林亞股份有限公司

資訊安全政策

114 年 11 月 12 日 董事會通過

林亞秉持「打造韌性、安全、值得信任的企業」的資訊安全管理使命，制定資訊安全政策作為核心指導原則，全力推動數位轉型並全面導入資訊安全管理機制。我們專注於確保資訊處理的完整性與 可用性，並保障資訊系統、設備及網路的安全。透過定期執行資訊安全演練與教育訓練，我們致力於建立全面性的資安防護網，確保相關資訊資產不受威脅。

林亞預計於 2026 年取得資訊安全管理系統國際標準 ISO／IEC 27001：2022 驗證，依照此標準實施「Plan-Do-Check-Act」(PDCA) 之循環運作，每年至少進行一次內部自我稽查及一次外部公正第三單位稽查，確保公司落實 ISO 27001 管理機制，每三年也會執行證書重新驗證的程序，持續維持 ISO 27001 的有效認證。

第一條　政策目標

本公司為確保資訊資產之機密性、完整性與可用性，避免因未經授權存取、洩漏、竄改或遺失所造成之營運、法令或商譽風險，特訂定本資訊安全政策，作為資訊管理與使用之基本原則。

第二條　適用範圍

本政策適用於林亞股份有限公司全體員工、約聘、派遣人員、實習生及因業務需需要可接觸本公司資訊之第三方，涵蓋範圍包含電腦、筆電、伺服器、電子郵件、檔案系統、紙本文件與電子資料

第三條　資訊安全基本原則

一、存取控管

1. 資訊系統依業務需求授權使用
2. 帳號不得共用
3. 員工離職或職務異動時，應即時調整或取消存取權限

二、密碼與帳號管理

1. 密碼應妥善保管，不得外洩
2. 不得使用明顯或重複之簡易密碼
3. 定期檢視帳號使用狀況

三、資料保護

1. 含有個人資料、薪資或營運資訊之文件，應妥善保存
2. 對外提供資料時，應避免揭露不必要之內部或個資資訊

3. 重要資料應定期備份

四、設備與系統使用

1. 公司設備僅限公務使用
2. 禁止安裝未經授權之軟體
3. 發現異常（病毒、可疑郵件）應立即通報

五、事件通報與處理

如發生或疑似發生下列情形，應立即通報主管，公司將依事件性質採取必要處理與改善措施。

1. 資料外洩或遺失
2. 非授權存取
3. 系統異常或惡意程式感染

第四條　教育與宣導

公司將視需要進行資訊安全宣導，提升員工對資訊安全與資料保護基本認知。

第五條　施行

本政策經本公司董事會通過後施行，修正時亦同。

本政策經 2026 年 1 月管理階層年度檢視，內容持續適用。