資通安全管理

（一）資通安全管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源：

1. 資通安全風險管理架構

友邦集團由董事會負責監督集團內風險管理活動，其中包括資通安全，並由風險管理委員會提供支援與建議。本分公司依據集團風險管理委員會的組織架構原則，於資訊部下設立獨立資通安全單位，並配置資訊安全人員，負責以下作業：

(1) 負責本分公司轄內資通安全及技術風險管理作業
(2) 與集團協作資通安全相關作業
(3) 監控適於本分公司轄內之各項資通安全狀態

為確保本分公司所屬之資訊資產的機密性、完整性及可用性，並保障資訊使用者資訊隱私，以符合相關法規之要求，免於遭受內、外部蓄意或意外之威脅，並衡酌本分公司之業務需求，本分公司已導入並取得資訊安全管理制度(ISO 27001)及個人資料管理制度(BS 10012)認證。

2. 資通安全政策

本分公司為有效落實資安管理，遵循集團各項強制性政策要求，以達成以下目標：

- 建立有效的資訊治理
- 使資訊作業與營運策略保持一致
- 提高所提供資訊服務的品質
- 降低提供服務的長期成本
- 遵守與資訊作業相關的適用法令和監管要求

本分公司已於民國 106 年取得 ISO/IEC 27001 資訊安全管理制度認證並持續維護認證有效性，及持續落實各項資安管控措施。為了加強個資保護，亦於民國 111 年導入 BS 10012:2017 個人資料管理制度並取得認證。

3. 具體管理方案

本分公司由資訊長擔任召集人，設立資訊安全委員會，以統籌辦理各項資訊安全政策研議、計畫執行、資源調度等事項，具體管理方案包含：

(1) 網路環境安全，如強化網路區域控管措施、端點防毒防駭及上網保護。
(2) 資料保護及存取權限管理、脆弱性管理，如定期安全檢測及漏洞修補作業。
(3) 應用程式安全，實施軟體發展生命週期管理及持續強化應用程式安全控管機制，並整合於開發及維運管理流程。
(4) 第三方管理，加強供應商及合作夥伴資訊安全管理檢核機制，並持續關注安全管理狀態。
(5) 辦理資訊安全認知宣導措施，如訓練課程及各項演練，強化員工資訊安全意識。

4. 投入資通安全管理之資源

(1) ISO/IEC 27001(ISMS)認證維護
持續落實資訊安全管理要求，持續保持認證的有效性
(2) BS 10012(PIMS) 認證維護
導入個人資料管理制度，落實個資各項保護之要求
(3) 資訊安全評估
A. 配合集團資訊安全活動辦理各項監控及強化改善
B. 委託外部專家定期執行公司資訊安全評鑑作業
(4) 社交工程郵件演練
集團內每季辦理社交工程郵件，演練未通過比率<3%，低於業界標準
(5) 資訊安全及營運持續演練
A. 參與集團資訊安全應變演練
B. 個資外洩事件應變程序演練
C. 辦理異地備援演練
D. 辦理 DDoS 演練，以提升攻擊承受韌性及驗證相關保護與通報機制之有效性
(6) 資訊安全教育訓練
A. 資訊安全人員完成 15 小時以上專業訓練
B. 全公司完成 3 小時一般認知教育訓練
C. 物聯網設備管理人員完成進階資安課程
(7) 脆弱性管理
A. 對外服務網站定期辦理入侵滲透測試，以強化防護韌性
B. 定期弱點掃瞄及風險處理作業
C. 安全修補程式更新作業

(二)最近年度因重大資通安全事件所遭受之損失、可能影響及因應措施：

本分公司近年無發生重大資安事件。

(三)資通安全風險對公司財務業務之影響及因應措施：

1. 資訊技術安全之風險

來自任何第三方癱瘓系統的網路攻擊，可能企圖竊取公司的營業祕密及其他機密資訊，如以非法方式入侵本分公司的內部網路系統，破壞公司之營運與損及公司商譽等活動，並可能影響資訊系統及設施之正常運作。

這些攻擊可能導致公司因延誤或中斷服務而需賠償客戶的損失；或需擔負龐大的費用實施補救和改進措施，以加強公司的網路安全系統；也可能使本分公司因涉入公司對其有保密義務之員工、客戶或第三方資訊外洩而導致的相關法律案件或監管調查，而承擔重大法律責任。

2. 資訊技術安全之管理措施

友邦集團為因應日新月異的資訊科技及各種資訊安全威脅，制定集團資訊管理政策涵蓋資訊作業營運之各方面要求，並規範一致性之資訊交付價值鏈，包含規劃、SDLC、資訊營運服務與支援、監督管理和治理等功能框架。

在每項功能框架中，將其拆分為不同的細項策略領域。資訊交付價值鏈的第1層級是端對端資訊營運的核心功能領域，建構了友邦集團重要的交付程序，包含敏捷與技術交付的價值。第2層級則是能力領域，定義了資訊管理的核心工作，係根據業務需求進行操作與調整，在此層級中建構了本集團資訊管理政策，涵蓋資訊營運的所有重要構面，持續推動資通安全管理願景的實現，並為有效管理關鍵網路安全功能提出了標準及指導。

本分公司依據上述標準與指導要求，已建立全面的網路與電腦系統相關資安防護措施，透過持續檢視和評估資訊安全規章及程序，以確保其適當性和有效性，控管或維持公司營運及財務等重要企業功能之電腦系統，並期在瞬息萬變的資訊安全威脅中，降低各種推陳出新的風險和攻擊影響。