台灣櫻花股份有限公司

113 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。

二、資訊安全具體執行方案如下：

類　別	說　明	執　行　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。

三、本公司每年執行員工常態性資訊安全教育訓練，所有同仁每年應至少參與資安教育訓練時數1小時。另針對不同角色與職能人員規劃不同性質資安課程，透過不斷的培訓以提升本公司員工資安意識並內化於各項作業中，以落實最安全及嚴密的資安保障。

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
113.05.07	資安宣導	1	390
113.08.05	個資宣導	1	390
113.11.04	資安宣導	1	390

四、 相關資訊安全政策及具體實施情形於 113 年 12 月 18 日董事會中重點報告。