環資國際有限公司

資通安全政策

機密等級：■一般 □敏感 □機密

編號：I-1-01

版本：2.0

發行日期：113 年 1 月 1 日

文件制／修訂紀錄頁

版次	發行日期	修訂摘要	修訂者	文管人員
1.0	109.1.1	初次發行	陳盈竹	陳盈竹
1.1	109.7.1	因應組織職位及任務異動、ISO 擴項驗證調整程序書	柯上茗	尤麗華
2.0	113.1.1	配合 ISO 27001:2022 新版發行	柯上茗	尤麗華

目錄

壹、目的：

為維護環資國際有限公司（以下簡稱本公司）所屬資訊資產之機密性、完整性及可用性，並符合相關法規之要求，並保障使用者資料隱私，使其免於遭受內、外部的蓄意或意外之威脅。本公司整合各層級部門資通安全目標，建立本公司整體資通安全政策目標如下：

一、保護本公司業務活動資訊，避免未經授權存取，確保機密性。

二、保護本公司業務活動資訊，避免未經授權修改，確保正確完整性。

三、建立資訊業務永續運作計畫，維持本公司業務持續運作，確保可用性。

四、本公司之業務執行符合相關法規之要求，確保法規遵循性。

貳、適用範圍：

本政策適用於本公司人員、委外服務廠商與訪客皆應遵守本政策，以及資通訊安全之相關作業規範管理事宜。

為避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本公司帶來各種可能之風險及危害。資通訊安全管理除透過「資通安全政策」、「適用性聲明」、「文件管理程序書」、「資通安全風險管理程序書」、「資通安全稽核管理程序書」、「矯正預防管理程序書」、「資通安全目標管理程序書」、「組織全景分析程序書」外，亦建立組織、人員、實體、技術等相關管理程序書，規範各項資訊安全控制措施，俾利遵行，各管理程序書應規範控制措施之範圍分述如下：

一、組織控制措施：運用本公司建立之「資通安全組織管理程序書」、「威脅情資管理程序書」、「資訊資產管理程序書」、「存取管制與密碼管理程序書」、「供應商關係管理程序書」、「供應商關係管理程序書」、「資通安全事件管理程序書」、「業務持續管理程序書」、「法規遵循管理程序書」、「作業安全管理程序書」等系列管理程序書，對「資訊安全政策」、「資訊安全之角色及責任」、「職務區隔」、「管理階層責任」、「與權責機關之聯繫」、「與特殊關注群組之聯繫」、「威脅情資」、「專案管理之資訊安全」、「資訊及其相關聯資產之清冊」、

「可接受使用資訊及其他相關聯資產」、「資產之歸還」、「資訊之分類分級」、「資訊標示」、「資訊傳送」、「存取控制」、「身分管理」、「鑑別資訊」、「存取權限」、「供應者關係中之資訊安全」、「於供應者協議中闡明資訊安全」、「管理 ICT 供應鏈中之資訊安全」、「供應者服務之監視、審查及變更管理」、「使用雲端服務之資訊安全」、「資訊安全事件管理規劃及準備」、「資訊之評鑑及決策」、「對資訊安全事故之回應」、「由資訊安全事故中學習」、「證據之蒐集」、「中斷期間之資訊安全」、「營運持續之 ICT 備妥性」、「法律、法令、法規及契約要求事項」、「智慧財產權」、「紀錄之保護」、「隱私及 PII 保護」、「資訊安全之獨立審查」、「資訊安全政策、規則及標準之遵循性」、「書面記錄之運作程序」等 37 項控制措施實施資安作業管理。

二、人員控制措施：運用本公司建立之「人力資源管安全理程序書」、「資通安全事件管理程序書」等管理程序書，對「篩選」、「聘用條款及條件」、「資訊安全認知及教育訓練」、「獎懲過程」、「聘用終止或變更後之責任」、「機密性或保密協議」、「遠端工作」、「資訊安全事件通報」等 8 項控制措施實施資安作業管理。

三、實體控制措施：運用本公司建立之「實體與環境安全管理程序書」，對「實體安全週界」、「實體進入」、「保全辦公室、房間及設施」、「實體安全監視」、「防範實體及環境威脅」、「於安全區域內工作」、「桌面淨空及螢幕淨空」、「設備安置及保護」、「場所外資產之安全」、「儲存媒體」、「支援之公用服務事業」、「佈纜安全」、「設備維護」、「設備汰除或重新使用之安全」等 14 項控制措施實施資安作業管理。

四、技術控制措施：運用本公司建立之「實體與環境安全管理程序書」、「存取管制與密碼管理程序書」、「作業安全管理程序書」、「網路安全管理程序書」、「系統發展與維護管理程序書」等管理程序書，對

「使用者端點裝置」、「特殊存取權限」、「資訊存取限制」、「對原始碼之存取」、「安全鑑別」、「容量管理」、「防範惡意軟體」、「技術脆弱性管理」、「組態管理」、「資訊刪除」、「資料遮蔽」、「資料洩露預防」、「資訊備份」、「資訊處理設施之多備」、「存錄」、「監視活動」、「鐘訊同步」、「具特殊權限公用程式之使用」、「運作中系統之安裝」、「網路安全」、「網路服務之安全」、「網路區隔」、「網頁過濾」、「密碼技術之使用」、「安全開發生命週期」、「應用系統安全要求事項」、「安全系統架構及工程原則」、「安全程式設計」、「開發及驗收中之安全測試」、「委外開發」、「開發、測試與運作環境之區隔」、「變更管理」、「測試資訊」、「稽核測試期間資訊系統之保護」等 34 項控制措施實施資安作業管理。

參、權責：

為落實執行本公司資通安全政策，權責劃分如下：

一、本公司設置資通安全委員會，董事長為當然委員並兼資通安全長，該委員會統籌資通安全政策、計畫、作業、資源調度之協調與管理審查。

二、資通安全委員會下設置資通安全工作小組，由資通安全長指定專人擔任管理代表，配合本公司資通安全需求制修訂各階管理程序文件，維持本公司資通安全管理系統之有效運作，每年應至少一次將資通安全工作執行成果，陳報資通安全委員會進行管理審查。

三、本公司各單位應遵循資通安全工作小組制定之相關資通安全規定。

四、本公司員工、本公司辦公場所以外之系統連線使用者及承接本公司業務之廠商，應遵循本公司資通安全政策及相關管理規定。

五、有任何危及資通安全之行為者，應依法負擔民事、刑事責任，並依本公司相關規定進行行政懲處。

肆、名詞定義：

無。

伍、作業說明：

一、審查：

本政策應至少每年評估審查一次，以符合政府法令之要求，並反映資通科技發展趨勢，確保本公司資通安全管理作業之有效性。

二、實施：

（一）資通安全政策應配合資通安全委員會召開時機，每年定期進行資通安全政策及執行成效管理審查。

（二）本公司每年應遵循「資通安全目標管理程序書(I-2-05)」，使用「資通安全目標有效性量測表(I-2-05-01)」定期量測並審查資通安全目標執行績效，亦應每年定期審核本公司各層級、各部門及整體資通安全管理系統政策目標之有效性和適切性。

（三）本公司每年應依據「組織全景分析程序書(I-2-19)」，使用「組織全景鑑別表(I-2-19-01)」定期進行組織資通安全全景分析，鑑別可能影響組織達成資通安全管理系統預期成果能力者之內部及外部議題，瞭解利害關係者關注方對於資通安全之需要及期望。

（四）本公司應定義並每年定期進行資通安全管理系統「適用性聲明書(I-1-02)」審查，包含檢討資通安全管理系統適用範圍、納入或排除資通安全控制措施之項目及其理由之正確及適切性。

（五）本公司應建立資通安全管理系統配套管理程序，具體規範本公司之資訊安全暨個資保護各項作業準則，以符合資通安全暨個資保護法規之遵循要求。

（六）本政策經本公司「資通安全委員會」通過後實施，修訂時亦同。

陸、 使用表單與相關文件：

一、相關文件：

（一）本公司資通安全管理各階文件。

二、使用表單：

（一）組織全景鑑別表(I-2-19-01)

（二）資通安全目標有效性量測表(I-2-05-01)