

台灣櫻花股份有限公司

114 年資訊安全具體管理方案

一、本公司目前資訊安全風險管理方案內容已能有效防護資訊安全，且考量資安保險仍是新興險種，因此經資訊安全執行小組評估後暫不購買。

1. 資訊安全具體執行方案如下：

類 別	說 明	內 容
預防外部入侵	安裝防火牆與防毒軟體	◆ 設置網路防火牆。 ◆ 伺服器與電腦主機安裝防毒軟體。 ◆ 定期系統更新 ◆ 防毒軟體病毒碼自動更新。 ◆ 定期執行防毒軟體電腦掃描。
預防資料外洩	帳號、權限管理	◆ 人員帳號審核及管理。 ◆ 定期執行系統權限設定檢核。
日常營運維持	資料備份與相關檢核	◆ 依資料性質進行資料備份。 ◆ 異地備份。 ◆ 定期執行資料還原測試。 ◆ 每日執行伺服器主機檢核暨系統測試。 ◆ 定期電腦檢核。 ◆ 每日 19:10 自動抓取 ERP 離職員工名單自動停用。
資安事件處理	災害復原計劃	◆ 訂定「資訊災難緊急應變計劃」。 ◆ 定期模擬演練災害發生。 ◆ 事後撰寫災害復原計劃執行報告並檢討改善。

2. 本年度舉辦資訊安全相關教育訓練如下：

日 期	課程名稱	時數	參與人數
114.05.05	月會宣導-個資宣導_總公司	1	190
114.05.06	月會宣導-個資宣導_整廚	1	48
114.05.07	月會宣導-個資宣導_製造&研發&家居	1	160
114.12.01	月會宣導-資訊安全宣導_總公司	1	190

日 期	課程名稱	時數	參與人數
114.12.02	月會宣導-資訊安全宣導_整廚	1	48
114.12.03	月會宣導-資訊安全宣導_製造&研發&家居	1	160