1 Purpose：

The purpose of this information security manual is to define the information security requirements for all employees of Porite Taiwan Co., Ltd ("the company"). The manual is designed to help employees protect the Company's information assets, including confidential data, intellectual property, and systems. The company aims to achieve the following two goals:

1.1 To assist users in the smooth operation of all business activities, ensure the security of all information media, and achieve the Company's information security goals.

1.2 To comply with domestic and international automotive cybersecurity regulations, improve cybersecurity measures in the product development process, enhance customer confidence to enhance corporate brand value and competitiveness.

2 Scope：

Applies to all employees. Including regular employees, contract employees, dispatched personnel, as well as external visitors, vendors, and other personnel hired by the company.

3 Authorities：

Responsibility Units of The Company's Information Security Management System and TISAX.

4 Definition of terms：

4.1 Information Security

It includes ensuring the confidentiality, integrity, and availability of information, so that information can be securely, accurately, appropriately, and reliably used for the planning, execution, management, and related activities to achieve the business objectives of the company.

4.2 Information Security Management System

The Information Security Management System (ISMS) is part of the overall management system. Based on a risk-driven approach, it is used to plan, establish, implement, operate, monitor, audit, maintain, and improve an information security management system.

4.3 Confidentiality

Ensuring that only authorized users can access information.

4.4 Integrity

Ensuring the accuracy and completeness of information and information processing methods.

4.5 Availability

Ensuring that authorized users can access information and related assets in a timely manner when needed.

5 Operation content：

5.1 Information Security Management System

5.1.1 Overview

5.1.1.1 To demonstrate our commitment to the comprehensive implementation of information security management, ensuring the appropriate protection of all information and information systems, we establish, document, implement, and maintain an Information Security Management System in accordance with the requirements of ISO/IEC 27001:2022 and TISAX standards. We are dedicated to continuously improving the effectiveness of our system.

5.1.1.2 The first to fourth level documents of the information security management system are developed based on the ISO/IEC 27001:2022 standard. Appropriate control measures are selected to formulate the "Statement of Applicability" (8012-0001-0001), which outlines the control points and verification scope adopted by the company.

5.1.1.3 The company's "Information Security Statement" (8012-0001-0002) and (8012-0001-0003) are appropriately aligned with the Information Security Manual.

5.1.2 Information Security Objectives

5.1.2.1 Implementing appropriate protection and preventive measures for the information stored or transmitted by the company.

5.1.2.2 Reducing the impact of information security incidents such as damage, theft, leakage, tampering, abuse, and infringement.

5.1.2.3 Continuously improving the confidentiality, integrity, and availability of all operations related to information services systems.

5.1.3 Measurement of Objectives

The measurement objectives of information security management system should be explained in terms of how the effectiveness of the objectives will be measured, how these measurements will be used to evaluate control measures, the timing of measurements, and how comparable and reproducible results will be generated. This process aligns with the 'Information Security Indicator Management Regulations' (8011-0004G).

5.1.4 Operation Mechanism

The company follows the "Plan-Do-Check-Act" (PDCA) cycle, as outlined in the ISO/IEC 27001:2022 standard, to establish and implement an Information Security Management System, and to maintain its effective operation and continuous improvement.

5.1.4.1 Planning and Establishment (Plan): Based on the overall strategy and objectives of the company. In order to establish an Information Security Management System, an Information Security Management Organization is established to control potential threats and vulnerabilities, plan risk assessments, as well as design and implement control mechanisms.

5.1.4.2 Implementation and Operation (Do): Establish and revise the necessary control mechanisms based on the results of the planned assessments.

5.1.4.3 Monitoring and Auditing (Check): Monitor the implementation of operations of the information security management system, and evaluate and audit their effectiveness.

5.1.4.4 Maintenance and Improvement (Act): Implement corrective measures and improvements based on the results and recommendations of auditing. Continuously maintain the operation of the information security management system and its control mechanisms.

5.2 Management Responsibility

5.2.1 Establish an Information Security Management Organization. Responsible for promoting, coordinating, and overseeing the following matters:

5.2.1.1 Approval, dissemination, and supervision of information security policies.

5.2.1.2 Allocation and coordination of information security responsibilities.

5.2.1.3 Advocate for compliance with information security objectives, responsibilities under information security policies and legal norms, and the need for continuous improvement.

5.2.1.4 Provide adequate resources to establish, implement, operate, monitor, review, maintain and improve information security management systems.

5.2.1.5 Criteria for determining acceptable risk and acceptable risk level.

5.2.1.6 Formulate information security audit plans, assess information risks and perform information security tests from time to time.

5.2.1.7 Conduct management reviews of the information security management system.

5.2.1.8 Identify internal and external stakeholders in the information security management system, consider their information security needs and expectations of the company, and determine internal and external communication.

5.2.1.9 Review and monitor information security incidents and consider internal and external issues that may affect the information security management system.

5.2.1.10 Implement information security related education training and publicity every year to evaluate the effectiveness of information security education and training provided.

5.2.1.11 Approval of other information security matters.

5.2.2 Management Review

The management review process of our company is carried out by the Information Security Management Committee. The management team should conduct a management review at least once a year to ensure the adequacy, effectiveness, and appropriateness of the information security management system. The review scope includes the assessment of improvement plans and change requirements for the information security management system. The results of the review should be documented thoroughly and retained appropriately.

5.2.3 Information Security Indicators

The company should establish information security indicators to assess the performance of information security and the effectiveness of the information security management system. The information security indicators should include at least the items to be measured, methods, timing, frequency, and responsible personnel to ensure the effectiveness of measuring information security indicators. The information security indicators should be appropriately aligned with the company's information security policies.

5.2.4 Information Security Internal Audit

Management should ensure that security assessments or audits are conducted regularly or irregularly to review whether the control objectives, measures and procedures comply with relevant standards, laws and regulations or information security requirements, and effectively implement and maintain them in accordance with the expected plan so as to continuously enhance the effectiveness of the information security management system.

5.2.5 Improvement of Information Security Management System

5.2.5.1 Continuous Improvement

The company should continuously enhance the effectiveness of the information security management system through mechanisms such as internal and external audit results, analysis of information security incidents, corrective measures, and management reviews.

5.2.5.2 Corrective Measures

The company should implement appropriate control measures to reduce non-conformities identified during the establishment and operation of the information security management system. The operational procedures for corrective measures are as follows:

5.2.5.2.1 Identification of Non-Conformities.

5.2.5.2.2 Determination of causes for Non-Conformities.

5.2.5.2.3 Evaluation of required corrective measures to ensure Non-Conformities do not recur.

5.2.5.2.4 Determination and Implementation of required corrective measures.

5.2.5.2.5 Recording and reviewing the effectiveness of implemented corrective measures.

5.2.6 Document Management System

5.2.6.1 Document Control

The control, issuance, and change of information security documents related to the company's information security management system should be carried out in accordance with the procedures specified in the company's document control-related operational procedures for the first to fourth level information security documents.

5.2.6.2 Record Control

Any documents, forms and records generated by the operation of the company's information security management system shall be properly kept by designated record keepers, and the retention period and review authority shall be specified to facilitate the tracking of the implementation of the information security management system and maintain the effective operation of the system.

5.2.7 Information Security Policy Direction and Review

The information security policy of the company should be evaluated, reviewed, and revised at least once a year to ensure that it aligns with the needs and expectations of internal and external stakeholders, and to ensure the effectiveness of information security practices.

5.2.8 Compliance with regulations and laws implementation.

All personnel must adhere to this information security policy, and violations will be subject to disciplinary actions according to the relevant company regulations. In cases involving criminal or legal liability, such as the Trade Secrets Act, Copyright Act, Personal Data Protection Act, etc., legal responsibilities will be pursued based on the circumstances.

6. Related operation methods

Code	Name of Regulation/Instruction
8011-0001G	Information Security Management System Implementation Regulation
8011-0002G	Information Security Document and Records Management Regulation
8011-0004G	Information Security Indicator Management Regulation
8011-0015G	Information Security Audit Operation Management Regulation

7. Form Index

Form Code	Form Name
8012-0001-0001	Declaration of suitability
8012-0001-0002	Information Security Statement_
8012-0001-0003	Information Security Statement_

Document Modify Record		
Ver.	Modify Date	Modify Content
1^{st}	2023/03/29	ISMS Implementation
2nd	2023/11/20	TISAX Audit Adjustment