邑錡股份有限公司

113 年資訊安全風險管理措施及執行情形

一、資訊安全風險管理架構

公司資訊安全由行政管理處下資訊部負責統籌資訊安全及相關事宜，訂定資安規範與資安的推動與落實，並每年定期由內部稽核執行資通安全管理作業查核及向董事會報告。

二、資通安全政策

為落實資安管理，公司訂有內部控制制度—電子資料循環及網路安全管理辦法及個人電腦管理要點，藉全體同仁共同努力期望達成下列政策目標：

(1)確保資訊系統持續正常運作。

(2)依據各職能資料存取,防止未經授權的資料修改和審核。

(3)確保資訊系統不被外部破壞(病毒、駭客、意外災害…)。

(4)確保資料被破壞後的復原。

(5)人員資訊安全與教育訓練

三、具體資訊安全管理措施

相關資訊安全管理措施之辦法如下表：

資訊安全管理措施		
類型	**說明**	**相關作業**
人員安全管理	人員帳號,權限管理和教育訓練	●人員帳號權限管理與審核 ●人員離職調任帳號刪除 ●資訊安全教育訓練和宣導資訊安全訊息
電腦系統安全管理	系統安全管理,資料安全管理,電腦病毒和惡意軟體之防範	●電腦作業系統設定與管制 ●ERP 系統每日備份和每周異地備份 ●使用合法軟體,隨時更新病毒碼
網路安全管理	網路安全規劃與管理,網路使用者管理,電子郵件安全管理	●建置防火牆及防毒系統 ●定期資訊安全宣導 ●來路不明電子郵件,不隨意打開

資訊安全管理措施		
類型	**說明**	**相關作業**
人員安全管理	人員帳號,權限管理和教育訓練	●人員帳號權限管理與審核 ●人員離職調任帳號刪除 ●資訊安全教育訓練和宣導資訊安全訊息
系統存取控制	人員存取內外部系統及資料傳輸管道之控制措施	●系統存取權限以執行業務及職務所需為限 ●系統使用者開啟帳號後應自行設定密碼 ●使用者權限異動應提出申請同意後,資訊始得修改
資訊資產之安全管理	資訊資產故障及報廢之處置	●資訊設備報廢,應在報廢前移除所有記憶體內資料並紀錄 ●資訊設備故障應提出請修申請
系統發展與維護之安全管理	一般電腦系統及委外作業安全管理	●應用系統程式更新,由各應用系統負責人配合執行 ●委外資訊廠商除安全管理責任外,也應落實保密作為
實體及環境安全管理	電腦設備安全管理,電源供應系統的管理,電腦機房消防系統的設置管理	●電腦機房專人負責, 定期檢查機房消防環境、空調、硬碟空間、警示燈號 ●提供緊急供電暨不斷電系統 ●電腦機房實施門禁管控
業務永續運作計畫之規劃及管理	備援及回復作業,資訊安全事件通報處理機制	●每年應進行備援,回復作業之測試演練 ●發現有資訊安全事件時,應迅速通報權責主管單位及人員處理
資訊安全稽核	確認資訊安全管理作業之執行情形	●每年定期執行資訊安全查核和改善

公司針對資訊技術安全之風險，訂有資訊技術安全政策及相關管理措施，為公司資訊及電腦系統建立與維持一個安全的環境，因企業引用資訊科技，打破了企業組織服務和協調時間和空間的障礙，但公司所面臨的相關風險也隨之增加，因應於此，公司的企業網站和 Mail 服務專案管理採租用外部虛擬主機服務，除了可減少相關硬體設置維護也提供信件掃毒，垃圾信過濾和備援功能，防止服務中斷。

由於公司內部重要資訊及以及公司內部員工處理資料和系統都和公司營運有直接的關係，針對此項公司均有同地/異地備分和每年定期還原演練之管理，如遇無法避免毀損同時和營運中斷可備份還原並依重要性依序恢復運行。此外，公司每台終端機均安裝防毒軟體並每日更新病毒碼外還同時定期作資安宣導針對瀏覽的網站，惡意的 Mail 連結和程式下載，定期資安宣導，增加員工安全意識。

四、執行狀況：

113 年度本公司依計畫執行核心設備弱點掃描、資產辨識及資訊資產風險等級之評估和郵件社交演練，並針對執行結果進行檢討與改善，以上加上資訊設備維護更新投入經費約 1,100,000 元，資安人員接受外部教育訓練 14 小時，訓練費用 4,000 元。公司系統除執行版本更新和台電停電期間短暫無法使用外，目前無重大資安事件導致營業損害之情事並持續落實執行。