隴華電子股份有限公司

資訊安全政策

1 目的

為遵循相關法令並保護隴華電子股份有限公司（以下簡稱本公司）資訊資產(包括資料、軟體、硬體設備等)，免於因外在之威脅，或內部人員不當之管理與使用，致遭受竄改、揭露、破壞或遺失等風險，特制訂資訊安全政策以做為遵循依據。

2 政策說明與目標

2.1 政策目的與說明

本公司資訊安全目標為確保重要及核心系統之機密性(Confidentiality)、完整性 （Integrity）、可用性（Availability）及遵循性(Compliance)。並依各階層與職能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。

- 機密性:應避免本公司任何敏感資訊洩露於網際網路。
- 完整性:應確保本公司敏感資料（如:財務資訊、人事資料、系統資訊）之正確性。
- 可用性:應確保本公司所持有的重要資料確實備份。
- 遵循性:應確保本公司避免違反法律、法令、法規或契約義務對資訊安全之要求

為達成本公司之任務目標及最高管理階層對資訊安全之期許與要求,確保本公司資訊資產之安全，資訊安全政策訂為：

2.1.1 確保本公司相關業務資訊之機密性， 防止本公司機密資訊及個人資料外洩與遺失。

2.1.2 確保本公司相關業務資訊之完整性與可用性,以正確執行本公司作業與各項業務。

2.1.3 確保本公司相關業務資訊之遵循性,防止本公司違反法律法規與合約。

2.2 目標

為達成上述政策目的，將相關目標分為定量與定性二類：

2.2.1 定量化目標，舉例如下：

A. 每年至少進行一次營運持續運作計畫之測試及檢核。

B. 每年至少召開一次管理審查會議

C. 確保相關資訊安全措施或規範符合政策與現行法令之要求，每年至少進行一次資訊安全查核。

2.2.2 定性化目標，舉例如下：

A. 確保只有經授權的人員才能存取相關資訊。

B. 確保系統與網路之正常運作,避免因作業疏忽或意外導致系統或網路無法提供服務

C. 確保資訊資產受適當之保護與備份,防止未經授權或因作業疏忽對資產所造成之損害。

D. 確保所有資訊安全事件或可疑之安全弱點,皆依適當通報程序反映，並予以適當調查及處理。

E. 確保相關資訊安全措施、規範與作業符合政策與現行法令之要求，定期進行相關查檢。

F.定期實施資訊安全教育。

2.2.3 為落實資訊安全目標有效性評核,將另行訂定細部之年度資訊安全管理目標量測方式，經本公司資訊安全委員會核准通過後施行。

3 適用範圍

3.1 為推動資訊安全管理制度，經評估本公司之內外部資安議題、相關單位對資安的要求，及本公司資安防護措施，進而確定本公司資訊安全管理

架構範圍。

3.2 本政策適用於本公司各部門，以公司導入 ISO 27001 驗證範圍部門為主要執行範圍。

4 資通安全組織

為確保資訊安全管理系統能有效運作，本公司成立資訊安全管理委員會，統籌資訊安全管理制度之規劃及推動事宜，其組織架構請參考「資訊安全手冊」與「資訊安全組織及管理審查作業程序書」。

5 實施與管理原則

資訊安全管理系統之實施應依據規劃（Plan）、執行（Do）、查核（Check）及持續改善（Action）循環模式，以週而復始、循序漸進的精神，確保資訊安全之有效性及持續性。

本公司依照 ISO/IEC 27001:2013 管控要項條文規範如下：

5.1 人力資源安全：為降低人為因素影響本公司資訊安全，各單位應考量人力與工作職掌，實行分工與輪調措施；並視需要實施適當之資訊安全教育、訓練及宣導，以提升人員對資訊安全之認知。

5.2 資產管理：為保護本公司資訊資產安全，應建立資訊資產清冊，並訂定資訊資產分類、分級及管控措施作業原則。

5.3 存取控制：

5.3.1 為確保資訊處理設備之授權存取，應訂定使用者密碼、註冊、變更、刪除及定期審查機制，並訂定辦公桌及電腦螢幕淨空措施。

5.3.2 為維護網路安全，應訂定網路服務機制，區隔內部網路與聯外方式，管控遠距工作及行動裝置之使用。

5.4 密碼學：訂定適當與有效使用密碼政策，保護資訊的機密性、鑑別性及完整性。

5.5 實體及環境安全：為確保機房、辦公處所與相關設備之安全，應訂定電腦機房門禁、設備檢查與管理原則，並訂定辦公室一般資訊設備使用、管理及報廢原則。

5.6 運作及通訊安全：

5.6.1 為確保正確、安全地操作資訊設備，應訂定資訊正確使用之規範，以防範機密資訊外洩，並建立防範惡意程式碼及可移動程式

碼之機制。

5.6.2 為確保資訊資產完整性及可用性，應訂定資訊處理設施備份作業及採用外部資訊處理設施服務管控原則。

5.6.3 為維護網路安全，應訂定網路安全控制機制及監督系統使用狀況軌跡保護原則。

5.7 系統獲取、開發及維護：為確保應用系統開發管理、測試、驗收、上線、維護及委外管理作業之安全，應訂定標準管制程序。

5.8 供應者關係：訂定供應者關係與管理，以確保供應者存取、處理及管理本公司資訊與資訊處理設施之安全。

5.9 資訊安全事件管理：為降低資訊安全事件造成之損害，應建立資訊安全通報及處理程序，並加以記錄。

5.10 營運持續管理之資訊安全層面：為確保本公司業務持續運作，應明定營運持續管理之資訊安全層面控制原則，建立業務持續運作管理流程及架構，並撰寫及實施業務持續運作計畫。

5.11 遵循性：為確保資訊安全管理系統之施行符合相關法令、安全政策及最新技術趨勢，應訂定遵循性確認原則。

6 審查與修訂

6.1 本文件應至少每年評估審查一次，考量法令法規、科技變化、關注方期望、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。

6.2 本文件應依據審查結果進行修訂，並經發佈後始生效。

7 其他規定

7.1 本政策應以適當之方式(例如：口頭、書面、電子郵件或其他通知方式)溝通傳達予員工、接觸本公司業務之公私立機關（構）及提供資訊服務之廠商知悉，並配合相關資安規定要求。

7.2 本公司所有人員(正職與專案計畫人員)應遵循並落實本政策之要求，若有違反本政策，或發生其他任何危及本公司資訊安全之行為，都將訴諸適當之處置程序或法律行動。

7.3 本公司與委外服務廠商簽訂相關合約時應遵循本政策之規定與相關要求。

8 附則

8.1 訂定及修正已於民國 111 年 12 月 15 日經本公司董事會通過。