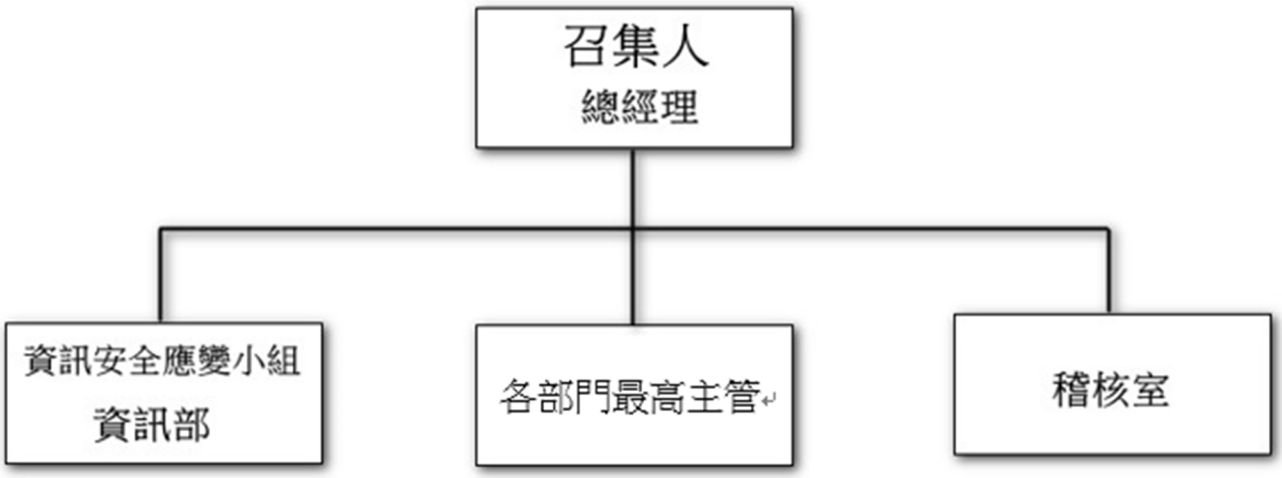
鴻碩精密電工股份有限公司
資訊安全政策實施、重要管理方案報告

資訊安全政策

資訊安全風險管理目的：
強化資訊安全管理、確保資訊的機密性、完整性與可用性、資訊設備(包括電腦硬體、軟體、週邊)與網路系統之可靠性以及同仁對資訊安全之認知，並確保上述資源免受任何因素之干擾、破壞、入侵、或任何不利之行為與企圖。

資訊安全風險管理組織：
「資訊安全推動小組」統籌資訊安全管理等事項之協調、規劃、稽核及推動，成立跨單位之資訊安全推動組織。若組織有重大變更時（如組織調整、業務重大異動等）重新評估本政策之適用性。本政策將依照評估結果、相關法令、技術及業務等最新發展現況予以適當修訂，以確保符合實際需求。

資訊安全推動小組：
組織成員包括各單位最高主管，由總經理擔任本組織的召集人，如因職務調動應即刻指派遞補人員並辦理交接。



資訊安全執行職責劃分：
由資訊部最高主管指派資訊部人員擔任資訊安全應變小組，負責資訊安全須知、計畫及技術規範之研議、建置及評估等事項以及執行各項資訊安全作業，包含資訊安全預防及事件處理。並由稽核室負責資訊機密維護及安全稽核等事項。

資訊安全防護及控制措施:
參考依據美國國家標準技術協會(NIST)的網路安全框架(Cybersecurity Framework，CSF)，採取「辨識」、「防禦」、「偵測」、「應變」、「復原」、「訓練」等步驟來為企業資安做把關。

第一步：辨識：掌握組織環境及關鍵資源與服務，進行風險評估與符合日常營運的風險管理策略 。

第二步：防禦：規劃並實作防禦措施，確保關鍵資源與服務不受資安事件影響 。

第三步：偵測：建置即時偵測網路資安事件與告警的機制，並定期更新系統、防毒軟體病毒碼 。

第四步：應變：順暢的內外溝通管道來處理資安事件應變，包括調查、鑑識與提出改善方案

第五步：復原：制定資料備援計劃，能在最短的時間內恢復正常運作 。

第六步：訓練：「資訊安全，人人有責」，持續強化員工的資訊安全意識。

資訊安全實施計劃：

一、人員管理及資訊安全教育訓練：

(1).對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

(2).針對管理、業務及資訊等不同工作類別之需求，進行資訊安全宣導，建立員工資訊安全認知，提升資訊安全水準。

二、電腦系統安全管理：

(1).辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守。

(2).依相關法規或契約規定複製及使用軟體，並建立軟體使用管理制度。

(3).採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

三、網路安全管理：

(1).開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

(2).與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網

路之資料傳輸與資源存取，防火牆之設定及工作日誌檔需定期檢核，並經適當主管核閱。

(3).利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

(4).定期更新偵測病毒軟體之版本，定時自動偵測病毒，並訓練所有人員使用偵測病毒軟體，防止外之病毒。

(5).訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。

(6).關閉不必要之網路服務。任何網路服務皆需提出申請，經權責主管核准後，由資訊部人員開通之。

四、系統存取控制：

(1).訂定系統存取政策及授權規定，並以書面、電子或其他方式告知員工及使用者之相關權限及責任。

(2).離(休)職人員，應立即取消各項資訊資源之所有權限，並列入離(休)職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

(3).建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過三個月為原則。

(4).對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。

(5).建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。

五、系統發展及維護安全管理：

(1).自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

(2).對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

(3).委託廠商建置及維護重要之軟硬體設施，應在本公司相關人員監督及陪同下始得為之。

六、資訊資產安全管理：

(1).建立與資訊系統有關的資訊資產目錄，訂定資訊資產的項目、擁有者及安全等級分類等。

(2).依據公司機密保護、電腦處理個人資料保護及公司資訊公開等相關法規，建立資訊安全相對應的保護措施。

七、實體及環境安全管理：

就設備安置、周邊環境及人員進出管制等，訂定實體及環境安全管理措施。

八、業務永續運作計畫之規劃與管理：

(1).訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。

(2).建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。

2023 年已實施之資訊安全重大管理方案 ：

項目	方案內容
防火牆防護控管	防火牆設定連線規則，預設只開放基本上網、郵件收發等連線。 如有特殊連線需求需經請權限經部門主管與資訊部最高主管核准始能開放。 隨時監控防火牆網路連線狀況。
資訊機房安全控管	機房進出有門鎖，進出需要有鑰匙，非經允許不得進入。 機房有 UPS 不斷電系統，不正常停電時電源不會中斷，待大樓發電機啟動仍可正常使用，資訊人員有時間可以做後續處置。 機房檢查紀錄表紀錄機房溫溼度、伺服器、網路設備狀況。
防毒軟體控管	公司有安裝企業端點防毒軟體伺服器集中監控管理。 使用者的電腦都要安裝企業端點防毒軟體並定時更新防毒軟體病毒碼，降低中毒風險。
郵件安全控管	郵件伺服器有主動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及惡意連結內容的郵件。 個人電腦接收郵件後,防毒軟體也會掃描是否包含不安全的附件檔案。 郵件伺服器會保留所有郵件進出的備份資料。
資料備份機制控管	資訊系統程式與資料庫皆設定每日完整備份，然後再備份一份到 NAS 備份主機。 公司內各部門檔案存放在檔案伺服器，並由資訊部統一備份到 NAS 備份主機保存。 每周將備份資料放到行動硬碟交管理部人員做異地備援存放。 重要相關文件由文件管理系統控管版本與權限，並在不同廠做主機與資料異地備援。