青鋼應用材料股份有限公司

資通安全管理

青鋼依據組織結構設立資訊安全室，並根據「公開發行公司建立內部控制制度處理準則」，於 2023 年設置了資安專責主管 1 名及專責人員 1 人，組成資通安全部門，每月定期召開會議，並加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)會員。

為確保資訊系統運作之安全性、穩定性與透明性，本公司訂定資訊管理辦法，涵蓋資訊部門職能、硬體與軟體資產管理、系統開發流程、資訊安全控制及災難復原計畫等重點，並配合相關法規及內部控制制度，持續提升資訊治理的效能。

資訊管理辦法	
項目	**管理內容**
一、資訊組織與職責	設有資訊安全室，負責系統開發、程式設計、資料管理、網路規劃與維運。
	電腦資料輸入權限由非資訊人員執行，確保職責分離與資料完整性。
	資訊安全室具年度目標與策略規劃，並負責內部網路及硬體基本維修。
二、資訊資產管理	硬體設備與軟體系統之請購、報廢、配置皆依正式流程辦理，並經資訊安全室會簽。
	設有明確資產保管責任，資訊安全室掌握資源調度權，各單位負責日常管理與維護。
三、系統開發與程式控管	系統開發及程式修改須申請並核准,依標準流程執行(分析、設計、測試、導入、文件化）。
	強調程式版本控管與文件完整,並執行使用者教育訓練。
四、資訊安全與存取控制	實施帳號與權限控管，資料異動需主管核准。
	存取權限採分級管理，由資訊安全室統籌維護。
	加密機密資料、定期更新密碼、嚴禁帳密共用與未經授權使用。
五、資料處理與報表管理	確保輸入資料經核准，報表透過邏輯檢核與核對清單確認正確性。
	機密資料由特定人員處理,依保存年限或法令妥善銷毀。
六、資訊設備安全與備份	電腦中心、主機房、網路系統與終端設備皆設專人負責安全。
	每日、每週、每月執行備份，資訊安全室負責控管備份媒體存取與管理。
七、災難復原與系統容錯	建立系統災難復原計畫並定期演練，記錄並改進。
	重要作業設有人工替代流程，提升營運持續能力。

八、資通安全政策	設有防火牆、防毒軟體與入侵偵測機制。
	禁止未經授權對外傳送公司資料，定期檢查非法軟體。
	設立資安事件通報與應變機制,依等級處置並保留紀錄。
九、公開資訊申報控管	採帳號分權管理，申報資料經核對後上傳。
	持續追蹤主管機關最新函令,確保申報資料即時、正確、合規。

2025 年進行教育訓練如下：

時間	課程名稱	訓練人次 (A)	課程時數 (B)	總人時 (A*B)
2025/2/1 2025/2/4	資訊安全意識、必備知識與責任E-Course	2	2	7
2025/2/2 2025/2/4	上市上櫃公司資通安全管控指引說明E-Course	2	1.5	3
2025/2/3 2025/2/4	資安事件說明及預防措施E-Course	2	2.5	5
合計				15