

資訊安全風險管理架構

本公司已全面導入資通安全體系，除了於2023年底導入安全營運中心 SOC(Security Operation Center)的機制外，並已設置資安長一職，由總經理兼任，負責帶領安全風險管理小組並確保資通安全管理制度之運作，鑑別資通安全管理制度之內、外部議題及利害相關團體對本公司之資通安全要求與期望。安全風險管理小組負責審查各子公司的安全政策，監督本集團安全管理的運作，並定期向高層會報告安全的管理；安全控制結構包括協助各點和保持集團安全性，每個點都有自己的本地安全控制，集團安全團隊負責監督和管理整個集團的安全控管，安全風險管理涵蓋各種範圍，如資料、資料庫、應用程式、可存取性、安全性。

I. 資通安全對象與範圍

1. 對象：包括員工、客戶、供應商和股東以及營運相關資訊軟硬體設備。
2. 範圍：為確保本公司資通安全，制定相關規章制度，應用技術和數據安全標準制定，並納入管理運作體系，以保障員工，供應商和客戶進行業務接洽時之隱私權保護與資通安全維護。

II. 資通安全風險架構

1. 由本公司總經理召集成立跨部門資通安全管理小組，資訊部門與行政管理部門負責主導及規劃，各業務相關單位配合執行，以確認本公司資訊安全管理運作之有效性。
2. 本小組負責制定資通安全管理政策，定期檢討修正。
3. 本小組定期召開會議檢討執行情形，並每年定期向董事會報告執行情形與檢討。

III. 資通安全政策目標

1. 政策

資訊安全與機密資料的保護是貿聯公司對於所有合作的夥伴、客戶及股東們責無旁貸的責任。有鑑於此，貿聯公司設置了安全長 (CSO)、導入安全營運中心機制及定期召開資安委員會，用以在公司組織內訂定完善的政策、充分利用各部門資源及降低資安風險，並發布了《[資訊安全宣言](#)》，用以明確宣告貿聯公司處理內外資安風險及如何推動資安目標的決心，維護客戶權益、保障合作夥伴的資料及提升貿聯公司的對外競爭力！



資訊安全宣言

貿聯公司為全球連接器與線材的領導廠商，不論對於客戶及合作夥伴的資料保護均以最嚴謹的態度來面對，對於資訊安全的風險為零容忍，期許成為所有客戶及伙伴的最佳後盾，共同發展彼此的戰略夥伴關係，以期能共同提升彼此的競爭力，達到共有共好的美好成果。

BizLink BizLink Technology, Inc.

2.目標

安全策略的主要目標是關注安全管理，法律合規和技術應用三個方面，從系統到技術，從人員到組織，全面提高安全防護能力。鑑於當前資產安全的新趨勢，如 DDoS (分散式拒絕服務) 攻擊，勒索軟件，社交工程 攻擊和虛假網站，我們每季度與國際安全廠商溝通，並通過專案合作定期關注安全問題和規劃。針對該計劃，對不同的安全場景進行了 DDoS 和其他攻防演練，加強處理人員的彈性，以便在第一時間檢測並完成防堵，此外也經常進行培訓和課程。所有的用戶都被要求參加。**2023年度共進行82場安全教育訓練，共計4,542人次。**

為了加強資訊安全管理，除了規劃具有最嚴格安全要求的網絡架構外，我們還定期邀請外部安全專家進行評估，並確保合乎法規，如 GDPR。

IV. 資通安全控制措施

1. 建立訂定期盤點資訊資產清單，依資安風險評鑑進行風險管理，落實各項管控措施。
2. 公司定期執行資通安全宣導作業，每年辦理與資通安全教育訓練，新進人員皆須簽定資訊保密協定及接受資通安全教育訓練。
3. 本公司所有員工、委外廠商暨其協力廠商須簽定保密聲明書，已確保使用本公司資訊以提供資訊服務或執行相關資訊業務者，有責任及義務保護其所取得或使用本公司之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露。
4. 重要資訊系統或設備應建置適當之備援或監控機制並定期演練，維持其可用性。
5. 個人電腦應安裝防毒軟體且定期確認病毒碼之更新，並禁止使用未經授權軟體。
6. 同仁帳號、密碼與權限應善盡保管與使用責任並定期換置。
7. 制定資通安全事件的回應及通報標準程序，以適當對資通安全事件做即時處理，避免傷害擴大。
8. 全體人員應遵守法律規範與資通安全政策要求，主管人員應督導資安遵行制度落實情況，強化同仁資安認知及法令觀念。
9. 考量資通安全之風險不確定性，**2023 年度已購買資安險(新台幣200萬)。**

此外，為了防止將資訊錯誤發送到外部電子郵件地址或外部連接到我們的網絡，我們會屏蔽並限制具有潛在風險域的進出，至少包含下列項目：

1. 每週對安全管理員進行培訓：利用每周的IT周會時間，112年共計實施52次的培訓，參與人員為各地的資訊人員代表，共21員。
2. 行動設備安全控制包括消除和刪除設備資料：我們嚴格禁止使用者使用週邊儲存設備存取電腦資源。
3. 資料遺失防護端點 - 設備可存取性的控制：利用防毒軟體及EDR(Endpoint Detection & Response)的導入，隨時掌握端點安全的狀況，2023年並未發生重大端點異常。
4. 可疑登錄和多重設備登錄的警報：本年度完整導入AD (Active Directory)的異常登入紀錄報告，故有任何大量破解或嘗試登入事項都能確實掌握，於可能出現的風險之前即與以清除。
5. 網路釣魚和惡意軟件防護：2023年共舉辦5次的網路釣魚郵件演練，演練人次共2,449人。
6. 災難恢復：本公司之重要系統定義為SAP、MES於Oracle Agile，本年度針對其中之SAP系統於2023年11月6日舉行災難復原演練計畫並成功完成。
7. 定期安全檢查：導入SOC機制，針對各項重大之設備及系統均能完整監控，各地區從機房管制、防毒系統、端點檢查、資安教育訓練等...均確實落實總部之政策，形成完整的安全防護網。
8. 密碼強度和長度的強制和監控：本年度針對密碼強度及帳號鎖定策略進行改善，有效降低安全風險及提供安全等級。
9. 多層登錄驗證：導入AVD(Azure Virtual Desktop)針對外部顧問及廠商進行多重驗證，確認其真實身分後方能允許連入公司內部資源並隔離環境，以避免不當的存取及破壞。
10. 電子郵件 TLS 安全加密回應網絡攻擊，為了能彈性應對最近的安全風險，如電子郵件攻擊和惡意軟體感染，將對所有員工進行安全演示和培訓：2023年共進行82場安全教育訓練，共計4,542人次。