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：1.3

發行日期：2024.10.18

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」

目　錄

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，使其免於遭受內、外部蓄意或意外之威脅，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。

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。

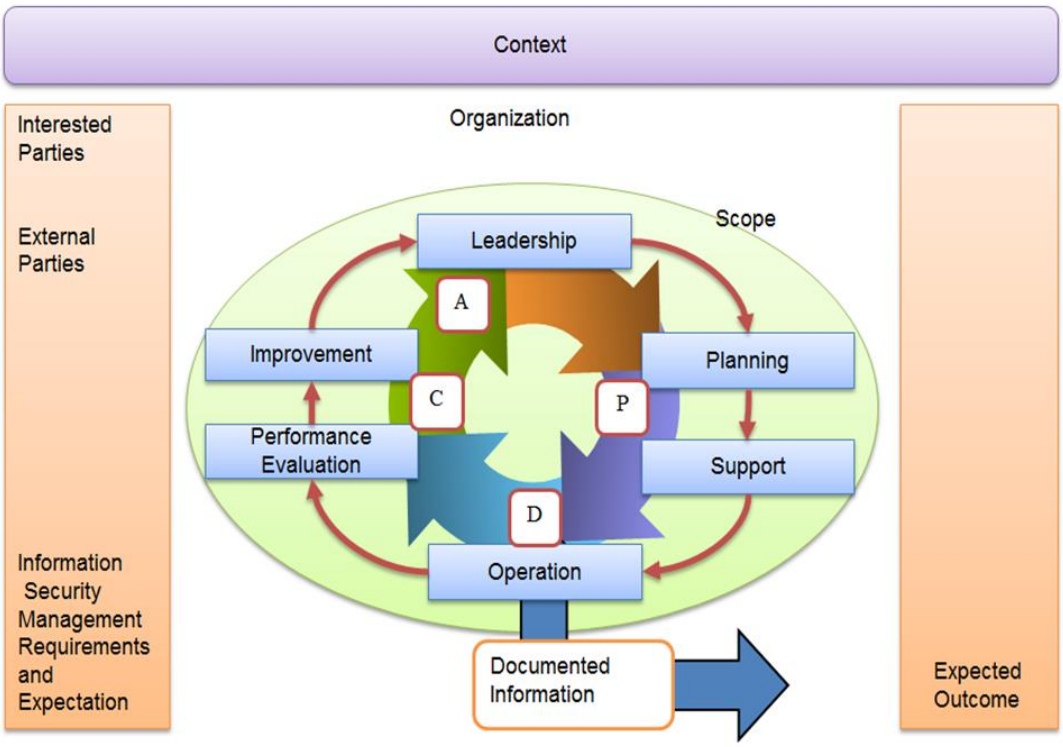
2.2 範圍訂定應考量：

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 本公司及其他單位所執行之活動間的界面及相依性相關驗證範圍及利害團體關注事項之鑑別結果，展現於管理系統驗證範圍核定函，並由資訊安全長核可。

2.3 依據 ISO27001 及 CNS27001 持續改善循環的精神與意義，建構本公司之計畫-支援-執行-檢查-改善循環及相關管理制度，各章節分述如下：



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

2.4 資訊安全管理範疇涵蓋 14 個領域，避免因人為疏失、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，對**本公司**造成各種可能之風險及危害，各領域分述如下：

2.4.1 資訊安全政策

2.4.2 資訊安全之組織

2.4.3 人力資源安全

2.4.4 資產管理

2.4.5 存取控制

2.4.6 密碼學

2.4.7 實體及環境安全

2.4.8 運作安全

2.4.9 通訊安全

2.4.10 系統獲取、開發及維護

2.4.11 供應者關係

2.4.12 資訊安全事故管理

2.4.13 營運持續管理之資訊安全層面

2.4.14 遵循性

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，以提供健康資料加值應用相關業務。

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。

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 27001 及 CNS 27001 要求，並負責向本公司

資訊安全長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。

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 定量化指標

5.1.1 確保**本公司**燒錄料加工料申請(業務申請燒錄)之資訊服務達全年時間 99%以上。

5.1.2 確保因資通安全事件、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，每季不得超過 3 次。

5.1.3 確保因資通安全事件、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 定性化指標

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。

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。

7 實施

本政策經本公司總經理核定後實施，修訂時亦同。

8 相關文件

8.1 資訊安全目標達成計畫