文曄科技股份有限公司

資訊安全政策

文件編號：WTMEC-ISMS-A-01
機密等級：一般

版　　次：1.6

發行日期：2026.07.01

WT Microelectronics Co., Ltd.

Information Security Policy

Document No.：WTMEC-ISMS-A-01

Confidentiality Level：General

Version：1.6

Issue Date：2026.07.01

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
0.1	2022.05.24	All	DeKnow	草擬
1.0	2022.08.01	All	文曄科技	初版發行
1.1	2022.11.15	4-5	文曄科技	1. 增修 4.3 加註 CNS 27001 2. 增修 6 政策審查時機
1.2	2023.12.01	4	文曄科技	修訂 SLA 達 99%以上
1.3	2024.10.18	1、4	文曄科技	2.2.3 及 4.3 之「資訊安全官」調整為「資訊安全長」
1.4	2025.04.01	2-4	文曄科技	修訂管理範圍
1.5	2026.03.24	All	文曄科技	文字勘誤與敘述潤飾
1.6	2026.07.01	2-7	文曄科技	1. 修訂 5.1 量化指標 2. 移除 CNS 27001 標準引用

Revision Record

Version	Revision Date	Revised Pages	Revised By	Summary of Revision
0.1	2022.05.24	All	DeKnow	Draft
1.0	2022.08.01	All	WT	Initial release.
1.1	2022.11.15	4-5	WT	1. Added note on CNS 27001 to Section 4.3. 2. Added timing of policy review to Section 6.
1.2	2023.12.01	4	WT	Revised SLA to exceed 99%.
1.3	2024.10.18	1、4	WT	Changed "Information Security Officer" to "Chief Information Security Officer" in Sections 2.2.3 and 4.3
1.4	2025.04.01	2-4	WT	Revised scope of certification.
1.5	2026.03.24	All	WT	Typographical Corrections and Wording Refinement.
1.6	2026.07.01	2-7	WT	1. Revised the Quantitative Indicators to Section5.1. 2. Removed references to the CNS 27001 standard.

目　錄

1 目的 1

2 適用範圍 1

3 目標 3

4 責任 4

5 管理指標 5

6 審查 8

7 實施 8

8 相關文件 8

Table of Contents

1 Purpose 1

2 Scope of Application 2

3 Objectives 4

4 Responsibilities 4

5 Management Indicators 6

6 Review 8

7 Implementation 8

8 Related Documents 8

1 目的

為確保**文曄科技股份有限公司**（以下簡稱「**本公司**」）所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，遭受到內、外部之威脅，並衡酌**本公司**之業務需求，訂定本政策做為遵循依據，期有效及合理地降低營運風險。

1 Purpose

To ensure the confidentiality, integrity, and availability of the information assets of **WT Microelectronics Co., Ltd.** (hereinafter referred to as "**the Company**"), and to comply with applicable laws and regulations, this policy is established to protect information assets from improper use, disclosure, alteration, or destruction caused by human error, malicious actions, or natural disasters.

Taking into consideration **the Company**'s business requirements, this policy serves as the basis for information security management to safeguard against internal and external threats and to effectively and reasonably reduce operational risks.

2 適用範圍

2.1 本政策適用範圍為**本公司**及其所屬關係企業，百分之百直接或間接持有或控制、或為其提供銷售、服務之子公司及上述組織之全體人員、委外服務廠商、工讀生與訪客等。

2.2 範圍訂定應考量：

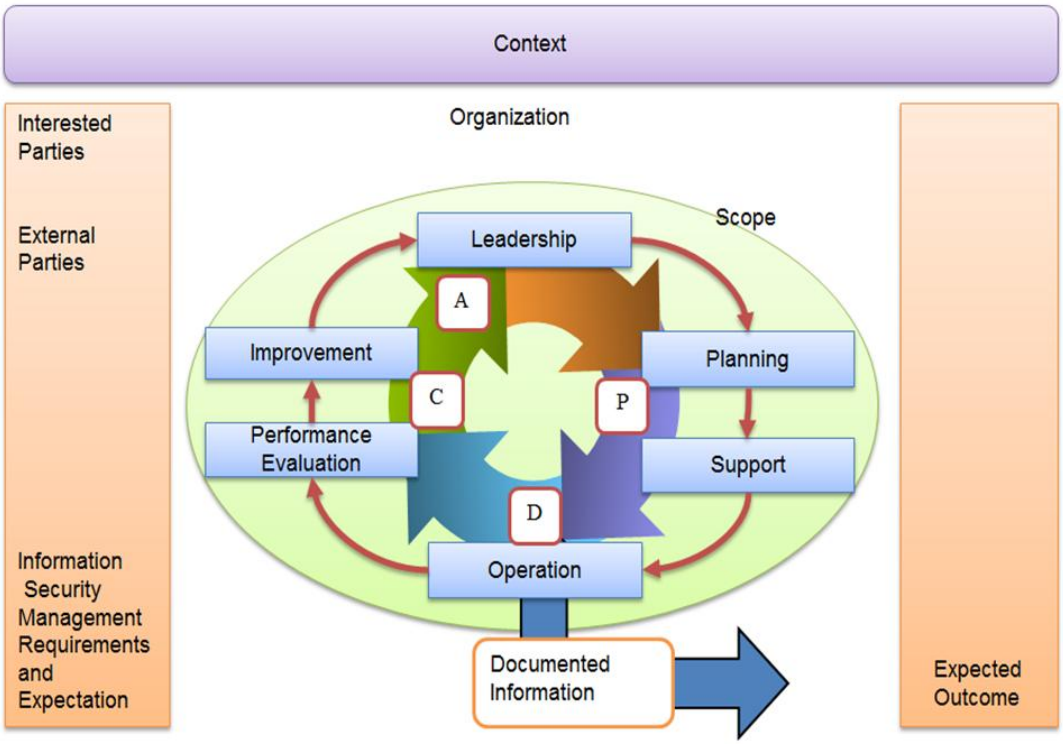
2.2.1 背景環境、內外部議題。

2.2.2 關注方（含法律、法規、合約）要求。

2.2.3 **本公司**與其他單位所執行之介面及相依性，以及利害關係人關注事項之鑑別

結果，應納入驗證範圍之評估，並呈現於「驗證範圍核定函」，經資訊安全長（CISO）核可。

2.3 依據 ISO/IEC 27001 持續改善循環的精神與意義，以「規劃-執行-檢查-改善」模式來建置與維護，確保此制度有效運作，降低**本公司**面臨之資安風險，包含：



2.3.1 組織全景

2.3.2 領導作為

2.3.3 規劃

2.3.4 支援

2.3.5 運作

2.3.6 績效評估

2.3.7 改善

2 Scope of Application

2.1 This policy applies to **the Company** and its affiliated enterprises, including subsidiaries that are directly or indirectly 100% owned or controlled, or that provide sales or services on behalf of **the Company**, as well as all personnel of the aforementioned organizations, outsourced service providers, interns, and visitors.

2.2 The scope shall be determined with consideration of:

2.2.1 Environmental background, internal and external issues.

2.2.2 Requirements of interested parties (including legal, regulatory, and contractual obligations).

2.2.3 The interfaces and interdependencies between the Company and other units, together with the results of identifying interested parties' concerns, shall be included in the assessment of the ISMS verification scope, documented in the "Scope of Verification Approval Letter," and approved by the Chief Information Security Officer(CISO).

2.3 In accordance with the principles and spirit of continual improvement defined in ISO/IEC 27001, the Information Security Management System (ISMS) shall be established and maintained using the Plan–Do–Check–Act (PDCA) model to ensure the effective operation of the system and to reduce the information security risks faced by **the Company**, including:

2.3.1 Organizational Overview

2.3.2 Leadership Commitment

2.3.3 Planning

2.3.4 Support

2.3.5 Operation

2.3.6 Performance Evaluation

2.3.7 Improvement

3 目標

為維護**本公司**資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全，期藉由**本公司**全體同仁共同努力以達成下列目標：

3.1 確保**本公司**業務資訊需經權責單位授權才可存取，以維護其機密性。

3.2 確保**本公司**業務資訊之正確與完整，避免被竄改或損壞。

3.3 確保**本公司**資訊服務之持續運作，以維持 ERP 系統相關業務可用性。

3.4 確保**本公司**各項業務之執行須符合相關法令或法規之要求。

3 Objectives

To protect the confidentiality, integrity, and availability of **the Company**'s information assets and safeguard the privacy of user data, **the Company** strives to achieve the following objectives through the collective efforts of all employees:

3.1 Ensure that access to **the Company**'s business information is granted only upon authorization by relevant authorities to maintain confidentiality.

3.2 Ensure the accuracy and integrity of **the Company**'s business information to prevent tampering or damage.

3.3 Ensure the continuous operation of **the Company'**s information services in order to maintain the availability of ERP-related business operations.

3.4 Ensure that all **Company** operations are conducted in compliance with applicable laws and regulations.

4 責任

4.1 **本公司**應成立資訊安全組織統籌資訊安全事項推動。

4.2 管理階層應積極參與並支持資訊安全管理制度，並透過適當標準及程序實施本政策。

4.3 應確保組織運行之管理系統符合 ISO/IEC 27001 要求，並負責向**本公司**資訊安全長（CISO）報告資訊安全管理成效。

4.4 **本公司**全體人員、委外服務廠商、工讀生與訪客等皆應遵守本政策。

4.5 **本公司**全體人員均有責任透過適當通報機制，通報資訊安全事件或弱點。

4.6 任何危及資訊安全之行為，將視情節輕重依**本公司**相關規定進行議處。

4 Responsibilities

4.1 **The Company** shall establish an information security organization to coordinate

and promote information security initiatives.

4.2 Management shall actively participate in and support the information security management system and implement this policy through appropriate standards and procedures.

4.3 It shall be ensured that the organization's management system complies with ISO/IEC 27001 standards and that the effectiveness of information security management is reported to **the Company**'s Chief Information Security Officer (CISO).

4.4 All **Company** personnel, outsourced service providers, interns, and visitors shall comply with this policy.

4.5 All **Company** personnel are responsible for reporting information security incidents or vulnerabilities through appropriate reporting mechanisms.

4.6 Any act that compromises information security will be handled in accordance with **the Company**'s relevant regulations, based on the severity of the case.

5 管理指標

應建立「資訊安全目標達成計畫」，為評量資訊安全管理目標達成情形，特訂定資訊安全管理指標如下：

5.1 量化指標

5.1.1 確保**本公司 ERP 系統**之資訊服務達全年時間 99%以上。

5.1.2 確保**本公司 ERP 系統**因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每半年不得超過 3 次。

5.1.3 確保**本公司 ERP 系統**因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每次最長不得超過 4 小時。

5.1.4 確保**本公司**資訊服務之機密性達 100%。

5.1.5 應適當保護**本公司**資訊資產之機密性與完整性，每年至少需進行乙次風險評鑑

及風險管理。

5.1.6 為確保**本公司**資訊安全措施或規範符合現行法令、法規之要求，每年至少需執行乙次內部稽核。

5.1.7 維護及演練業務永續運作計畫每年至少需進行乙次，以確保**本公司**資訊業務服務得以持續運作。

5.2 質化指標

5.2.1 應定期審查**本公司**資訊安全組織人員執掌，以確保資訊安全工作之推展。

5.2.2 應符合主管機關之要求，依員工職務及責任提供適當之資訊安全相關訓練。

5.2.3 應加強**本公司**電腦及網路設施之環境安全，採取適當之保護及權限控管機制。

5.2.4 應確保資訊不因傳遞過程，或無意間之行為，透漏給未經授權之第三者。

5.2.5 應加強存取控制，防止未經授權之不當存取，以確保**本公司**資訊已受適當之保護。

5.2.6 應確保所有資訊安全事件或可疑之安全弱點，均依循適當之通報機制向上反應，並予以適當調查及處理。

5 Management Indicators

An "Information Security Objective Achievement Plan" shall be established to evaluate the achievement of information security management goals. The following indicators are specifically set:

5.1 Quantitative Indicators

5.1.1 Ensure that the information service of **the Company**'s ERP system achieves an annual uptime of over 99%.

5.1.2 Ensure that operational service interruptions of **the Company**'s ERP system caused by system or server failures resulting from cybersecurity incidents, anomalies, or other security accidents do not exceed three occurrences per half-year.

5.1.3 Ensure that each occurrence of operational service interruption of **the Company**'s ERP system caused by system or server failures resulting from cybersecurity incidents, anomalies, or other security accidents does not last longer than 4 hours.

5.1.4 Ensure 100% confidentiality of **the Company**'s information services.

5.1.5 To appropriately protect the confidentiality and integrity of **the Company**'s information assets, conduct at least one risk assessment and risk management activity annually.

5.1.6 To ensure that **the Company**'s information security measures or standards comply with current laws and regulations, conduct at least one internal audit per year.

5.1.7 Maintain and conduct at least one drill of the business continuity plan each year to ensure the ongoing operation of **the Company**'s information services.

5.2 Qualitative Indicators

5.2.1 The responsibilities and duties of personnel in **the Company**'s information security organization shall be reviewed periodically to ensure the advancement of information security efforts.

5.2.2 In accordance with the requirements of the competent authorities, appropriate information security training shall be provided based on employees' roles and responsibilities.

5.2.3 **The Company** shall enhance the physical security of computer and network facilities by implementing suitable protection and access control mechanisms.

5.2.4 It shall be ensured that information is not disclosed to unauthorized third parties during transmission or due to unintentional behavior.

5.2.5 Access control shall be strengthened to prevent unauthorized access, ensuring **the Company**'s information is properly protected.

5.2.6 All information security incidents or suspected vulnerabilities shall be reported through appropriate channels and be properly investigated and addressed.

6 審查

本政策每年至少評估一次，並於組織有重大變更時（如組織調整、業務重大異動等）重新審查。依審查結果、相關法令、技術及業務等最新發展現況，予以適當修訂，以確保**本公司**業務永續運作之能力。

6 Review

This policy shall be evaluated at least once a year and be subject to re-evaluation upon any major organizational changes (such as restructuring or significant business adjustments). Based on the results of the review, as well as the latest developments in regulations, technology, and business, the policy shall be appropriately revised to ensure **the Company**'s capability for sustainable operations.

7 實施

本政策經**本公司**總經理核定後實施，修訂時亦同。

7 Implementation

This policy shall be implemented upon approval by **the Company**'s General Manager. Any revisions shall follow the same procedure.

8 相關文件

8.1 資訊安全目標達成計畫

8.2 驗證範圍核定函

8 Related Documents

8.1 Information Security Objective Achievement Plan

8.2 Scope of Verification Approval Letter