福裕事業股份有限公司

資通安全管理政策

機密等級：■一般 □內部 □機密

文件編號：FALCON-ISMS-1-01-00

發行版次：V1.0

發行日期：115 年 06 月 22 日

文件編號	FALCON-ISMS-1-01-00	資通安全管理政策	機密等級	一般
發行版次	V 1.0		發行日期	115/06/22

文件制/修訂紀錄

版次	發行日期	制/修訂說明	修訂單位	修訂者	核准者
V1.0	115.06.22	初版發行			

目 錄

1. 目的

福裕事業股份有限公司(以下簡稱本公司)資訊相關系統設備除提供內部人員作業處理外，亦透過電腦網路提供與外部人員互動之溝通管道，其相關資通系統作業應用之持續性運作，攸關本公司形象及業務推動，故訂定本資通安全管理政策，作為資通安全工作之指導方針，藉以降低資通風險。

2. 適用範圍

本公司所有單位及往來委外廠商均應遵守資通安全管理政策。

3. 名詞定義

3.1 機密性(Confidentiality, C)：使資訊不得被未經授權之個人、個體或過程所取得或揭露的性質。

3.2 完整性(Integrity, I)：保護資產之準確度和完全性的性質。

3.3 可用性(Availability, A)：在獲授權個體要求時，可取得及使用之性質。

4. 作業內容

4.1 政策聲明

為使本公司業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性(C)、完整性(I)及可用性(A)，特制訂本政策如下：

4.1.1符合法令法規。

4.1.2確保營運持續。

4.1.3資料不得外洩。

4.2 作業流程執行與要求

4.2.1資安組織：設置資通安全推動小組，負責本公司資通安全管理之建立及推動、執行、協調監督及審查。

4.2.2教育訓練：定期實施資通安全教育訓練，宣導資通安全管理政策及實施規定，以提升公司同仁資通安全知識與防範觀念。

4.2.3資源規劃：建立資訊資產管理機制，統籌分配並有效應用資源，解決安全問題。

4.2.4 情資蒐集：蒐集並分析資安相關資訊以產生威脅情資，並作為事件防範的參考依據。

4.2.5 資安防範：新資通系統或服務建置或推出前，應納入資通安全因素，以防範危害安全情況之發生。

4.2.6 安全監控：建立資通安全監控與防護措施，並定期進行檢視。

4.2.7 權限管理：明確規範資通系統、網路服務、敏感資訊之使用權限，防止未經授權存取之行為。

4.2.8 業務持續：訂定資通安全之營運持續計畫並實際演練，確保突發事故發生時得以應變。

4.2.9 持續改善：訂定及執行內外部稽核活動，以落實資通安全管理制度，並針對未盡事項執行改善。

4.2.10領導承諾：本公司管理階層應積極參與資通安全管理活動，並提供推展資通安全管理系統所需之支持及承諾。

4.3 資通安全責任

4.3.1 本公司管理階層負責建立及審查資通安全管理政策。

4.3.2 資通安全管理者應透過適當的標準和程序推動資通安全管理政策。

4.3.3 所有人員皆應遵守相關安全管理程序以維護資通安全管理政策。

4.3.4 所有人員均有責任通報資通安全事件和任何已鑑別出的弱點。

4.3.5 任何蓄意違反資通安全的行為將受到相關規範或法律行動。

4.4 溝通或傳達

為使本公司之政策、需求及目標能有效地傳達到與業務相關之關注方，將利用媒體、函文、會議、網頁、電子郵件及文宣等途徑，進行彼此關注議題討論及溝通，於必要時得邀請相關人員參與，並留存紀錄作為後續之依據。

4.5 政策修訂

4.5.1本政策每年應至少評估檢討一次，以反映本公司資通安全需求、合作夥伴要求、政府法令法規、外在網路環境變化及資通安全技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力。

4.5.2本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知與業務相關之關注方，以利共同遵守。

4.6 目標之核定與評量

參考來自內、外部關注方之法律、法規與契約相關資通安全要求事項，每年於管理審查會檢討及議定下年度之目標並透過有效性量測機制確認各項資安目標之達成狀況。

5. 資安目標

5.1 資訊安全機密性量測指標：
同仁遭查獲洩漏機敏資料件數每年不得發生。

5.2 資訊安全完整性量測指標：
同仁回報資料遭竄改件數每年不得發生。

5.3 資訊安全可用性量測指標：
連外主幹網路中斷 4 小時件數每年需低於 2 次。

5.4 資訊安全法律遵循量測指標：
同仁違反「國家機密保護法」、「營業秘密法」、「著作權法」等相關法規件數每年不得發生。

5.5 資安認知課程訓練量測指標：
員工接受資訊安全管理系統或資安認知課程訓練時數每年應大於 2 小時。

5.6 資安專職(責)人員專業證照指標：
總計應持有一張以上資通安全專業證照，並持續維持證書之有效性每年應大於 1 張。

6. 參考文件

6.1 ISO/IEC 27001:2022(Information security, cybersecurity and privacy protection — Information security management systems — Requirements)

6.2 ISO/IEC 27002:2022(Information security, cybersecurity and privacy protection — Information security controls)