新竹市政府

資訊安全組織程序書

機密等級：	■公開□內部□機敏
文件編號：	ISMS-2-01-00
制(修)訂日期：	110 年 03 月 05 日
版　次　：	V2.3

文件制／修訂紀錄表

文件版本	修訂日期	制／修訂摘要說明	制(修)訂單位	核准者
V1.0	107 年 06 月 20 日	新制訂文件	行政處資訊科	召集人
V2.0	108 年 02 月 26 日	調整本府資安長由秘書長擔任	行政處資訊科	召集人
V2.1	108 年 11 月 13 日	修訂參考文件	行政處資訊科	副召集人
V2.2	109 年 09 月 22 日	於資訊安全處理小組成員內增加資安專責人員	行政處資訊科	召集人
V2.3	110 年 03 月 05 日	1. 資安委員之成員：修訂為本府各單位及所屬機關副主管擔任 2. 資訊安全處理小組資安專責人員修訂為資通安全專職人員並增加其業務職掌及能力需求	行政處資訊科	召集人

目　錄

壹、總則

一、制訂目的：新竹市政府（以下簡稱本府）為順遂推動資訊安全管理系統，明確規定資訊安全相關組織之角色及職掌，以示對資訊安全之重視及支持，進而使內部組織及內部控制達到最佳化，特訂定資訊安全組織程序書以資遵循。

二、適用範圍：本府資訊安全管理系統之建立、實施與控制等作業。

三、權責單位：本府行政處資訊科。

四、名詞定義：無。

五、工作流程：無。

貳、內容

一、組織與分工

(一) 資訊安全管理委員會

由本府資安相關業務人員組成，並紀錄於「ISMS-2-01-01 資訊安全組織名冊」。

1. 召集人(資安長)

(1) 成員：由本府秘書長擔任。

(2) 職責：

A. 擔任資訊安全管理系統之驗證代表。

B. 督導資訊安全管理系統之核准及實施。

C. 發生 3 級以上資安事件時，資安長(或其授權人員)應召開會議研商相關事宜，並請相關機關(單位)提供協助。

D. 調配資通安全事件(故)處理所需之資源，必要時得請求相關人員協助。

2. 副召集人

(1) 成員：由本府行政處處長擔任。

(2) 職責：

A. 協助擔任資訊安全管理系統之驗證代表。

B. 協助督導資訊安全管理系統之核准及實施。

3. 執行秘書

(1) 成員：由本府行政處資訊科科長擔任

(2) 職責：

A. 推動資訊安全管理系統之核准及實施。

B. 負責資安工作推動之各項協調工作。

C. 綜理安全預防及危機處理事宜

4. 資安委員

(1) 成員：

本府各單位及所屬機關副主管擔任，如有更新，需通知本府行政處資訊科

(2) 職責：

A. 審核資訊安全管理系統目標及實施範圍。

B. 審核資訊安全管理相關作業執行情形及改善的有效性。

C. 檢討資訊安全相關政策及規定，協調資源之分配及使用。

D. 監督營運持續演練之辦理。

E. 審核實施矯正措施所需之資源，包括人力、時間及經費。

F. 審核矯正措施之有效性。

G. 每年至少召開管理審查會議 1 次，必要時得召開臨時會議。

H. 資訊安全相關事項宣導與傳達。

(二) 資訊安全工作小組

1. 資訊安全處理小組

(1) 成員：

A. 組長: 由本府行政處資訊科指派同仁擔任。

B. 組員: 由組長指派適當人員擔任。

C. 資通安全專職人員: 由資安長於資訊安全處理小組依「資通安全責任等級分級辦法」配置 2 名成員。

(2) 職責：

A. 蒐集並提供資訊安全相關資訊，如防護、防毒及防駭等，並適時發布公告。

B. 建置資訊安全措施，執行資訊安全監控等安全事項。

C. 規劃危機處理程序，清查危機事件原因、確定影響範圍及損失評估，執行應變措施，辦理資訊安全通報，並執行解決辦法等危機處理事項。

D. 依據相關營運持續計畫與資安事件管理作業說明書，執行災害復原工作。

E. 矯正措施啟動時間之鑑別，定期追蹤查核實施成效。

F. 資訊安全管理系統文件撰寫及修訂

G. 辦理資訊安全管理系統文件教育訓練與執行

(3) 資通安全專職人員職務內容：

A. 2 名專職人力：1 名負責策略面及管理面工作，另1 名負責技術面工作。

B. 策略面：

(A)機關(及所屬)資安政策、資源分配及整體防護策略之規劃。

(B)機關導入資安治理成熟度之協調與推動。

(C)資通安全維護計畫實施情形之績效評估與檢討。

(D)稽核所屬(或監督)公務機關之資通安全維護計畫實施情形。

C. 管理面：

(A)訂定、修正及實施資通安全維護計畫並提出實施情形。

(B)辦理下列機關資通安全責任等級之應辦事項：資訊安全管理系統之導入及通過公正第三方之驗證、業務持續運作演練、辦理資通安全教育訓練等。

(C)針對所屬(或監督)公務機關，審查其資通安全維護計畫及實施情形。

D. 技術面：

(A)整合、分析與分享資通安全情資。

(B)訂定、建立及執行資通安全事件通報及應變機制。

(C)辦理資通安全事件通報之審核、應變協處與改善報告之審核。

(D)規劃危機處理程序，清查危機事件原因、確定影響範圍及損失評估，執行應變措施，辦理資訊安全通報，並執行解決辦法等危機處理事項。

(E)辦理下列機關資通安全責任等級之應辦事項：安全性檢測、資通安全健診、資通安全威脅偵測管理機制、政府組態基準、資通安全防護等。

(F)配合主管機關辦理機關資通安全演練作業，並針對所屬(或監督)公務機關，規劃及辦理資通安全演練作業。

2. 文件管制小組

(1) 成員：由本府行政處資訊科指派同仁擔任組長，組員由組長指派適當人員擔任。

(2) 職責：

A. 資訊安全管理系統內部文件及外來文件發行、保管、借閱與銷毀及版本管理。

B. 資訊安全管理系統文件進行電子公告及更新管理。

C. 紙本紀錄儲存與管理。

D. 協助資訊安全教育訓練資料彙整。

3. 內部稽核小組

(1) 成員：由本府政風處指派人員擔任組長，組員由組長指派適當人員擔任。

(2) 職責 ：

A. 訂定相關之稽核計畫、執行稽核作業。

B. 稽核資訊安全業務。

C. 提出稽核報告及相關建議事項。

D. 複查稽核報告不符合事項之矯正措施。

(三) 人員能力需求

1. 資訊安全管理委員會各小組成員能力需求說明如下表：

角色	成員能力需求
召集人、副召集人	具備管理專長之高階主管。
執行秘書	具備資通訊或管理專長之主管。
資安委員	本府各單位及所屬機關各選一名代表。

角色	成員能力需求
資訊安全處理小組	依成員角色需求不同，熟悉領域知識，如： 一、ISO 27001 LA。 二、需了解資安風險評鑑方法。 三、網路管理能力，如：防火牆、路由器、交換器、防毒、防駭能力。 四、核心網路管理能力。 五、軟體開發管理能力。 小組成員應至少具備以上一種條件
資通安全專職人員	資通安全專職(責)人員至少應取得 1 張資通安全專業證照及資通安全職能評量證書
文件管制小組	不限制。
內部稽核小組	一、接受至少 3 小時以上之 ISO 27001 標準介紹訓練課程。 二、接受至少 3 小時以上之稽核工作內容訓練課程。 三、參加至少 1 天以上之資訊安全稽核見習。 四、現職政風處人員。 小組成員應至少具備以上一種條件

2. 文件管制小組負責收集人員能力相關資料以備查驗。(人員能力相關資料可以為上課/受訓證明、證書、過往工作經歷、工作導師指導紀錄...等)。

參、附則

一、參考文件

(一) 資訊安全管理政策(ISMS-1-01-00)。

(二) 資訊安全實施程序書(ISMS-2-02-00)。

(三) 資通安全管理法及相關子法。

二、相關表單

(一) 資訊安全組織名冊(ISMS-2-01-01)。

三、制訂與公告

參照「文件與紀錄管理程序書(ISMS-2-03-00)」相關規定。