# 邑錡股份有限公司

## 114 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**

本公司之資訊安全由行政管理處資訊部統籌，負責資訊安全政策之制定、執行與維運，並設置資安專責主管 1 人和 1 名資安專責人員；並由內部稽核單位每年定期辦理資通安全管理作業查核，以確保資訊安全管理制度之有效運作，定期向董事會報告。

**二、資通安全政策**

為維護資訊資產完整性、可用性與機密性，本公司制定「電子資料循環及網路安全管理辦法」及「個人電腦管理要點」，並推行全員資訊安全意識，使資訊安全能持續落實。政策目標如下：

(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) 建立資料備援及復原能力，降低營運風險。

(5) 持續推動人員資訊安全教育訓練。

**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<br>●離職及職務異動帳號即時停用<br>●定期辦理資安教育訓練與宣導 |
| **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 | ●電腦作業系統設定控管<br>●ERP 系統每日備份和每周異地備份<br>●安裝合法軟體並每日更新病毒碼 |
| **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<br>●定期資訊安全宣導<br>●加強電子郵件安全使用（慎防惡意信件與附件） |
| **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<br>●系統使用者開啟帳號後應自行設定密碼<br>●權限異動須經主管核可後由資訊部執行 |
| **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<br>●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<br>●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<br>●提供緊急供電暨不斷電系統<br>●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<br>●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 |

公司為降低資訊技術使用所伴隨之資安風險，訂定資訊技術安全政策並建立相應管理制度，以維持系統可用性、完整性及機密性。企業導入資訊科技後雖能提升運營效率，但資安威脅亦相對增加。為強化防護與確保營運連續性，本公司網站及 Mail 服務採外部虛擬主機架構，降低硬體維運成本並具備信件掃毒、垃圾郵件過濾與備援功能，有效減少服務中斷風險。

針對公司內部重要系統與資料，採行同地/異地備份策略並每年執行至少一次還原演練，確保災害發生時能依營運優先順序逐步恢復系統運作。

公司端點設備均安裝防毒軟體並自動更新病毒碼，非預期病毒事件通報件數為 0 件。同時不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，宣導涵蓋惡意郵件辨識、安全下載與網站風險識別，有效提升員工資安認知。

。

四、執行狀況：

2025 年度本公司依年度資安計畫完成核心設備弱點掃描、資訊資產盤點與風險等級評估，以及郵件社交工程演練，並針對結果進行檢討及改善措施落實。年度資訊設備維護與汰舊更新投入經費約新台幣 95 萬元，資安人員參與外部專業訓練時數共計 14 小時。全年系統運作穩定，除版本更新作業與台電停電期間曾短暫影響服務外，無重大資訊安全事件造成營運損害。本公司將持續推動資安管理制度強化，確保營運持續性與資訊安全防護能力。