滿心企業股份有限公司

資通安全管理

滿心企業由電腦室負責建立資訊系統架構，並依規定配置資安專責主管及專業人員，主要工作範疇包括資通安全事件應變、威脅情報防禦、資訊安全檢測、漏洞管理、資安意識教育訓練及資訊安全治理。

■ 資通安全政策

為落實資安管理，公司訂有內部控制制度—電子計算機循環及資訊安全管理辦法。

1.確保資訊資產之機密性、完整性。

2.確保依據部門職能規範資料存取。

3.確保資訊系統之持續運作。

4.防止未經授權修改或使用資料與系統。

5.定期執行資安稽核作業，確保資訊安全落實執行。

6.加入台灣電腦網路危機處理暨協調中心，隨時取得資安事件資訊防範之，及如發生重大資安事件隨時回報。

■ 資安風險管理架構

1.總經理室：

負責訂定年度計畫並協助各部門訂定部門計畫，評估長期經營方針，以降低策略性風險。

2.稽核室：

負責稽核、評估各部門運作及協助改善風險之管理及控制，並基於風險評估結果，稽核室負責評估公司治理之適當性及有效性。

3.電腦室：

負責建立資訊系統架構，依其風險等級建立高可用性之異地主機備援及資料備份機制，以確保系統不中斷，並將備份媒體送往異地保管存放。加強機房各項模擬測試與緊急應變等演練以確保資訊系統之正常運作及資料保全，可降低無預警天災及人為疏失造成之系統中斷風險。並依據風險等級，規劃設計與提升適當軟硬體設備資源，改善作業流程等因應措施。統籌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、產品或程序等。

■ 具體管理方案

網際網路資安管控	資料存取管控	應變復原機制	員工宣導
• 架設防火牆（Firewall） • 定期對電腦系統及資料儲存媒體進行病毒掃瞄 • 各項網路服務之使用應依據資訊安全政策執行 • 定期覆核各項網路服務項目之System Log，追蹤異常之情形	• 電腦設備應有專人保管，並設定帳號與密碼 • 依據職能分別賦予不同存取權限 • 調離人員取消原有權限 • 設備報廢前應先將機密性、敏感性資料及版權軟體移除或覆寫	• 定期檢視緊急應變計劃 • 每年定期演練系統復原 • 建立系統備份機制，落實異地備份 • 定期檢討電腦網路安全控制措施 • 如有重大資安事件即刻於TwCert 通報	• 隨時宣導資訊安全資訊，提升員工資安意識

■ 投入資通安全管理之資源

1.定期對公司資通系統使用者宣導資安觀念。

2.資通安全專業人才之培育。

3.與 SI 配合廠商定期簽訂資安設備年度維護合約，不定期進行資安事件發生狀況演練及災難復原。

■ 114 年資源投入情形

1.人力資源投入

資安專職人員數量：負責資安管理的員工數為 2 人。

資安訓練時數：資安人員年度接受的資安培訓計時數 9 小時。

2.財務資源投入

年度資安預算：投入資通安全管理的年度預算約 120 萬元。

資安硬體維護費用支出：防火牆、ERP、網路空間硬碟等年度費用計 478,290 元。

資安軟體維護費用支出：防毒軟體、備份軟體、郵件系統等年度費用計 548,000 元。

3.資訊技術與基礎設施

部署防火牆數量：企業級防火牆數量 2 台。

端點防護設備數量：網路封包蒐集器數量 1 台、防毒與 EDR（端點偵測與回應）系統設備數量 130 台。

4.備份與災難復原

備份頻率：資料庫備份的頻率為每日 1 次。

備份測試還原成功率：每半年測試備份還原的成功比例為 100%。

5.內部宣導

每月由電腦室專責人員隨時宣導資安訊息，提醒公司所有員工每三個月更換個人電子郵件密碼，並注意郵件連結網路詐騙問題，以提升員工資安意識。

6.外部廠商會議

電腦室每季一次每年計四次與合作的外部廠商開會，針對網路安全或設備維護問題進行討論。另一方面，平日若有遇到問題，則雙方即時電話連繫溝通以解決公司所遇到的相關資訊問題。

■ 114 年資通安全結論

上述數據能有效評估資通安全的資源投入情況，並作為未來資安策略與預算規劃的重要參考依據。公司本年度無重大資安事件導致營業損害之情事發生，公司將持續落實資訊安全管理政策，並定期實施復原計劃演練，保護公司重要系統與資料安全。