文件履歷表

文件名稱：資通安全政策	文件編號：WS380C
制修訂部門：資訊部	

申請單編號	版本	修訂內容簡述	修訂頁次	申請日期	修訂者
ISO202207250069	A	資通安全政策		2022.7.25	王嘉滿
發行份數：電子檔發行					

Unictron 詠業科技股份有限公司 Unictron Technologies Corporation	文件編號	WS380C
資通安全政策	版　　本	A
	日　　期	2022.7.25

一、資通安全政策

為使本機關業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

(1) 落實資通安全管理系統執行及通過公正第三方驗證。
(2) 有效管理資訊資產，持續執行風險評鑑，並採取適當之防護措施。
(3) 保護資訊及資通系統避免受到未被授權的存取，保持資訊及資通系統的機密性。
(4) 防護未經授權的修改以保護資訊及資通系統之完整性。
(5) 確保經授權之使用者當需要時能使用資訊及資通系統。
(6) 符合法令與法規要求。
(7) 評估各種人為或天然災害之影響，訂定核心資通系統之復原計畫，以確保核心業務可持續運作。
(8) 落實資通安全教育訓練及新進人員資安宣導，以提高員工之資通安全意識。
(9) 落實人員辦理業務涉及資通安全事項之獎懲機制。
(10) 落實委外廠商管理，以確保資通服務之安全。
(11) 落實稽核執行及管理審查流程，以達致資訊安全管理制度之持續改善。
(12) 推動資安防護整合，強化資安聯防及情資分享。

二、資通安全目標

(1) 量化型目標

1. 資通系統可用性達 99.99%以上。(中斷時數/總運作時數≤ 0.01%)。
2. 知悉資安事件發生後，於規定的時間完成通報、應變及復原作業的比率為100%。採用最低授權原則（PLOP）
3. 電子郵件社交工程演練之郵件開啟率低於 4%。

4. 電子郵件社交工程演練之郵件附件點閱率低於 2%。
5. 辦理資安及社交工程教育訓練(1 次)。
6. 資通系統發生資料外洩之資通安全事件(≦2 次/年)。
7. 「全球資訊網」發生資料遭竄改之資通安全事件(≦2 次/年)。
8. 帳號權限管理未授權事件(≦1 件/年)。
9. 辦理滲透測試及弱點掃瞄作業 1 次。
10. 每年資訊安全稽核 1 次。

(2) 質化型目標：

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。
3. 強化委外廠商之選任、監督、管理，嚴格審視委外契約，建構安全服務通道，確保供應鏈關係之資通安全。
4. 提升人員資安防護意識、有效偵測與預防外部攻擊等。