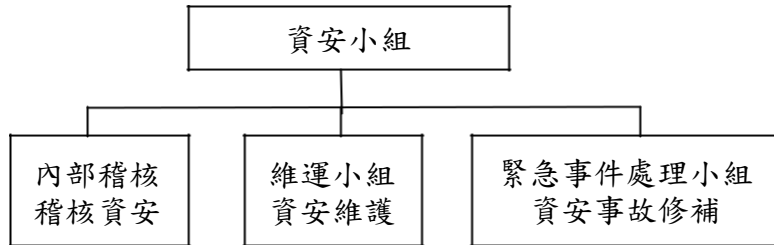


廣豐實業股份有限公司

資訊安全管理

壹、 資訊安全風險管理架構



本公司與合併子公司統籌成立資安小組(如上組織架構圖)，負責整合並執行資訊安全政策，宣導資訊安全訊息，提升員工資安意識，蒐集及改進組織資訊安全管理系統績效及有效性之技術、產品或專案等。由稽核人員每年就內部控制制度進行資訊安全查核，評估公司資訊作業內部控制之有效性。

每年定期由內部稽核單位執行資訊安全管理作業查核，並出具稽核報告，並定期於審計委員會及董事會作稽核結果業務報告。

貳、 資通安全政策

一、目的

為增進本集團資訊作業安全及穩定之運作，提供可信賴之資通訊服務，確保資訊資產之機密性、完整性及可用性，並順利推展各項業務，以符合資通安全管理作業，特制定本公司資通安全政策(以下簡稱本政策)做為資通安全管理最高指導方針。

二、範圍

本政策適用於本公司及關係企業同仁、接觸本公司業務資訊或提供服務之廠商及第三方人員。

三、目標

- 確保本公司業務相關資訊之機密性，保障本公司業務機密與個人資料。
- (一)確保本公司業務相關資訊之完整性及可用性，提高工作效能與品質。
 - (二)提昇本公司資通安全防護能力。
 - (三)達成本公司業務持續運作之目標。

四、策略

- (一)應考量相關法律規定及企業營運要求，評估資通訊作業安全需求，建立相關程序，以確保資訊資產之機密性、完整性及可用性。
- (二)建立本公司資通安全組織並訂定分工權責，俾利推行資通安全作業。
- (三)依資通安全責任等級分級辦法之規定執行各項應辦事項。
- (四)建立資通安全事件通報應變機制，以確保資安事件妥善回應、控制及處理。
- (五)定期執行資通安全稽核作業，以確保資通安全管理落實執行。

五、審查

本政策由董事長核定，資訊處每年至少評估一次，或於組織有重大變更時（如組織調整、業務重大異動等）重新評估。依評估結果、相關法令、技術及業務等最新發展現況，予以適當修訂。

參、 資訊安全具體管理方案

項目	具體管理措施
防火牆防護	<ul style="list-style-type: none"> • 防火牆設定連線規則。
	<ul style="list-style-type: none"> • 如有特殊連線需求需額外申請開放。
使用者上網控管機制	<ul style="list-style-type: none"> • 使用自動網站防護系統控管使用者上網行為。
	<ul style="list-style-type: none"> • 自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。
防毒軟體	<ul style="list-style-type: none"> • 使用防毒軟體，並自動更新病毒碼，降低病毒感染機會。
作業系統更新	<ul style="list-style-type: none"> • 作業系統自動更新，因故未更新者，由資訊部協助更新。
郵件安全管控	<ul style="list-style-type: none"> • 有自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，及擴大防止惡意連結的保護範圍。
	<ul style="list-style-type: none"> • 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。
資料備份機制	<ul style="list-style-type: none"> • 重要資訊系統資料庫皆設定每日備份。
重要檔案上傳伺服器	<ul style="list-style-type: none"> • 公司內各部門重要檔案存放於伺服器，由資訊部統一備份保存。

肆、 資訊安全管理作業

一、目的

為維護公司資訊系統安全及強化資訊安全防護機制，訂定相關規範，以為公司執行之依據。

二、管制範圍

電腦主機系統、電腦設備、電腦程式、資料庫檔案、電腦輸出之螢幕、報表及媒體。

三、管理作業程序

1. 機房規範

(1) 非資訊處理人員，機房未經核准不得隨意進入，進出時需填寫進出登記簿。

(2) 機房內不得擺置易燃物品，並需定期請廠商檢測防火設施。

2. 電腦設備請採購及安裝規範

(1) 更新及購買設備需填寫請購單，會簽主管單位核准後，由資訊部進行採購及安裝。

(2) 電腦設備之安裝需由資訊人員會同進行，不得安裝非法軟體，並確實安裝防毒軟體，定期作病毒掃描及更新病毒碼。

(3) 人員離職時，可移式電腦設備需進行移交手續。

(4) 主機 SERVER 設置防火牆，由公司外部進入作業，皆需經由防火牆進入。

3. 操作控制

- (1)使用者用完電腦時必須離線，電腦不使用時需關機。
- (2)禁止擅自利用資訊中心系統設備，處理與本身業務無關的作業。
- (3)非辦公時間或假日要使用主機，應將使用目的及使用時間先經權責主管核准，並通知資訊部門作相應之措施。
- (4)資訊部門應隨時檢視系統異常 JOBLOG，並做必要之處理。
- (5)資訊部門需定期做資料備份，異地存放，同時定期做回覆測試。

4. 密碼控制

每一位使用者都有獨自的使用代碼，和使用密碼。

- (1)授權使用密碼者應造冊列管，個人之密碼不得借他人使用。
- (2)職員離職或更換工作，其使用代碼應立即註銷或更新。
- (3)凡已上線之檔案，均應由應用程式維護之，而應用程式均應列入使用權限管制範圍。
- (4)密碼之更換，每 3 個月需變更一次，密碼長度至少 6 位，且第 1 位需為英文字。
- (5)第 1 次使用者之帳戶及權限應經資訊單申請，經部門主管核准，再由資訊部門系統安全管理員執行。

5. 權限控制

- (1)使用者應依核准權限擁有相關使用功能。
- (2)資料使用權限應有分層授權系統，稽核及管理人員無權更新資料庫。
- (3)非指定之財務人員無權使用財務報表系統。
- (4)一般應用程式之使用者除執行應用系統外，應無存取主機系統公用程式、工具及指令之權限。
- (5)系統發展／程式撰寫人員對於上線系統之程式與資料檔案應無存取權限。
- (6)設定供廠商於軟、硬體維護時使用之使用者代號，平時應限制未經授權之存取 (disabled)。
- (7)設置電腦工作日誌供系統操作員記載系統之情況，並經主管覆核。
- (8)系統應記錄使用者使用系統之情形，並由系統管理員定期覆核及追蹤久未登錄系統之使用者。
- (9)資訊人員對於正式上線之應用程式應無存取權限。
- (10)密碼應不可顯示於電腦螢幕上，亦不可未經亂碼化即列印於任何報表上。
- (11)資訊人員離職時先填寫離職申請書，經單位主管核准，辦理離職移交程序方可離職，移交程序表需交接人簽名，作業才算正式完成。

伍、 投入資通安全管理之資源

(1) 網路硬體設備

品項	數量
防火牆	1
電腦防毒主機	1
垃圾軟體過濾	1

(2) 軟體系統

品項	數量
電腦防毒軟體	1
備份管理軟體	1

(3) 資通安全投入人力

維護項目	人力
每日各系統狀態檢查	1
每週定期備份	1
備份媒體異地存放之執行	1
每年資安宣導	1
每年系統災難復原模擬演練	2
每年對資訊循環之內部稽核	2

(4) 資安宣導及會議項目

項目	次數/年	參加總人數
112 年度員工資安宣導教育訓練	2	50
112 年度資通安全會議	4	10
112 年度資安事件案例分享	2	50