資訊安全政策

一、目的

1. 確保公司內部網路設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險。
2. 確保業務資訊之機密性、完整性與可用性。
   A. 機密性：確保機密資訊資產受必要之保護，以防機密外洩。
   B. 完整性：確保使用之資訊資產正確無誤、未遭竄改。
   C. 可用性：確保僅被授權之人員能取得所需資訊資產。

三、適用範圍

1. 公司資訊安全管理制度所涵蓋範圍皆適用之。
2. 本公司資訊安全管理涵蓋組織控制(A.5 系列)、人員控制(A.6 系列)、實體控制(A.7 系列)、技術控制(A.8 系列)等領域，依據 ISO 27001:2022 年版條文展開必要之資安管制措施，以避免因人為疏失、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，造成公司可能產生風險及危害。

四、資安政策框架

1. 公司各項資訊安全管理規定必須遵守政府相關法規。
2. 成立資訊安全管理組織負責資訊安全制度之建立及推動事宜。
3. 定期實施資通安全教育訓練，宣導資訊安全政策及相關實施規定。
4. 建立主機及網路使用之管理機制，以統籌分配、運用資源。
5. 新設備建置前，將全因素納入考量，應防範潛在之危害。
6. 明確規範網路系統之使用權限，防止未經授權之存取動作。
7. 訂定內部稽核計畫，定期檢視公司資訊安全管理制度執行成效。
8. 定期向管理者報告資訊安全之持續改善事項，並定期追蹤。

五、資安宣示

1. 建置合宜資安制度。
2. 強化實體網路環境。
3. 落實各項控制措施。
4. 持續優化資安認知。

六、資安政策之評估與審查

本政策應至少每年評估及審查一次，以反映政府政策、法令、現行技術及公司業務等之最新發展現況，以確保公司資訊安全管理制度的適切性及有效性。

七、實施

本政策經總經理核准，於公告日施行，並以書面、電子或其他方式通知本公司同仁及利害相關者，修正時亦同。