protection system, intrusion detection system, and Security Operations Center ("**SOC**"), and periodically inspects the information security architecture.
Respond	MediaTek establishes Cyber Security Incident Response Team ("CSIRT") to be accountable for incident responses, such as incident investigation, forensics, and proposing improvement solutions. All incidents shall be reported and dealt with in accordance with MediaTek's information security rules of procedure.
Recover	MediaTek sets up data recovery plans to be able to resume normal within the shortest possible time upon the occurrence of any information security incident which affects operation.