法規名稱：臺北市政府資通安全管理規定

修正日期：民國 111 年 07 月 13 日

當次沿革：中華民國 111 年 7 月 13 日臺北市政府（111）府授資安字第 1113008933 號函修正全文 36 點；並自函頒日生效

壹、總則

一、臺北市政府（以下簡稱本府）為強化所屬各機關（構）及受監督行政法人（以下簡稱各機關）資通安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備、網路安全及人員安全，降低因人為疏失、蓄意或天然災害等導致之資通訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，特訂定本規定。

二、本府資通安全政策之目的、目標及責任如下：

（一）資通安全政策之目的：各機關應確保執行業務時，資訊之機密性、完整性、可用性及法律遵循性。

1. 機密性：確保經授權之人員始得使用資訊。

2. 完整性：確保資訊之準確性及可靠性。

3. 可用性：確保被授權之人員能取得所需資訊。

4. 法律遵循性：確實遵循資通系統設置或運作涉及之資通安全相關法令。

（二）資通安全政策之目標：

1. 每年各機關應達成資通安全責任等級分級辦法之要求，並降低資通安全風險之威脅。

2. 強化受託者之選任、監督、管理，確保委外辦理資通系統建置、維運或資通服務提供（以下簡稱受託業務）之資通安全

。

3.提升資安防護意識、有效偵測及預防外部攻擊等。

（三）資通安全政策之責任：各機關所有人員，包含機關組織編制表內人員及接觸或使用機關資通系統服務之各類人員，應充分了解本府資通安全政策之目的、目標，並遵守資通安全管理相關規定。

貳、資通安全組織

三、本府資通安全委員會：

（一）由市長指派副市長或適當人員兼任本府資通安全長，臺北市政府資訊局（以下簡稱資訊局）局長為本府副資通安全長，負責推動、協調及監督府內資通安全相關事務。

（二）各一級機關之資通安全長為委員。

（三）每半年召開一次資通安全會議，並得視需要邀請專家學者、非委員之各機關資通安全長或相關資訊人員與會。

四、各機關資通安全推動組織：

（一）資通安全長：依資通安全管理法第十一條規定，各機關應置資通安全長，負責督導、協調及分配機關之資通安全相關事項。

（二）資通安全專職人員：各機關應依資通安全責任等級分級辦法規定，置專職人員，負責執行機關資通安全業務。

（三）資通安全業務窗口：依資通安全責任等級分級辦法規定無須置專職人員之機關，仍應指派適當人員擔任資通安全業務窗口，負責機關之資通安全事件通報等各項資通安全業務。

（四）各機關得視需要由資訊單位主管成立跨單位資通安全推動小組，負責推動機關資通安全作業。

（五）各機關應依其資通安全責任等級，定期或視需要召開資通安全管理會議，檢視當年度各單位相關辦理情形，並作為次年度持續精進之依據。

（六）各機關之資訊機密維護及稽核使用管理事項，由機關負責稽核業務單位會同相關單位負責辦理，或由機關首長指定適當單位及人員負責辦理。

參、人員安全及教育訓練

五、人員安全管理：

（一）各機關對職務及工作，應進行安全評估，並於指派工作及任務時，審慎評估人員之適任性，及進行必要之考核。對於可存取機密性及敏感性資訊或系統之人員，及因工作需要配賦資訊或系統特別權限之人員，應加強評估及考核。

（二）各機關針對管理、業務及資訊等不同工作類別之人員，應妥適分工，分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。

（三）各機關人員均應遵守維護公務機密之相關法令規定；在職及離退職後，均不得洩漏所知悉之公務機密，或為不當之使用。

（四）各機關應依本府所定資通安全宣導單範本自訂宣導單，並於新進人員報到時說明宣導資通安全相關規定；新進人員應簽章以示知悉。

（五）機關人員請假、暫離職務或帳號、網路位址等相關資通訊資源超過九十日未使用，機關應停用帳號或權限。

（六）機關人員離退職時，機關應適時取消或調整資訊或系統之各項權限。

（七）各機關人員應遵循臺北市政府員工使用資通訊裝置應注意事項及資通安全管理相關規定。

六、資通安全認知及訓練：

（一）各機關應每年透過教育訓練、內部會議、張貼公告等方式，針對管理、業務及資訊等不同工作類別之人員進行安全宣導，並定期進行考核，以建立人員資通安全認知，提升人員資通安全水準。

（二）各機關應依資通安全責任等級，每年度完成資通安全專職人員、資通安全專職人員以外之資訊人員、一般使用者及主管之教育訓練；各機關資通安全專職人員並應完成資通安全專業證照及職能訓練證書之要求。

肆、資通訊資產及電子資料安全

七、資通訊資產及電子資料安全應依臺北市政府資通訊資產及電子資料安全作業指引規定辦理。

八、物聯網設備應依臺北市政府使用物聯網安全作業指引規定辦理。

伍、系統發展及維護安全

九、系統發展及維護安全應依臺北市政府資通系統安全作業指引規定辦理。

陸、實體及環境安全

十、實體及環境應定期整理（整理工作區域）、整頓（物品確實定位，明確標示）、清掃（保持整潔）；各機關應訂定標準規範且持續落實，並以人員健康與安全為優先目標，設置相關防護措施。

十一、辦公處所及機房實體區隔：

（一）應使用安全周界，如圍牆、入口閘門或人員駐守之接待櫃檯等或藉由適當之入口控制措施加以保護，確保經授權人員始得進出。

（二）設計辦公室、隔間及設施之實體安全措施時，應考慮火災、水災及其他形式自然或人為之災害所造成損失之可能性。

十二、設備安全如下列說明：

（一）設備應安置於適當地點並予以保護，以減少環境不安全所引發之危險及未經授權存取系統之機會。

（二）設備之電源使用應依製造廠商提供規格設置，並應防止斷電或電力不正常導致之損害。

（三）重要設備得考量使用不斷電系統（ UPS），並應定期維護及測試。

（四）電力及通信用之電纜線，應予適當之保護，以防止被破壞或

資料被截取。

（五）重要設備應妥善維護，以確保設備之完整性及可以持續使用。

（六）設置在外部以支援業務運作之資通訊設備，應同樣遵守資通安全管理相關規定，維持與內部資通訊設備相同之安全水準；內、外部區分應以單位或機關之主要辦公處所為準。

（七）設備應由專人負責保管並定期維護保養，以確保設備之完整性及可以持續使用。

十三、機房管理：

（一）機房應設置以下措施及設備：

1. 門禁管制措施：應記錄進出日期、時間、區域及身分，並定期檢視比對監視錄影進出人員是否有未經授權之行為。

2. 合理之照明設備及緊急照明設備。

3. 監視錄影設備：應定期校時。

4. 滅火設備、警報設備、避難逃生設備及防火、空調設備。

（二）應備有掃毒設備，供可攜式儲存媒體檔案交換前進行掃毒。

（三）支援或維護服務人員應由機關承辦同仁陪同並經登記後，始得進出管制區域。

（四）設備進機房前應評估電力、實體空間、機櫃負重及空調等是否足夠。

（五）機房機櫃應依網路需求佈署，機房內各項設備除正常作業外，非經核准，不得任意變動，以免影響正常運作。

（六）機房內不得攜入或存放磁性、放射性、易燃性及易爆性物品，且嚴禁嬉戲、吸菸及飲食，非經核准不得攝影，並應定期

維護及清潔（含高架地板下）。

（七）各機關自建機房（含資料中心、雲端資料中心及通訊機房）者，應依本點規定訂定管理規範。

柒、網路安全

十四、網路安全應依臺北市政府網路管理規範規定辦理。

捌、通訊安全

十五、通訊安全應依臺北市政府員工使用資通訊裝置應注意事項規定辦理。

玖、受託業務之資通安全管理

十六、各機關於選任及監督受託業務之受託者時，應依資通安全管理法施行細則第四條規定辦理相關事項。

十七、受託業務之資通安全管理應依臺北市政府資通訊業務委外作業指引辦理。

十八、各機關辦理含資通服務或以資通系統輔助規劃或執行之活動，且為該活動之主辦單位或承辦單位者，應依臺北市政府資通訊業務委外作業指引辦理。

各機關為前項活動之指導單位、協辦單位或合辦單位，並協助資通系統或資通服務部署、介接或其他技術支援者，準用前項規定。

拾、資通安全事件通報應變、演練及情資分享

十九、資通安全事件通報應變、演練及情資分享應依資通安全事件通報及應變辦法、資通安全情資分享辦法及臺北市政府資通安全事件通報及應變作業指引規定辦理。

二十、各機關應將所接收之本府及外部情資分享納入資通安全防護及資通安全威脅偵測管理機制，進行防護及監控，並作必要之預防性處置。

二十一、各機關應定期自行辦理社交工程演練與資通安全事件通報及應變演練等演練工作，並視需要辦理網路攻防實兵演練，確保相關人員熟悉各項通報、調查及處理流程。另應配合資通安全管理法主管機關及本府之演練作業。

二十二、社交工程年度演練基準，依臺北市政府資安事件通報及應變管理程序規定辦理。

二十三、各機關於資通事件處置過程，得要求相關資通系統及設備針對違

規、有高風險、異常之 IP、裝置及帳號權限等進行停用、中斷服務或降權等措施。

前項違規、高風險、異常等情形，如屬使用者故意行為或無正當理由拒絕相關處置而導致者，得依相關規定懲處。

拾壹、業務持續運作管理

二十四、各機關應視組織業務目的，建立營運持續管理計畫（包含關鍵核心業務及流程），透過定期演練，避免關鍵性業務中斷造成營運衝擊。相關執行紀錄及後續檢討改善應予以文件化，並管考追蹤。

二十五、業務持續運作演練之腳本應以各機關提供之服務為導向，相關機關及利害關係人均應參與演練，並納入歷次發生服務嚴重中斷案例、有單點失效問題、重大災害應變等嚴重影響業務持續運作之情境，並得配合資通安全事件通報及應變進行整合演練。

二十六、各機關核心資通系統應落實服務之備份備援機制（包含人員、環境、設備、程式碼、組態、資料庫資料與文件檔案等），並確保於災害發生時得於業務營運可接受之時間內恢復至可接受之營運水準，且應定期檢視相關機制是否支援上開恢復時間及營運水準。

拾貳、資通安全稽核作業

二十七、資通安全稽核作業應依資通安全管理法第十三條規定辦理。

二十八、上級機關應負監督之義務，定期審查受稽核單位缺失或待改善項目之改善措施、進度規劃及佐證資料，並留存相關執行紀錄。

二十九、為提升資通安全稽核作業之效率，本府得建置資通安全稽核人員資料庫，並針對人員之技術面與管理及認知訓練面向辦理專才註記。稽核人員得為公務機關代表或專家學者，須具備資通安全政策或特定稽核任務所需之技術、管理、法律或實務專業知識。

本府及各機關辦理資通安全稽核作業時，得自資通安全稽核人員資料庫聘請稽核人員擔任稽核委員。

第一項資料庫應由本府定期更新。

三十、為鼓勵同仁參與稽核作業，各機關得依同仁擔任稽核委員之工作難度、量度及貢獻度等情形，綜合考量覈實敘獎。

三十一、為持續培養本府之資通安全稽核人才，及提升資通安全稽核能量，各機關辦理稽核作業時，得邀請機關內部其他人員擔任觀察員，參與稽核作業。

拾參、資通安全業務考核與獎勵及懲處

三十二、資訊局應依臺北市政府所屬各機關資訊人力管理實施要點第六點規定辦理各機關資通安全業務考核。

三十三、各機關應依公務機關所屬人員資通安全事項獎懲辦法第三條及第四條規定，參酌臺北市政府資訊專業人員獎懲標準表之獎懲建議額度，辦理獎勵及懲處。

拾肆、附則

三十四、本規定簽奉本府資通安全長核定後實施，修訂時亦同。

三十五、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。

三十六、本規定之內容，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，本規定之內容有不能因應之虞時，資訊局應即時辦理檢視及整理。