臺北市政府

資通安全維護計畫

中華民國108年4月

目　　錄

壹、 依據及目的

本計畫依據下列法規訂定：

一、 資通安全管理法第10條及其施行細則第6條。

二、 臺北市政府資訊安全管理規範。

貳、 適用範圍

本計畫適用範圍涵蓋臺北市政府所屬機關、學校 (以下簡稱各機關)，所屬機關計144個，學校計250所(含14所幼兒園)，其清單詳附件1。

參、 業務(資通)系統及重要性評估

各機關之業務(含資通)系統及重要性，詳如附件2。

肆、 資通安全政策及目標

一、 資通安全政策

為使本府業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），並依「臺北市政府資訊安全管理規範」為辦理本府資通安全作業參考依據，供全體同仁共同遵循：

1. 應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 應強固核心資通系統之韌性，確保機關業務持續營運。
4. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高同仁之資通安全意識，各機關同仁亦應確實參與訓練。
5. 針對辦理資通安全業務有功人員應進行獎勵。

6. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。

7. 禁止多人共用單一資通系統帳號。

8. 配合稽核活動及持續改善精進資訊安全管理。

二、 資通安全目標

(一) 各機關量化型目標

1. 發生「資通安全事件通報及應變辦法」所定義之3級以上資訊安全事件，每年不得高於一次。

2. 依「資通安全責任等級分級辦法」之附表九「資通系統防護需求分級原則」所評鑑之防護需求等級「高」之系統可用性每年(365天*24小時)達99%。

3. 與民眾相關之服務與系統可用性每年(365天*24小時)達97.5%。

(二) 各機關質化型目標：

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。

3. 提升人員資安防護意識、有效偵測與預防外部攻擊等。

三、 資通安全政策及目標之核定程序

本府資安政策目標由機關首長核定，各機關配合辦理。

四、 資通安全政策及目標之宣導

1. 各機關之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。

2. 各機關應每年向利害關係人(例如 IT 服務供應商、與機關連線作業有關單位)進行資安政策及目標宣導，並檢視執行成效。

五、 資通安全政策及目標定期檢討程序

本府資安政策目標由本府資訊局定期檢討修訂，各機關配合辦理。

伍、 資通安全推動組織

一、 資通安全長

依本法第11條之規定，各機關設置資通安全長並簽陳機關首長核可，負責督導各機關之資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。

2. 資通安全責任之分配及協調。

3. 資通安全資源分配。

4. 資通安全防護措施之監督。

5. 資通安全事件之檢討及監督。

6. 資通安全相關規章與程序、制度文件核定。

7. 資通安全管理年度工作計畫之核定

8. 資通安全相關工作事項督導及績效管理。

9. 其他資通安全事項之核定。

二、 資通安全推動組織及分工

(一) 組織

各機關組織與任務依「臺北市政府資訊安全管理規範」貳、資訊安全組織規定辦理。

各機關之資訊安全推行小組依分工進行責任分組，並依其資通安全長之指示分派業務，各機關資訊安全推行小組分組人員名單及職掌應列冊，詳如附件3，並適時更新之。

陸、 專職(責)人力及經費配置

一、 專職(責)人力及資源之配置

1. 各機關依資通安全責任等級分級辦法之規定，設置資通安全專職(責)人員詳如附件1，其負責業務如下：

(1) 資通安全管理面業務，負責推動資通系統防護需求分級、資通安全管理系統導入及驗證、內部資通安全稽核、機關資安治理成熟度評估及教育訓練等業務之推動。

(2) 資通系統安全管理業務，負責資通系統分級及防護基準、安

全性檢測、業務持續運作演練等業務之推動。

(3) 資通安全防護業務，負責資通安全監控管理機制、政府組態基準導入，資通安全防護設施建置及資通安全事件通報及應變業務之推動。

(4) 資通安全管理法法遵事項業務，負責對所屬公務機關或所管特定非公務機關之法遵義務執行事宜。

2. 各機關之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。各機關之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

3. 資安專職(責)人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定持有資通安全專業證照或資通安全職能評量證書。

4. 各機關負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽署書面約定，並視需要實施人員輪調，建立人力備援制度。

5. 各機關之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

6. 專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

二、 經費之配置

1. 各機關之資訊安全推行小組於規劃配置相關經費及資源時，應考量各機關之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

2. 各機關於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。

3. 各機關如有資通安全資源之需求，應配合機關預算規劃期程向各機關之資訊安全推行小組提出，由資訊安全推行小組視整體資通安全資源進行分配，並經其資通安全長核定後，進行相關

之建置。

4. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

柒、 資訊及資通系統之盤點

一、 資訊及資通系統盤點

1. 各機關每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為資訊資產、軟體資產、實體資產、支援服務資產等。

2. 資訊及資通系統資產項目如下：

   (1) 資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。

   (2) 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。

   (3) 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。

   (4) 支援服務資產：相關基礎設施級其他機關內部之支援服務，如電力、消防等。

3. 各機關每年度應依資訊及資通系統盤點結果，製作「資訊及資通系統資產清冊」等相關文件，欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級。資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。核心資通系統及相關資產，並應加註標示。

4. 各機關管理之資訊或資通系統如有異動，應即時通知資訊安全推行小組更新資產清冊。

二、 機關資通安全責任等級分級

依資通安全責任等級分級辦法之規定，各機關之資通安全責任等級詳如附件1。

捌、 資通安全風險評估

一、 資通安全風險評估

1. 各機關應每年針對資訊及資通系統資產進行風險評估。

2. 各機關爰引用風險管理策略基準法，參考「臺北市政府資訊安全管理規範」及「資通安全責任等級分辦法」之附表九「資通系統防護需求分級原則」、附表十「資通系統防護基準」，實施相對應之資訊安全控制措施。

3. 各機關應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外開發之資通系統防護需求分級。

二、 核心資通系統及最大可容忍中斷時間

各機關核心系統及最大可容忍中斷時間，詳如附件2

玖、 資通安全防護及控制措施

各機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施如下:

一、 資訊及資通系統之管理

各機關依「臺北市政府資訊安全管理規範」伍、資訊系統作業安全管理規定辦理。

二、 存取控制與加密機制管理

各機關依「臺北市政府資訊安全管理規範」陸、網路安全管理及柒、系統存取控制規定辦理。

三、 作業與通訊安全管理

各機關依「臺北市政府資訊安全管理規範」肆、實體與環境安全及伍、資訊系統作業安全管理規定辦理。

四、 系統獲取、開發及維護

各機關依「臺北市政府資訊安全管理規範」捌、系統發展與維護安全管理規定辦理。

五、 業務持續運作演練

各機關依「臺北市政府資訊安全管理規範」壹拾壹、業務持續運作管理規定辦理。

六、 執行資通安全健診

各機關辦理資通安全健診，其項目與頻次應依其資通安全責任等級分級辦法規定辦理，並檢討執行情形。

七、 資通安全防護設備

1. 各機關應依資通安全責任等級分級辦法規定辦理，建置相關資通安全防護設備，持續使用並適時進行軟、硬體之必要更新或升級。

2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

壹拾、 資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，各機關應訂定資通安全事件通報、應變及演練相關機制，詳資通安全事件通報應變程序與「臺北市政府資訊安全管理規範」-壹拾、資訊安全事件之管理規定。

壹拾壹、 資通安全情資之評估及因應

各機關接獲資通安全情資，應評估該情資之內容，並視其對各機關之影響、各機關可接受之風險及各機關之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、 資通安全情資之分類評估

各機關接受資通安全情資後，應指定資通安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏

洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(二) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

(三) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(四) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

二、 資通安全情資之因應措施

各機關於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一) 資通安全相關之訊息情資

各機關由資訊安全推行小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(二) 入侵攻擊情資

由資通安全專職(責)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三) 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

(四) 涉及核心業務、核心資通系統之情資

資訊安全推行小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

壹拾貳、 資通系統或服務委外辦理之管理

各機關委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

一、 選任受託者應注意事項

1. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

2. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

3. 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

4. 受託業務涉及國家機密者，應考量受託業務所涉及國家機密之機密等級內容，於招標公告、招標文件及契約中，註明受託者辦理該項業務人員及可能接觸該國家機密人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

5. 前點適任性查核得在必要範圍內就下列事項查核，查核前應經當事人書面同意：

(1) 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案者。

(2) 曾任公務人員因違反相關安全保密規定，受懲戒處分、記過以上行政懲處者。

(3) 曾受到外國政府、大陸地區或香港、澳門官方之利誘、脅迫，從事不利國家安全或重大利益情事者。

(4) 其他與國家機密保護相關之具體項目。

二、 監督受託者資通安全維護情形應注意事項

1. 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

2. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

3. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。

4. 受託者應採取之其他資通安全相關維護措施。

5. 各機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

壹拾參、 資通安全教育訓練

一、 資通安全教育訓練要求

各機關辦理資通安全教育訓練，其項目與頻次應依其資通安全責任等級分級辦法規定辦理。

二、 資通安全教育訓練辦理方式

1. 各機關承辦單位應於考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

2. 各機關資通安全認知宣導及教育訓練之內容得包含：

(1) 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。

(2) 資通安全法令規定。

(3) 資通安全作業內容。

(4) 資通安全技術訓練。

3. 員工報到時，應使其充分瞭解各機關資通安全相關作業規範及其重要性。

4. 資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

壹拾肆、 公務機關所屬人員辦理業務涉及資通安全事項之考核機制

各機關所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法及「臺北市政府資訊安全管理規範」等相關規定辦理之。

壹拾伍、 資通安全維護計畫及實施情形之持續精進及績效管理機制

一、資通安全維護計畫之實施

為落實本安全維護計畫，使各機關之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本府資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、資通安全維護計畫實施情形之稽核機制

(一) 稽核機制之實施

1. 各機關稽核機制之實施依「臺北市政府及所屬各機關辦理資訊使用管理稽核作業規定」辦理。

2. 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

3. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼）。

(二) 稽核改善報告

1. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

2. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生

之原因，並評估是否有其類似之缺失或待改善之項目存在。

3. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。

4. 機關應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

5. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

三、資通安全維護計畫之持續精進及績效管理

1. 各機關之資訊安全推行小組應召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

2. 管理審查議題應包含下列討論事項：

(1) 過往管理審查議案之處理狀態。

(2) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資訊安全推行小組決議事項等。

(3) 資通安全維護計畫內容之適切性。

(4) 資通安全績效之回饋，包括：

A. 資通安全政策及目標之實施情形。

B. 資通安全人力及資源之配置之實施情形。

C. 資通安全防護及控制措施之實施情形。

D. 內外部稽核結果。

E. 不符合項目及矯正措施。

(5) 風險評鑑結果及風險處理計畫執行進度。

(6) 重大資通安全事件之處理及改善情形。

(7) 利害關係人之回饋。

(8) 持續改善之機會。

3. 持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾陸、 資通安全維護計畫實施情形之提出

各機關依據資通安全管理法第11(16, 17)條之規定，應向其上級或監督機關，提出資通安全維護計畫實施情形，使其得瞭解各機關之年度資通安全計畫實施情形。

壹拾柒、 參考表單

1. 附件1、臺北市政府各機關、責任等級及專職(責)人員設置表
2. 附件2、臺北市政府各機關核心業務(非核心業務)及重要性列表
3. 附件3、臺北市政府各機關資訊安全推行小組成員列表
4. 臺北市政府資訊安全管理規範
5. 臺北市政府及所屬各機關辦理資訊使用管理稽核作業規定