智新資通股份有限公司

文件名稱：資訊安全組織與管理審查程序			
文件編號：ISMS-2-002	版本：B	頁次：1/6	發行日期：2025/01/24

版本修訂紀錄表

文件版本	制/修訂日期	修訂重點內容	修訂人員
A	2023/01/07	初稿	潘彣昕
B	2025/01/20	新增項次5.2.4.簽到表/7.3簽到表。	Judy

智新資通股份有限公司

文件名稱：資訊安全組織與管理審查程序			
文件編號：ISMS-2-002	版本：B	頁次：2/6	發行日期：2025/01/24

1. 目的：

確保本公司資訊安全管理架構建立並能透過管理審查，能使資訊安全系統能持續有效的運作，並符合國際規範之標準。

2. 範圍：

本公司與資訊安全組織架構及相關權責之管理。

3. 權責：

3.1. 資訊安全組織建立：最高管理階層。

3.2. 資訊安全管理會議主席：主任委員。

3.3. 資訊安全管理會議通知：管理代表。

3.4. 資訊安全管理會議紀錄：資訊安全管理委員會。

3.5. 資訊安全管理會議出席人員：資訊安全管理委員會成員。

4. 名詞釋義：無。

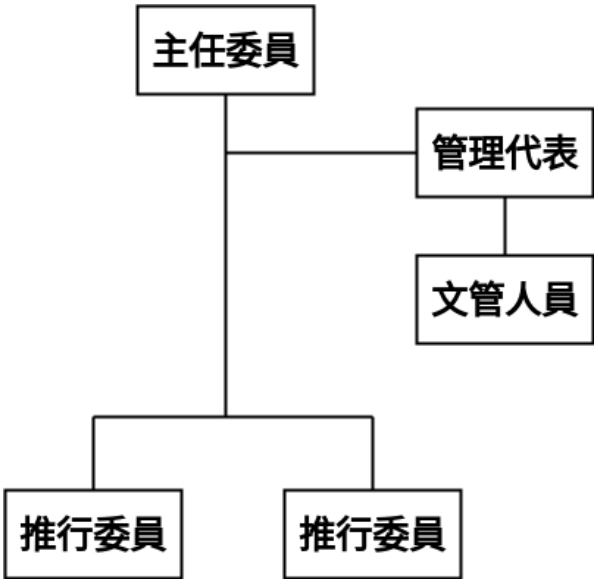
5. 作業內容：

5.1. 資訊安全組織

5.1.1. 資訊安全委員會組織圖

智新資通股份有限公司

文件名稱：資訊安全組織與管理審查程序			
文件編號：ISMS-2-002	版本：B	頁次：3/6	發行日期：2025/01/24



5.1.2. 資訊安全管理委員會由負責人指派高階管理階層擔任主任委員，負責公司資訊安全管理制度之政策及目標核准、相關事務之資源取得、分配、協調與督導。

5.1.3. 主任委員指派適當人員擔任管理代表，負責資安各標準制度之建置、實施與維持，資源調度等事項之協調及研議。

5.1.4. 建立「資訊安全組織成員表」，以確保任務明確之指派及ISMS有效之聯繫。

5.1.5. 「資訊安全組織成員表」需呈主任委員核准。

5.1.6. 資訊安全委員會之任務分配如下：

5.1.6.1. 主任委員：

5.1.6.1.1. ISMS管理制度之政策核准。

5.1.6.1.2. ISMS系統之目標的核准與確保審查框架的建立。

5.1.6.1.3. ISMS管理制度相關事務之資源取得、分配、協調與督導。

5.1.6.2. 管理代表：

5.1.6.2.1. 管理代表本身具有一切與資訊安全管理運作的監督權責，當資訊安全管理

系統運作發生異常時賦有向高階管理階層直接提報權力，不受行政系統與外部影響。

5.1.6.2.2. 協助召開管理審查會議、資訊安全會議。

5.1.6.2.3. 依照國際標準、公司政策及客戶需求之規定，負責要求建立、執行、維護符合資訊安全管理活動的書面化程序。

5.1.6.2.4. 督導資訊安全事務之分配與協調，包含資訊安全管理認證單位之聯繫窗口。

5.1.6.2.5. 協助高階管理階層提升全員對客戶資訊安全要求、法令法規的認知。

5.1.6.2.6. 透過內部稽核活動成果，負責將資訊安全管理實施成效，向管理階層報告，以作為系統改善依據。

5.1.6.2.7. 召開ISMS各階段會議。

5.1.6.3. 文管人員：

5.1.6.3.1. 應於定期（臨時）會議中報告有關本管理系統之運作及有關之紀錄。

5.1.6.3.2. 統一對公司員工發佈本系統相關事項。

5.1.6.3.3. 宣達與執行本委員會決議事項。

5.1.6.3.4. 配合輔導顧問實施輔導工作。

5.1.6.3.5. 協同驗證機構辦理驗證工作。

5.1.6.4. 推行委員：

5.1.6.4.1. ISO 27001 資訊安全管理系統的推動、維持及改善。

5.1.6.4.2. 負責資訊安全管理制度相關程序文件之審查。

5.1.6.4.3. 負責資訊資產盤點、風險評估、風險處置、殘餘風險處理的策劃之全過程。

5.1.6.4.4.相關法令、法規遵循之界定與更新。

5.1.6.4.5.負責資訊安全之適用性聲明書之修訂。

5.1.6.4.6.緊急應變通報、災害復原系統的規劃。

5.1.6.4.7.負責持續營運計畫之制定、修訂與維護。

5.1.6.4.8.出席資訊安全管理審查會議。

5.2.資訊安全管理審查：

5.2.1.資訊安全管理會議每年執行一次，由資訊安全管理委員會規範開會議題，並收集開會資料。

5.2.2.資訊安全管理會議議程如下：

5.2.2.1.過往管理審查之議案的處理狀態，由管理代表提報。

5.2.2.2.與資訊安全管理系統有關之內部及外部議題的變更：「組織前後環節鑑別表」審查，由管理代表提報。

5.2.2.3.資訊安全績效之回饋，包括下列之趨勢。

5.2.2.3.1.不符合項目及矯正措施：資安事件及矯正活動審查，由事件負責人提報。

5.2.2.3.2.監督及量測結果：LOG監控、容量管理、防毒監控及弱點掃描…等結果，由網路/系統負責人提報。

5.2.2.3.3.稽核結果：內部及外部稽核結果，由管理代表提報。

5.2.2.3.4.資訊安全目標之達成：資訊安全目標達成狀況審查，由各目標負責單位提報。

5.2.2.4.關注方之回饋：客戶、供應商或員工對資訊安全管理系統之反應及意見，由與會成員依需求提報。

5.2.2.5.風險評鑑結果及風險處理計畫之狀態，由管理代表提報。

5.2.2.6.持續改善之機會，由與會成員依需求提報。

5.2.2.7.資訊安全政策的的合宜性、適切性及有效性，由管理代表提報。

5.2.3. 由管理代表在開會前，通知各單位開會時間、議程與開會地點。

5.2.4. 各與會成員收到資訊安全管理會議通知時，應依資訊安全管理會議議程進行資料收集與彙整，並於開會前完成，參加會議時應於「簽到表」簽到。

5.2.5. 會議討論順序，可參照會議議程順序進行討論，並應做成改善或討論決議事項。

5.2.6. 資訊安全管理會議應依議程討論後，結果應包含與持續改善機會有關之決策，以及任何對資訊安全管理系統變更之需要。

5.2.7. 由與會成員提供會議紀錄資料，再由管理代表指派專人完成「會議紀錄」，再呈管理代表及主任委員核准。

5.2.8. 資訊安全管理會議「會議紀錄」至少應保存3年。

6. 相關文件：無。

7. 使用表單：

7.1. 資訊安全組織成員表(ISMS-2-002-01)

7.2. 會議紀錄(ISMS-2-002-02)

7.3. 簽到表(ISMS-2-002-03)