資訊安全政策	文件編號	ISMS-MC-01	機密等級	內部使用
	版本	1.0	頁次/總頁數	1 / 9

資訊安全政策

目　錄

目　　錄 1
文件履歷 2
目　　的(1) 3
範　　圍(2) 3
參考文件(3) 3
權　　責(4) 3
名詞定義(5) 4
內　　容(6) 5
相關文件(7) 9
相關表單(8) 9
附　　件(9) 9

資訊安全政策	文件編號	ISMS-MC-01	機密等級	內部使用
	版本	1.0	頁次/總頁數	2 / 9

文件履歷

版本	變更理由	修訂內容	核准	審查	制定	日期
1.0	新發行	1、 導入 ISMS 管理系統	鍾又新	王宗祿	羅美伶	2026.01.05

資訊安全政策	文件編號	ISMS-MC-01	機密等級	內部使用
	版本	1.0	頁次/總頁數	3 / 9

1 目的

1.1 鑑於資訊安全乃維繫各項資訊服務安全運作之基礎，為確保本公司具備共識落實資訊安全的使命，特訂定本資訊安全政策（以下簡稱本政策），做為本公司資訊安全管理系統（Information Security Management System，以下簡稱 ISMS）的最高指導原則，以確保本公司管轄資訊資產之機密性、完 整性、可用性及符合相關法規之要求，進而保障全公司人員及客戶之權益。

2 範圍

2.1 適用範圍：本公司「適用性聲明書」所定義之 ISMS 實施範圍之所有組織單位、內外部人員、資訊資產及相關作業活動。

3 參考文件

3.1 ISO/IEC 27001:2022

3.2 ISO/IEC 27002:2022

3.3 個人資料保護法

3.4 資通安全管理法

3.5 NIST Cybersecurity Framework

3.6 客戶資安要求

3.7 產業相關最佳實務

4 權責

4.1 管理階層：

4.1.1 核准資訊安全政策。
4.1.2 確保政策與組織營運目標一致。
4.1.3 提供推動 ISMS 所需之資源。
4.1.4 展現對資訊安全之承諾與領導。
4.1.5 確保資訊安全角色與責任已被指派與溝通。
4.1.6 主持資安管理審查會議，確保持續改進。

4.2 資安代表：

4.2.1 規劃、建立與維護 ISMS。
4.2.2 制定資訊安全相關政策、程序與標準。
4.2.3 執行資訊安全風險評估與風險處理。
4.2.4 監督資訊安全控制措施之落實。
4.2.5 協調資安事件通報與應變處理。
4.2.6 定期向管理階層報告資訊安全狀態。

4.3 資訊單位：

4.3.1 實施資訊安全技術控制措施。
4.3.2 維護系統、網路與設備安全設定。
4.3.3 管理帳號、存取權限與系統記錄。
4.3.4 執行弱點修補與更新管理。
4.3.5 支援資安事件調查與處理。
4.3.6 定期執行資安監控與日誌分析。

4.4 部門主管：

4.4.1 負責其部門資訊資產之安全管理。
4.4.2 審核人員存取權限之申請與異動。
4.4.3 確保部門同仁遵循資訊安全政策。
4.4.4 配合資訊安全稽核與改善作業。

4.5 全體員工：

4.5.1 遵守資訊安全政策與相關規範。
4.5.2 妥善保護帳號、密碼及資訊資產。
4.5.3 即時通報疑似資訊安全事件。
4.5.4 不得從事違反資訊安全之行為。

4.6 第三方與供應商

4.6.1 遵守本組織相關之資訊安全要求與合約規範。
4.6.2 保護存取之資訊與系統。
4.6.3 發生資安事件時應即時通報。

5 名詞定義

5.1 資訊安全管理系統（Information Security Management System, ISMS）：基於風險管理方法，用來建立、實施、維護與持續改善資訊安全的一組政策、流程、程序與控制措施。

5.2 機密性（Confidentiality）：確保只有經授權的人員才能存取相關資訊資產。

5.3 完整性（ Integrity ）：維持資訊資產之正確與完整。

5.4 可用性（Availability）：確保經授權的人員在需要時，均能在可接受的時間內取得相關資訊資產。

5.5 核心系統：本公司核心業務持續營運之必要資通系統，包含核心業務所使用到的實體設備/作業系統/應用程式/資料庫、雲端服務、閘道網路存取控制軟硬體、核心網路設備。

5.6 資訊安全：係避免因人為疏失、蓄意或自然災害等風險，運用系統化之 控制措施，包含政策、實施、稽核、組織結構和軟硬體功能等，以確保本公司資訊資產受到妥善保護。

5.7 資訊資產：凡本公司作業流程中使用之各項相關資訊資產，包含人員、文件、網路服務、資訊設備軟硬體、基礎環境與便利設施等皆屬之。

6 內容

6.1 資訊安全管理要求事項

6.1.1 訂定資訊安全目標

6.1.1.1 本公司依照適用之法律法規要求、提供客戶專業之客戶服務。

6.1.1.2 為確保客戶服務品質，確保公司持續營運、保障客戶資訊安全之權益，本公司資訊安全目標為確保核心系統管理業務之機密性、完整性、可用性，依相關風險管理程序以及資訊安全目標、績效管理程序，定義及量測資訊安全績效之量化指標，以確認資訊安全管理系統實施狀況及是否達成資訊安全目標。

6.1.2 執行審查與評估

6.1.2.1 本政策應至少每年評估審查一次，考量法令法規、科技變化、利害相關團體之需求與期望、業務活動、內部管理與資源等最新現況，確保資訊安全實務作業之有效性。

6.1.2.2 本政策應依據審查結果進行修訂，修正時亦同。

6.1.2.3 本政策訂定或修訂後應以適當方式告知內外部利害相關團體。

6.2 建立資訊安全管理系統：依據 ISO/IEC 27001 指導規範之『規劃—執行—檢查—行動』模式，發展、維護及持續改善文件化的資訊安全管理規範，內容說明如下：

6.2.1 安全政策：訂定資訊安全政策做為資訊安全管理系統的指導方針，經由資訊安全組織管理階層核准、頒行，並透過適當管道，宣導給全體同仁，且於重大改變時或定期審查政策內容，以確保其適當性與有效性。

6.2.2 全景分析：透過風險評鑑會議或其它型式溝通渠道，蒐集並考量內外部議題與利害相關者要求，進行全景分析與風險管理。

6.2.3 資訊安全組織：成立資訊安全組職並賦予相對權責，以建置與維運本系統。

6.2.4 人力資源安全

6.2.4.1 處理高度機敏資訊之人員應執行適當之安全評估調查。

6.2.4.2 資訊安全職責載入工作職掌、僱用合約或協議中，且相關人員須簽署該份文件。

6.2.4.3 管理階層須要求人員遵循既定的安全規範。

6.2.4.4 政策與程序與資安認知須透過適當的教育訓練，告知相關人員並定期更新。

6.2.4.5 所有人員於離開工作崗位時，須按照既定的程序辦理相關資產退回與存取權限的變更或取消。

6.2.4.6 違反資安規範時，須施以適當的懲戒，以確保安控規範之實施成效。

6.2.5 資產管理

6.2.5.1 鑑別所有資產，將重要的資產作成清冊並維護之。

6.2.5.2 所有資訊資產都要指派專人管理。

6.2.5.3 確保機密專案結束或報廢之儲存媒體，內含之資料無法恢復。

6.2.5.4 根據資訊本身的價值、法律上的要求、敏感性或重要性等因素，區分其等級並做適當的標示，以妥當保護資訊資產，與風險管理。

6.2.6 存取控制

6.2.6.1 須有存取控制機制文件，以便遵循。

6.2.6.2 核心系統或關鍵業務流程應有使用者註冊、變更與刪除流程並定期審查權限。

6.2.6.3 使用者使用資訊服務設施，須設定使用密碼。

6.2.6.4 針對個資或敏感業務資料的顯示與存取進行限制。

6.2.6.5 訂定辦公作業保護措施。

6.2.6.6 訂定網路服務存取機制，以維護網路安全。

6.2.6.7 訂定遠端連線管理機制，以保護系統安全。

6.2.6.8 訂定應用系統之存取控制與隔離機制，以保護其相關的資訊。

6.2.7 密碼學

6.2.7.1 若使用金鑰加密資訊，應妥善保管金鑰，且熟悉如何更新金鑰與汰換。

6.2.7.2 非公開資料資訊的傳輸或保存，應視資料機密等級與實際需求予以加密或其它安全保護方式。

6.2.8 實體及環境安全

6.2.8.1 規範實體安全界限、進出管制方式、保護辦公處所及機房設備、載明在安全區域中工作的規範。

6.2.8.2 設備妥為安置與保護、提供適當服務之基礎公共設施、傳輸線需考慮其佈置安全性，及有適當的方法保護在公司內、外使用的設備。

6.2.9 作業安全

6.2.9.1 以實際系統運作狀況規劃資訊處理設施的需求，且採購時要確實執行驗收工作；設施運作時若需變更，須依據變更管理程序執行系統變更。

6.2.9.2 建立防範惡意程式碼之機制。

6.2.9.3 蒐集來自於府機關、設備原廠及產業專業社群之威脅情資政，以確保預警之即時性。

6.2.9.4 定期備份核心系統資料，以維持服務之完整性與可用性。

6.2.9.5 針對核心系統重要設備的設定，應建立組態基準。

6.2.9.6 機敏性資料外洩防護。

6.2.9.7 隨時監督系統使用是否發生異常狀況，並記錄之，同時妥善保存核心系統軌跡紀錄，以防止遭受竄改或破壞。

6.2.10 通訊網路安全

6.2.10.1 依據業務機敏程度落實網路分割，確保專案區域與一般區域網路邏輯隔離。

6.2.10.2 建立網路安全控制機制以維護網路安全。

6.2.10.3 業務應用系統、電子商務、電子郵件與即時傳訊軟體等，均須有適切的保護措施。

6.2.10.4 資訊傳遞應視資訊機密等級，予以安全地傳送。

6.2.11 供應商管理

6.2.11.1 落實供應商資安風險評鑑，並於合約中訂定資安違約處置方式。

6.2.11.2 資通訊委外服務包含雲端服務，應於合約或第三方協議中考慮資訊安全要求。

6.2.11.3 應定期或不定期監督供應商服務過程是否符合本公司資安要求。

6.2.11.4 應確保第三方之複委託機構亦應遵守本公司資安要求。

6.2.11.5 合約變更、調整應以不影響本公司資訊安全為最高原則。

6.2.12 資訊安全事故管理

6.2.12.1 建立資安事件、弱點發現與軟硬體失能通報機制，並從中學習以改善資訊安全環境。

6.2.12.2 訂定資訊安全事件/事故管理規範。

6.2.12.3 確實記錄與蒐集相關資安紀錄。

6.2.12.4 定期彙總分析資訊安全事件/事故，以採取適切的管控措施。

6.2.13 營運持續管理

6.2.13.1 明訂營運持續運作的管理流程。

6.2.13.2 針對關鍵營運流程與高機密專案之設備與資料，應確保具備容錯或快速恢復能力。

6.2.13.3 執行營運持續運作的計畫。

6.2.13.4 審查營運持續運作計畫的結果，以維持其適合性。

6.2.14 遵循性管理

6.2.14.1 鑑別適用的法令及規章，以確保法規與密碼學要求的符合性。

6.2.14.2 訂定使用智慧財產與營業秘密之相關合法保護要求，所有產出之研發成果、技術圖面與商業資訊均應視為公司資產，並依法採取合理之保護措施。

6.2.14.3 保障個人資訊與隱私權。

6.2.14.4 妥善保守公司重要之資訊紀錄。

6.2.14.5 訂定管理審查程序，定期審查安全政策與技術之符合性。

6.2.14.6 週期性的對資訊安全管理系統進行審查，確認資訊安全的控制目標、控制措施、政策、過程及程序的作法是否落實，並透過稽核制度防止舞弊事件。

6.2.15 專案資安管理

6.2.15.1 針對不同機敏等級之專案，建立差異化之資安控管措施。

6.2.15.2 對於高機密性專案，應於專案規劃階段即納入實體隔離、網路加密及資料外洩防護之要求，以確保專案資訊之生命週期安全。

7 相關文件

7.1 本公司 ISMS 一階至三階文件

8 相關表單

8.1 本公司 ISMS 四階表單

9 附件

9.1 無