台灣半導體股份有限公司

Taiwan Semiconductor Co., Ltd.

資訊安全政策

Information Security Policy

文件編號 Document No.	ISMS-1-00001
初次發行日期 Initial Issue Date	2024-12-24
修訂發行日期 Revision and Issue Date	
版本 Version	V1.0

版本記錄 Version History

版本 Version	日期 Date	修訂說明 Description	備註 Note
1.0	2024-12-24	初版 Initial Release	

目 錄 Table of Contents

1. 目的 Purpose

台灣半導體股份有限公司 (以下簡稱台半) 鑑於資訊安全乃維繫各項服務安全運作之基礎，更對品牌信譽有重要的意義，特訂定本政策，宣示台半提供安全無虞服務的決心與承諾，並作為台半資訊安全工作之指導方針，以保護台半重要資產免受內部或外部，蓄意或意外之威脅。

Taiwan Semiconductor Co., Ltd. (hereinafter referred to as TSC) recognizes that information security is the foundation for ensuring the secure operation of all services and holds critical importance for brand reputation. This policy is established to declare TSC's determination and commitment to providing secure and reliable services. It serves as a guiding principle for TSC's information security efforts to protect critical assets from internal or external, intentional, or accidental threats.

2. 目標 Objectives

台半資訊安全目標為：建置符合國際標準所要求之資訊安全管理系統 (Information Security Management System，以下簡稱 ISMS)，確保各項服務符合機密性 (Confidentiality)、完整性 (Integrity)、可用性 (Availability) 與適法性 (Compliance) 之要求。並依各階層與職能定義及量測資訊安全績效之量化指標，以確認資訊安全管理系統實施狀況及是否達成資訊安全目標並持續改善之。

The goal of TSC’s information security policy is to establish an Information Security Management System (ISMS) in compliance with international standards. This ensures that all services meet the requirements of Confidentiality, Integrity, Availability, and Compliance. Quantitative performance indicators for information security are defined and measured according to levels and functions to evaluate the implementation of the ISMS, confirm achievement of information security objectives, and ensure continuous improvement.

3. 聲明 Statement

以符合資訊安全管理目標為原則，特訂定台半資訊安全政策聲明為：「服務不間斷，資料不流失，個資不外洩」。

In alignment with the objectives of the ISMS, TSC’s information security policy statement is as follows:
"Uninterrupted Services, No Data Loss, and No Personal Information Leakage."

4. 適用範圍 Scope

本資訊安全管理系統考量內部及外部議題、關注方之需要與期望，以及台半活動與其他組織活動間之介面及相依性，適用範圍為：「資訊通訊安全課、網路及機房維運與管

理」。

The ISMS considers internal and external issues, the needs and expectations of interested parties, and the interfaces and interdependencies between TSC activities and other organizational activities. The scope applies to **"Information and Communications Security Division, Network and Data Center Maintenance and Management."**

5. 涵蓋內容 Coverage

資訊安全管理系統包括內容如下，有關單位及人員就下列事項，應訂定對應之管理規範或實施計畫，並據以實施及定期評估實施成效：

- 資訊安全組織與管理審查
- 文件與紀錄管理
- 資產管理
- 風險管理
- 人力資源安全管理
- 實體環境安全管理
- 存取控制管理
- 資訊系統獲取、開發與維護管理
- 營運持續管理
- 績效管理
- 供應商關係管理
- 資訊安全內部稽核
- 運作安全與密碼學技術管理
- 通訊安全管理
- 遵循性管理
- 資訊安全事故管理

The ISMS includes the following areas. Relevant units and personnel shall establish corresponding management regulations or implementation plans, execute them, and regularly evaluate their effectiveness:

- Information security organization and management review
- Documentation and record management
- Asset management
- Risk management

- Human resource security management
- Physical and environmental security management
- Access control management
- Information system acquisition, development, and maintenance management
- Business continuity management
- Performance management
- Supplier relationship management
- Internal audits of information security
- Operational security and cryptographic techniques management
- Communication security management
- Compliance management
- Information security incident management

6. 組織與權責 Organization and Responsibilities

為確保資訊安全管理系統能有效運作，應明定資訊安全組織及權責，以推動及維持各類管理、執行與查核等工作之進行。

To ensure the effective operation of the ISMS, the organization and responsibilities of information security shall be clearly defined. This facilitates the promotion and maintenance of various management, implementation, and auditing tasks.

7. 實施原則 Implementation Principles

資訊安全管理系統之實施應依據規劃 (Plan)、執行 (Do)、查核 (Check) 及調整 (Act) 流程模式，確保資訊業務運作之有效性及持續性。

The implementation of the ISMS shall follow the Plan-Do-Check-Act (PDCA) cycle to ensure the effectiveness and continuity of information security operations.

8. 審查與評估 Review and Evaluation

8.1. 本政策應於資訊安全管理系統發生重大變更時審查或於年度管理審查會議時進行審查，以反映相關法令法規、技術、業務及相關部門等最新發展現況，確保資訊安全實務作業之有效性。

8.2. 本政策應依據審查結果進行修訂，並經召集人簽核發佈後始生效。

8.3. 本政策訂定或修訂後應以書面、電子郵件、文件管理系統或其他方式告知相關關注方，如：所屬員工、契約客戶、供應商、合作夥伴等。

8.1. This policy shall be reviewed when significant changes occur in the ISMS or during the annual management review meeting to reflect the latest developments in laws, regulations, technologies, business, and related departments, ensuring the effectiveness of information security practices.

8.2. Revisions to this policy shall be made based on the review results and become effective only after approval and issuance by the convenor.

8.3. After formulation or revision, this policy shall be communicated to relevant interested parties through written notifications, emails, document management systems, or other methods. These parties include employees, contractual clients, suppliers, and partners.

本政策包含中英文版本，若有不一致者，應以中文版本為準。

In the case of any inconsistency between the English and Chinese versions of this policy, the Chinese version shall prevail.