臺北市政府
資通安全維護計畫

中華民國114年5月

目　　錄

壹、 依據

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、臺北市政府資通安全管理規定。

貳、 適用範圍

本計畫適用範圍如下（以下簡稱各機關）:

一、依本府組織自治條例第六條至第八條設置之局、處、委員會、區公所，以及所屬次級機關、機構、及學校。

二、本府依自治條例設置之行政法人。

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，詳如各機關於數位發展部資通安全署資通安全作業管考系統（https://spm.nat.gov.tw/，以下簡稱管考系統）填報之機關資通系統與服務資產清冊。

肆、 資通安全政策及目標

一、依「臺北市政府資通安全管理規定」壹、總則各規定辦理。

二、各機關目標：

(一) 量化型目標：

1. 知悉資安事件發生後於規定之時間完成通報、應變及復原作業。

2. 每年社交工程信件演練至少辦理2次、資通安全事件通報及應變演練至少辦理1次。

(二) 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。

伍、 資通安全推動組織

依「臺北市政府資通安全管理規定」貳、資通安全組織各規定辦理。

陸、 專職（責）人力及經費配置

一、專職（責）人力及資源之配置

(一) 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）人員或資通安全業務窗口（詳如國家資通安全通報應變網站（https://www.ncert.nat.gov.tw/）之機關資安人員資料)，其負責業務如下：

1. 資通安全管理面業務，負責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、業務持續運作演練、資安治理成熟度評估等業務之推動。

2. 資通安全技術面業務，負責核心資通系統安全性檢測、資通安全健診、資通安全威脅偵測管理機制、政府組態基準導入、資通安全弱點通報機制、端點偵測及應變機制、資通安全防護等業務之推動。

3. 資通安全認知與訓練面業務，負責資通安全教育訓練業務之推動。

4. 資通安全管理法及其子法法遵事項業務，負責對所屬或監督機關之法遵義務執行事宜。

(二) 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職（責）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。

(三) 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。

(四) 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。

(五) 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。

(六) 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

(一) 各機關之資通安全專職（責）人員或資通安全業務窗口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、資通安全責任等級，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。

(二) 各機關於規劃資通系統建置時，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。

(三) 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通安全專職（責）人員或資通安全業務窗口提出，由資通安全專職（責）人員或資通安全業務窗口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。

(四) 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

(一) 依「臺北市政府資通訊資產及電子資料安全作業指引」及「臺北市政府使用物聯網安全作業指引」各規定辦理。

(二) 各機關每年度應依資訊及資通系統盤點結果，落實填報管考系統。

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」之規定辦理，各機關之資通安全責任等級應先提報本府審核，並由本府提交主管機關核定。

捌、 資通安全風險評估

一、資通安全風險評估

依「臺北市政府資通訊資產及電子資料安全作業指引」各規定辦理。

二、核心資通系統及最大可容忍中斷時間

各機關應訂定核心資通系統及其最大可容忍中斷時間，詳如各機關於管考系統填報之資通系統與服務資產清冊。

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、系統獲取、開發及維護

依「臺北市政府資通系統安全作業指引」、「臺北市政府資通訊資產及電子資料安全作業指引」、「臺北市政府資通訊業務委外作業指引」及「臺北市政府目錄服務管理要點」規定及相關程序辦理。

二、存取控制與加密機制管理

依「臺北市政府資通安全單一識別碼管理要點」及「臺北市政府資通系統安全作業指引」規定及相關程序辦理。

三、作業與通訊安全管理

依「臺北市政府網路管理規範」、「臺北市政府資通系統安全作業指引」及「臺北市政府員工使用資通訊裝置應注意事項」規定及相關程序辦理。

四、業務持續運作演練

依「臺北市政府資通安全管理規定」拾壹、業務持續運作管理規定及相關程序辦理。

五、執行資通安全技術性安全檢測

各機關應配合本府依各機關資通安全責任等級辦理之資通安全相關檢測，並依檢測結果檢討改善。

六、資通安全防護設備

網路安全防護應依「臺北市政府網路管理規範」辦理，端點安全（包含防毒、沙箱與端點偵測及回應）應使用本府提供之軟體與管理規範辦理。

壹拾、 資通安全事件通報、應變及演練相關機制

依「臺北市政府資通安全事件通報及應變作業程序」及「臺北市政府資通安全管理規定」拾、資通安全事件通報應變、演練及情資分享規定辦理。

壹拾壹、 資通安全情資之評估及因應

依「臺北市政府資通安全事件通報及應變作業程序」與「臺北市政府資通安全管理規定」拾、資通安全事件通報應變、演練及情資分享規定辦理。

壹拾貳、 資通系統或服務委外辦理之管理

依「臺北市政府資通訊業務委外作業指引」及「臺北市政府資通安全管理規定」玖、受託業務之資通安全管理規定辦理。

壹拾參、 資通安全教育訓練

依「臺北市政府資通安全管理規定」參、人員安全及教育

訓練規定辦理。

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」、「臺北市政府所屬人員資通安全事項獎懲基準」、「臺北市政府資訊專業人員獎懲標準表」及「臺北市政府資通安全管理規定」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，各機關執行資通安全管理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

本府每年度依「臺北市政府資通安全管理規定」拾貳、資通安全稽核作業及「臺北市政府所屬各機關辦理資訊使用管理稽核作業規定」訂定稽核計畫，各機關應依該計畫訂定內部稽核計畫，本府資訊局會同政風處等相關單位每年對本府特定比例之機關進行府級稽核。

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12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、 相關法規、程序及表單

為使本府資通安全管理有效運作，各機關應依相關文件、流程、程序或控制措施確實執行，並應保存相關之執行紀錄；如各機關已有資通安全管理系統之文件，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。

一、相關法規

(一) 臺北市政府資通安全管理規定

(二) 臺北市政府所屬各機關辦理資訊使用管理稽核作業規定

(三) 臺北市政府員工使用資通訊裝置應注意事項

(四) 臺北市政府網路管理規範

(五) 臺北市政府資通訊業務委外作業指引

(六) 臺北市政府使用物聯網安全作業指引

(七) 臺北市政府資通系統安全作業指引

(八) 臺北市政府資通訊資產及電子資料安全作業指引

(九) 臺北市政府資通安全事件通報及應變作業程序

(十) 臺北市政府所屬人員資通安全事項獎懲基準

(十一)臺北市政府資訊專業人員獎懲標準表

(十二)臺北市政府目錄服務管理要點

(十三)臺北市政府資通安全單一識別碼管理要點