

# 資訊安全政策

## 1. 目的

為保護富智康國際股份有限公司(以下簡稱本公司)，產品與服務的資訊財產及客戶機密資訊，避免有未經授權之存取、修改、使用及揭露，以及天然災害所引起之損失，並適時提供完整與可用之資訊，本公司致力於資訊安全管理，確保本公司重要資訊財產之機密性、完整性及可用性，並符合相關法令法規之要求，以降低資訊安全風險與對公司營運衝擊，進而獲得客戶信賴、達到對股東的承諾，保證公司重要業務持續運作，特定此政策規範。

## 2. 適用範圍

2.1 本公司依實際需要及符合政府與相關法令要求建立資訊安全系統。系統適用範圍設定為本公司台北民生、北京、越南及墨西哥廠區的核心研發及測試系統之開發、生產製造、維護與管理、網路基礎及其所構成之資訊安全管理系統。透過 SWOT 分析與利害關係對應表，充份掌握資訊運作及管理過程並滿足各項安全要求與期盼。

2.2 本公司於建置資訊安全管理系統之初衷及系統執行之結果，均應將內外部單位對資訊安全方面之議題，及關注方對資訊安全管理系統之期盼與要求納入考量，並列入目標與成效評估範圍。這些資訊安全相關議題、期盼或要求，應列入風險評估及風險管理，以確保資訊安全管理系統能達成預期效果及持續改善。並於風險評鑑過程中必須要能識別風險擁有者。

2.3 本公司政策方針為：

確保資訊資產的機密性、完整性、可用性並符合法規與客戶要求保證公司業務持續運作。

2.4 本公司應於相關部門及層級建立資訊安全保護目標，並可與資訊安全政策、方針對應或連結，且必須符合以下 4 項條件：

- 可以量測
- 成效量測方式
- 需訂定完成日期
- 需有負責人員(負責單位)

2.5 本公為能有效支持高階政策之展開，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，對本公司帶來各種可能之風險及危害，本公司訂定之功能性政策如下，以能接續相對應之控制項目或措施：

- 確實執行存取控制管理。
- 有效執行重要資訊遮罩。
- 貫徹實體及環境安全管控，含重要區域之監控。
- 進行資訊資產管理。
- 確保資訊傳輸安全。
- 安全配置及處理使用者終端裝置。
- 執行網路安全管控。
- 網路作業，須妥予執行監視活動。
- 資訊安全事件管理。
- 確實執行備份管理。
- 執行金鑰管理。
- 妥善進行資訊分類及處理。
- 定期實施技術漏洞管理。
- 執行系統開發安全管控。
- 須建立及執行雲服務資訊安全。
- 資訊安全管理系統需有效建立及落實執行。
- 資訊安全管理系統運作之相關人員，應明定責任與義務。
- 資訊安全處理，需建立紀錄並予以維護。

## 3. 權責

- 3.1. 本公司資訊安全管理委員會之技術暨政策推行小組負責擬定此政策，並呈 管理代表審查核准後實施。
- 3.2. 資訊安全管理者透過適當的標準和程序以實施此政策。
- 3.3. 所有人員和委外服務廠商均須依照相關管理程序以維護資訊安全政策。
- 3.4. 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點，若因而防止可能發生之資訊安全威脅事件，得視情況予以適當獎勵。
- 3.5. 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或 依本公司「違反資訊安全及個人隱私保護政策懲處作業指導書」之相關規定進行懲處。

## 4. 作業說明

4.1. 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。藉由全體同仁共同努力來達成下列目標：

- 保護本公司業務活動資訊，避免未經授權的存取含雲端服務之存取與控制。
- 保護本公司業務活動資訊，避免未經授權的修改，確保其正確完整
- 保護本公司軟硬體研發過程均按照程序規範要求落實執行。
- 確保客戶間，具備資料安全之隔離，包含但不限於資料傳遞、交換及使用。
- 專案相關人員於服務過程中不得及無法接觸客戶資產，如因作業需要，須取得客戶同意。
- 客戶及相關人員，於進入雲服務系統時，需透過身分驗證過程，以確保雲服務之資訊安全。
- 作業過程如有變更，須通知客戶，或進行必要溝通。
- 虛擬化作業，須具備資訊安全之考量。
- 當客戶終止接受服務時，權責單位須將該客戶之所有資訊資產清除，以確保客戶權益及服務資訊安全及個人隱私保護。
- 當不符合事項發生或違規行為發生時，須與客戶進行必要之溝通，並視需要提供調查結果及相關資訊。
- 建立跨部門之資訊安全組織，制訂、推動、實施及評估改進資訊安全管理事項，確保本公司具備可供業務持續運作之資訊環境。
- 辦理資訊安全教育訓練，推廣員工資訊安全意識與強化其對相關責任之認知。
- 執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。
- 實施資訊安全內部稽核制度，確保資訊安全管理之落實執行。
- 本公司之業務活動執行須符合相關法令或法規之要求。
- 本公司與委外廠商應訂定資訊安全責任與規定。
- 同仁皆有責任報告資訊安全事件或提出強化資訊安全之建議，若因而防止可能發生之資訊安全威脅事件，將視情況予以適當獎勵。同時若有從事任何危及資訊安全之行為，也將視情節輕重依本公司之相關規定進行懲處，以維護本公司資訊資產，並保障公司與客戶資料隱私與安全。