資通電腦股份有限公司
資訊安全政策

機密等級：公開
文件編號：ISMS-01-01
發行日期：109 年 10 月 21 日
修訂日期：無
版次：1.0

版本記錄

版本	日期	修訂說明	備註
1.0	109 年 10 月 12 日	初版	

目 錄

1 目的

鑑於資訊安全乃維繫各項服務安全運作之基礎，為確保資通電腦股份有限公司（以下簡稱本公司）具備共識落實資訊安全的使命，特訂定資訊安全政策（以下簡稱本文件），做為本公司資訊安全管理系統的最高指導原則。

2 目標

本公司資訊安全目標為確保核心系統管理業務（意即 ISO27001 驗證範圍內之資訊系統與相關管理活動）之機密性（Confidentiality）、完整性 （Integrity）、可用性（Availability）與法遵性（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。

2.1 機密性：應避免本公司任何敏感資訊洩露於網際網路。

2.2 完整性：應確保本公司敏感資料之正確性。

2.3 可用性：應確保本公司所持有的重要資料確實備份。

2.4 法遵性：應遵循我國相關法律（如：個人資料保護法、營業秘密法、智財權相關法律），避免本公司或第三方人士權益受侵害。

3 適用範圍

本公司。

4 組織與權責

為強化本公司資訊安全，健全資訊安全管理制度，確保資訊安全管理系統能有效運作，特設立資安管理委員會（以下簡稱本委員會），以推動及維持各類管理、執行與查核等工作之進行。本委員會由總經理、資訊長、管理部主管、稽核經理、資服部技術支援組同仁組成。由資訊長兼任召集人，於必要時得邀請相關人員召開會議。

本委員會權責如下：

4.1 定期會同資安管理代表及各組代表召開管理審查會議。

4.2 核准並頒行資訊安全政策及相關規範等一、二階資訊安全管理系統文件。

4.3 資安管理委員會成員異動之核准與發佈。

4.4 進行資訊安全管理制度之審查

4.5 審核風險評鑑的結果與風險處理計畫

4.6 資訊安全事務之分配、協調與督導。

5 實施原則

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。

6 審查與評估

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，並經董事會通過後由資訊安全管理委員會發佈始生效。

6.3 本文件訂定或修訂後應以適當方式（例：E-Mail 或網站公告或紙本印出）告知利害關係人，如：所屬員工、供應商、客戶、外部稽核人員等。

管理架構

- 為強化本公司資訊安全，健全資訊安全管理制度，確保資訊安全管理系統能有效運作，特設立資安管理委員會（以下簡稱本委員會），以推動及維持各類管理、執行與查核等工作之進行。本委員會由總經理、資訊長、管理部主管、稽核經理、資服部技術支援組同仁組成。由資訊長兼任召集人，於必要時得邀請相關人員召開會議。
- 109 年執行情形：為提升本公司資訊安全管理能力，自 109 年 5 月起每月定期召開資安管理審查會議，審查資訊安全發展現況及未來方向，確保資訊安全管理制度持續運作。
- 自 5 月以來，針對資訊安全政策與辦法、資安教育訓練、機房管理辦法、安裝監視攝影設備、重要資料備份與還原演練、VPN 管理措施、防火牆政策、外部人員使用本公司網路規範…等均有討論後改進修訂，使資安管理機制更佳完備。
- 資訊安全政策條文修訂已於 109 年 10 月 21 日第 5 次董事會報告在案。

資安政策

- 目的：鑑於資訊安全乃維繫各項服務安全運作之基礎，為確保資通電腦股份有限公司（以下簡稱本公司）具備共識落實資訊安全的使命，特訂定資訊安全政策，做為本公司資訊安全管理系統的最高指導原則。
- 目標：本公司資訊安全目標為確保核心系統管理業務之機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）與法遵性（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。
  - 法遵性：應遵循我國相關法律（如：個人資料保護法、營業秘密法、智財權相關法律），避免本公司或第三方人士權益受侵害。

管理方案

- 資訊資產管理：所有的資訊資產都需依其性質及其存在方式作適當的處理與防護，必須依資訊資產之特性於明顯處註明資訊等級，以為所有相關人員之作業準則。
- 存取控制管理：控管同仁與第三方人員對服務營運相關之資產、網路、系統、應用程式及其資訊之存取防止任何未經授權之存取行為，及保護機敏性資料或設備免於竊取或破壞之風險。
- 網路安全管理：網路分成外網及內網，其間以網路閘道設備區隔。定期檢測網路運作環境之安全漏洞。應用監控措施，以確保安全相關活動的紀錄留存。
- 實體與環境安全管理：保護本公司之設備及周邊設施，降低因環境安全、設備操作、維護與管理疏失或不當，造成資產遭受失竊、破壞、遺失之機會，以達成安全控管的目的。
- 資訊系統開發管理：系統購置或開發前應進行安全功能需求之評估，開發過程須確保開發人員於原始碼及敏感資料之存取權限適切地劃分，並確保資訊系統於資料處理過程中的正確性及系統開發環境之安全。