

邑錡股份有限公司

110 年資訊安全風險管理措施及執行情形

為使本公司電子資訊資料，系統,設備和網路安全,避免因人為疏失，蓄意破壞和自然災害等風險，本公司於 108 年訂定資訊安全管理辦法，本辦法目的是讓同仁於日常工作時對資訊安全有明確的執行原則和監督資安管理運作情形。不會因不當使用，洩漏，竄改，破壞等情事，而影響公司業務運行和權益。期望透過資安單位之管理、規畫、督導及推動執行，建構出全方位的資安防護能力及同仁良好的資安意識。

為統籌本公司資訊安全管理事宜由行政管理處最高主管擔任召集人，包含各處單位聯絡窗口共同承辦資訊管理工作。

權責分工:

- 1、資訊系統、安全、控制、技術由資訊單位負責。
- 2、資料、資訊系統和設備之安全使用及保護事宜由各單位負責辦理。

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	<ul style="list-style-type: none"> ●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
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	<ul style="list-style-type: none"> ●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	<ul style="list-style-type: none"> ●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
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	<ul style="list-style-type: none"> ●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	<ul style="list-style-type: none"> ●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	<ul style="list-style-type: none"> ●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	<ul style="list-style-type: none"> ●電腦機房專人負責,定期維護保養及測試 ●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	<ul style="list-style-type: none"> ●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	<ul style="list-style-type: none"> ●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

110 年執行狀況如下：

邑錡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。每年稽核會定期查核，若查核發現缺失，旋即要求受查單位提出改善措施，且定期追蹤改善結果，以降低內部資安風險。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，本公司的企業網站和 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，異常警示，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，針對此項本公司均有同地/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。

因應 110 年度疫情影響，除了宣導居家上班時資安觀念，並再公告公司個人電腦管理要點，禁止電腦資源被濫用和維護公司網路資訊之安全，年度內無重大資安事件。