臺北市政府網路管理規範

中華民國110年1月21日臺北市政府(110)府授資設字第1103003104號函訂定全文三十一點，自函頒日生效

壹、總則

一、臺北市政府（以下簡稱本府）為有效運用本府網路資源，正確且合理使用網路，明確網路使用準則及維護資訊機密與安全，特訂定本規範。

貳、網路管理組織及權責

二、本府市政骨幹網路由臺北市政府資訊局（以下簡稱資訊局）統籌負責網路架構規劃、建置、維護管理及網路安全等事宜。

三、本府各機關（構）（以下簡稱各機關）應由專責單位統一管理規劃及整合內部網路，並協助網路管理單位進行網路管理（包含機關內所有IP及連網設備進行造冊、核准連線、下架、禁用等）。

四、各機關原則應以本府市政骨幹網路對外服務及存取外部資源，不得未經申請自行申裝連外網路；如因業務需要而有申裝必要者，應向資訊局提出申請，並說明網路安全管理及管控架構等規劃，經同意後始得安裝。

五、各機關不得私自向 GSN申請開放中國大陸連接本府市政網路，如有業務需要應向資訊局申請開放。

參、網路位址配置原則

六、各機關在部署完成網路規劃後，應繪製機關邏輯網路架構圖及實體網路架構圖，並訂定網路檢核表檢測部署狀況及運作狀況。

七、各機關對外服務網路位址通訊協定（IP）應同時支援第四版及第六版，並應定期盤點所有配發網路位址。

肆、網路設備及服務管理原則

八、重要服務之網路線路及設備，應有備援或容錯機制，避免單點失效，並應依資訊局訂定之相關安全基準，定期稽核。

九、網路設備應擺設於安全防護區域內，以避免遭受非授權人員進行實體上之接觸或存取；設備管理介面之網路應隔離。

伍、網路分區設計原則

十、無線網路、民眾上網或遠端 VPN等網段，應與辦公室、內部伺服器及網路設施等進行網路分區設計；內部伺服器及網路設施應依正式區或測試區等進行細部分區設計。

陸、網路互連原則

十一、各機關因業務需要連結本府市政骨幹網路者，應向資訊局申請連線使用，並依資訊局網路位址配置規劃辦理。

十二、各機關網路互連應以防火牆區隔，並依互連需求最小開放連線政策。

柒、無線網路管理原則

十三、各機關不得自行架設無線網路設備，如因業務需要而有架設必要者，應向資訊局提出申請，經同意後始得架設。

十四、各機關申請自行架設無線網路設備應向資訊局提報清單，其內容應至少包含以下資料：

（一）無線AP之管理IP位址。
（二）無線AP之配置使用者IP位址範圍。
（三）無線AP之SSID。
（四）無線網路連線架構、網段及是否可存取內部網路等。
（五）設備之製造商、型號及序號等資訊。
（六）設備安裝實體位置。
（七）設備管理者之相關資訊，如人員姓名、分機號碼等。
（八）設備韌體版本。

十五、自行架設無線網路設備之機關應定期盤點前點各款資料及管理帳號清單、近期登入紀錄與密碼變更時間等，並應依資訊局訂定之相關安全基準定期稽核。

捌、防火牆管理原則

十六、防火牆政策規則應符合本府公告之防火牆開放原則及相關安全檢核規則，來源位址、目的位址、通訊埠及使用期限等應採最小開放原則，並明確說明開通事由。

十七、防火牆政策規則應由來源位址或目的位址之權管機關申請，如有影響他機關服務者，應於該機關審核同意後，始得申請開通。

十八、防火牆每年應至少進行一次全面性政策及預設政策盤點。

十九、防火牆管理員應定期檢視防火牆政策，檢測防火牆政策規則是否妥善控管或未使用；如未妥善控管或未使用，經防火牆管理員通知申請單位或受影響之機關而逾期仍未處理者，管理單位有權停用或刪除該規則。

二十、各機關防火牆之管理活動，如管理者帳號登入、登出或網路連線進出規則變更等，應留存稽核紀錄（ log）；通過防火牆之網路連線亦應留存目的與來源IP位址、通訊埠等連線稽核紀錄（ log）。上述紀錄之留存期間至少一年，如法規另外規定外不在此限，並應異機備份保存妥善保護，防止未經授權之存取、竄改與刪除。

玖、遠端連線作業原則

二十一、因應本府政策或作業需要，須與本府網路資源進行遠端連線者，其遠端連線作業原則應使用虛擬私有網路（ VPN），並應採用符合本府所定之基本安全原則之設備。

二十二、使用虛擬私有網路（ VPN）應遵循提供服務機關之規定，來源位址、目的位址、通訊埠及使用期限等應採最小開放原則；如未妥善使用或未使用，經網路管理員通知而逾期仍未處理者，管理單位有權停用或限制使用權限及範圍。

拾、各機關網路安全管理原則

二十三、各機關應依機關資通安全責任等級及風險評估情形，建立防火牆、入侵偵測及防禦、應用程式防火牆、進階持續性威脅攻擊防禦措施等網路安全防護措施，針對內外網網路威脅進行偵測與防護及依機關安全需求針對連線存取設施進行存取控管機制，並納入資通安全威脅偵測管理機制，持續監控及調查處理。

二十四、各機關應定期針對網路架構、網路惡意活動、防火牆政策等進行資通安全健診；網路設備組態應導入政府組態基準（ GCB）及資訊局訂定之安全基準。

二十五、依各機關對危害國家資通安全產品限制使用原則，屬資通安全管理法主管機關或本府公告有資通安全疑慮之產品，應禁止使用；如有該類產品，亦不得與公務網路環境介接。

二十六、各機關針對有資通安全疑慮、非公務用途或大量耗用頻寬之連線行為應阻斷、限制及監控清查連線，並應依資通安全管理法主管機關或資訊局提供之惡意中繼站或網域等資通安全情資，進行阻斷、清查、監控及確認。

拾壹、其他規定

二十七、各機關應尊重網路隱私權，不得利用其網路管理權限任意窺視使用者之個人資料或有其他侵犯隱私權之行為。但有下列情形之一者，得不經通知逕行就所屬IP位址執行網路掃描及監測活動，並將掃描及監測異常結果通知該單位：

（一）為維護或檢查系統安全，以因應網路安全事件、網路病毒或蠕蟲大量傳播。

（二）依合理之依據，懷疑有違反本規範之情事時，為取得證據或調查不當行為。

（三）為配合司法機關之調查。

（四）其他依法令之行為。

二十八、違反本規範或有資通安全相關威脅者，本府得立即停止其網路使用權，並視情節輕重處以停權一個月、限制或撤銷其網路資源存取權，同時依相關法令處理。觸犯法令者，須自負相關責任。

二十九、各機關使用網路資源應依臺北市政府資通安全管理規定辦理；如有違反，依相關規定議處。

拾貳、附則

三十、各機關得依業務需要，自行訂定其他執行管理規範，並依機關流程簽核發布。

三十一、本規範之內容，應由資訊局每年至少辦理檢視及整理一次，以符合相關法令、技術、組織及營運之最新發展現況。

於資通安全之客觀環境發生重大變動，本規範之內容有不能因應之虞時，資訊局應即時辦理檢視及整理。