臺北市政府資通系統安全作業指引

中華民國111年2月24日臺北市政府(111)府授資安字第1113003287號函訂定發布

壹、 總則

一、 臺北市政府(以下簡稱本府)為明定各機關(構)(以下簡稱各機關)開發或購置資通系統應遵守或符合之資通安全原則及標準,特參酌資通安全責任等級分級辦法，訂定本指引。

貳、 資通系統之安全需求

二、 本府各機關開發或購置之資通系統，應依符合下列安全需求：

（一） 機密性：

1. 資通系統傳輸應採用HTTPS(透過TLS 1.2以上等加密協定)協定,以確保機敏資料以密文方式傳輸。
2. 廠商應採用公開、國際認可之演算法,如AES對稱式加密演算法、RSA非對稱式演算法及SHA安全雜湊演算法等，不得使用自行創造之加密方式。
3. 軟體中採用密碼學演算法時,應使用該演算法目前支援之最大金鑰長度,如：AES 256 bits、RSA 2048 bits以上或SHA-512等，以減少被暴力破解密碼之可能及弱點。
4. 產生網站HTTPS使用之憑證,原則應採用政府伺服器數位憑證管理中心(GTLSCA)發行之憑證，且應於憑證效期到期前進行更換。資通系統如另行使用自行產生之加密金鑰，亦應於屆期前更換，維持有效。
5. 機敏資料存於資料庫或其他儲存媒體時,應採用對稱式或其他加密方式,將機敏資料加密成密文後儲存,並於須取得原文明文時解密還原,減少機敏資料因儲存媒體有其他存取管道而洩漏之風險。
6. 加密金鑰不得與加密資料存放於同一系統中,且應對加密金鑰之存取進行限制,或採用獨立之硬體安全模組,將金鑰保護於硬體晶片環境以避免被竊取,並應同時具備多種驗證類型(PIN碼等),對金鑰存取進行限制。
7. 參數設定或系統設定存放處，應限制存取或進行加密。

（二） 完整性：

1. 資通系統於伺服器端應具有防範SQL命令注入攻擊之措施,如使用參數化查詢之Prepared statements、Stored procedures或輸入驗證(Input Validation)等。
2. 網頁應用軟體於伺服器端應具有防範跨站腳本攻擊(Cross-Site Scripting ,XSS)之措施，如黑名單過濾跳脫特殊字元、白名單正規表示式驗證、輸出編碼等。

3. 資通系統應具有防範「跨站請求偽造」(Cross-Site Request Forgery, CSRF)攻擊之措施。
4. 網頁應用軟體如提供網頁重導或導向之功能，必須確認使用者輸入欲重導向之網頁，其值在合法白名單內，以避免被利用於重導向至惡意網頁。
5. 重要資料或紀錄應以安全雜湊演算法產生並留存雜湊值，後續可對資料或紀錄再次產生雜湊值並與原先結果進行比對，以確保資料未遭到異動竄改。
6. 資通系統於伺服器端應以正規表示式(Regular Expression)方式，檢查使用者輸入資料合法性。
7. 資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時針對該事件進行分析。
8. 資通系統應納入監控或資通安全威脅偵測管理機制(SOC)，以偵測攻擊和未授權之連線，並識別資通系統之未授權使用。
9. 資通系統之文件及原始碼應使用本府或各機關提供之原始碼管理平臺或指定交付方式，於每次異動均應提交並說明異動內容。

（三） 身分授權及存取控制：

1. 資通系統除公開區域外，均應進行身分驗證登入成功後，始得存取，並應檢查該使用者權限是否允許其存取該功能。使用者如存取非公開區域，檢查機制發現其尚未通過身分驗證時，應不允許其存取頁面並將其導向至首頁或登入頁面。
2. 資通系統內外部使用者身分驗證，均應與本府或各機關使用者驗證及管理機制整合。
3. 資通系統在建立連線前，應識別允許存取之特定來源，如 IP。
4. 資通系統重要交易行為，於執行前應再次確認獲得授權，含要求使用者再次進行身分驗證，以防堵攻擊者透過其他方式取得使用者身分憑證後，直接偽冒使用者執行重要交易行為。
5. 資通系統身分驗證或重要交易行為身分驗證得配合本府或各機關要求採用多重因素身分驗證(二種以上驗證類型)、行動身分識別(Fast IDentity Online，FIDO)等強制機制，除另有規定外，並應由本府或各機關提供所需之識別服務。
6. 身分驗證機制應符合以下要求：
   (1) 確實規範使用者密碼強度，密碼長度應十二個字元以上，包含英文大小寫、數字及特殊字元。
   (2) 密碼應每三個月至少更新一次，使用者應定期更換密碼，且至少不得與前三次使用過之密碼相同。
   (3) 密碼最短效期為一日，最長效期為九十日。
   (4) 具備帳號鎖定機制，帳號登入進行身分鑑別失敗達三次後，

至少十五分鐘內不允許該帳號繼續嘗試登入，必要時請評估鎖定來源 IP。

(5) 密碼重設機制：重新確認使用者身分時，應發送一次性及具有時效性令牌(Token，如使用簡訊驗證碼或 E-mail 連結)，檢查傳回令牌有效性後，始得允許使用者進行重設密碼動作。

(6) 密碼添加亂數(Salt)進行雜湊函式(HASH Function)處理後，分別儲存亂數及雜湊後密碼。

(7) 使用預設密碼登入系統時，應於登入後要求立即變更。

7. 資通系統有與其他外部系統或資料庫等連線之需求，不得將連線之身分驗證資訊(如：帳號、密碼等)寫於程式原始碼(source code)中，而應採用設定檔或於系統啟動時動態輸入之方式。身分驗證資訊如以參數方式留存於設定檔，應確認僅有執行該系統之作業系統帳號可以存取設定檔。
8. 身分鑑別相關資訊不以明文傳輸。
9. 身分鑑別及重要交易行為應採用圖形驗證碼(CAPTCHA)機制，以防範自動化程式反覆之登入嘗試或填充攻擊。
10. 資通系統應遮蔽在鑑別過程中之資訊(如：密碼等)，以防止未授權之使用者可能之窺探或使用。
11. 不應使用國民身分證統一編號等可識別個人之資料或電子郵件作為帳號名稱，亦不可使用弱密碼作為使用者預設密碼。
12. 應採用伺服端之集中過濾機制檢查使用者授權。
13. 軟體程序(process)及伺服器服務，應以一般使用者權限執行，不以系統管理員或最高權限。
14. 對使用者或角色，僅賦予所需要之最低權限。
15. 資通系統應明確定義於軟體中之使用角色及對應之權限，每位使用者可具備多重使用角色，一個使用角色亦得由一個以上使用者擔任。
16. 資通系統應確保僅有特定管理員權限得以特定電腦於特定網段，讀取存取控制列表。
17. 應設計廠商維護專用之使用角色，並授予執行伺服器服務及讀寫相關檔案之有限範圍權限，使其可以正常執行維護服務作業，並避免過高權限之風險。
18. 資通系統重要行為必要時得採取須通過多人角色授權後始得以進行之設計。
19. 管理者介面應限制存取來源或不允許遠端存取。

(四) 日誌紀錄：

1. 身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為，資通系統應進行日誌紀錄。

2. 應稽核資通系統管理者帳號所執行之各項功能。
3. 日誌紀錄應包含下列項目，並得由各機關視業務狀況調整：
   (1) 使用者 ID(不可為個資類型)。
   (2) 經系統校時後之時間戳記。
   (3) 執行之功能或存取之資源名稱。
   (4) 事件類型或優先等級(priority)。
   (5) 執行結果或事件描述。
   (6) 事件發生當下相關物件資訊。
   (7) 網路來源及目的位址。
   (8) 錯誤代碼。
4. 應採用單一之日誌紀錄機制，確保輸出格式一致性。
5. 對日誌紀錄進行適當保護及備份，避免未經授權存取或竄改。
6. 定期備份稽核紀錄(log)至與原稽核系統不同之實體系統(如 Log 伺服器)。
7. 應依稽核紀錄(log)儲存需求，配置稽核紀錄(log)所需之儲存容量，除法規另有規定外，稽核紀錄(log)應留存至少六個月。
8. 資通系統應在稽核處理失效，如儲存容量不足之情況下，採取適當之行動，如關閉資通系統、覆寫最舊之稽核紀錄(log)或停止產生稽核紀錄(log)等。
9. 稽核失效事件發生時，對各機關特定之人員或角色提出告警。

(五) 會談(Session)管理：

1. 會談識別碼(Session ID)或使用者 ID 不得顯示於使用者可以改寫處(如網址列)。
2. 會談識別碼(Session ID)採亂數隨機產生且不可預測，儘量使用各種開發架構(J2EE、ASP.NET、PHP)提供之內建會談識別碼(Session ID)產生管理方式，以確保會談識別碼(Session ID)具隨機性及夠強健而不易被推測。
3. 使用者登入後，重新賦予會談識別碼(Session ID)，避免針對會談識別碼(Session ID)之 Session Fixation 攻擊。
4. 使用者在合理之時間內未活動，資通系統應自動將使用者及伺服器間之會談階段設為失效；合理之時間得以參數設定。
5. 使用者之會談階段在登出後應失效。

(六) 錯誤及例外處理：

1. 軟體應設計錯誤處理機制，當系統發生錯誤時，應採取錯誤代碼或簡短訊息呈現，避免將詳細或除錯用訊息直接顯示於使用者頁面，以防被攻擊者用來刺探系統內部資訊，或根據錯誤訊息推測出系統可能之弱點。
2. 所有功能均應進行錯誤及例外處理，並確保將資源正確釋放。

3. 資通系統應具備嚴重錯誤之通知機制，如電子郵件或簡訊。

（七） 檔案儲存及傳輸設計：

1. 檔案如需由伺服端下載至用戶端電腦進行處理或由用戶端上傳回伺服端時，均應識別確認傳輸二端之身分，並採用 SFTP 或其他安全協定進行檔案之存取或傳輸。
2. 資通系統除有特殊情形，且經機關同意者外，資料儲存均應實際儲存於各機關或本府機房(落地)；無法儲存於各機關或本府機房(落地)時，亦不得儲存於有危害國家資通安全疑慮之區域。

（八） 營運持續：

1. 重要資料應定時同步至備份或備援環境，並加以保護限制存取。
2. 重要資料應定期進行離線備份作業，並加以保護限制存取。
3. 應採用「高可用性」(High Availability)架構(分散式或叢集伺服器架構)。
4. 應至少二年辦理一次進行營運持續演練作業，降低營運風險。
5. 定期備份、備援頻率及備份保留代數，應依各資通系統訂定之可容許服務中斷之時間長度(RTO)及能容忍之最大數據丟失量(RPO)。
6. 應將備份還原，作為營運持續計畫測試之一部分。

（九） 其他：資通系統在處理 X.509 公鑰憑證時，應依國家發展委員會訂定之最新版「應用系統使用公鑰憑證處理之安全檢查表」實作各類憑證檢驗之功能。

參、 資通系統安全性檢測

三、 各機關開發或購置之資通系統，應符合下列安全性檢測要求：

（一） 靜態應用軟體安全測試：

1. 資通系統安裝部署前，其原始碼應通過靜態應用軟體安全測試(Static Application Security Testing，SAST)，後續如因錯誤修正、更新、改版或有其他任何異動，而造成原始碼與原測試內容不同時，亦同。但個別系統異動影響之資通安全風險，經各機關審查屬可接受範圍者，不在此限。
2. 資通系統屬依規定免交付原始碼者，不納入靜態應用軟體安全測試範圍。
3. 靜態應用軟體安全測試，通過標準如下：結果應不存在 OWASP(The Open Web Application Security Project，開放網站應用程式安全專案)歸納公布之最新版十大網路資通安全風險(OWASP Top 10)或其他中(Medium)、高(High)以上風險並通過規定之測試標準。

（二） 動態應用軟體安全測試：

1. 網頁應用軟體完成安裝部署，於上線前應通過動態應用軟體安全

測試(Dynamic Application Security Testing，DAST)。

2. 網頁應用軟體後續如有更新及異動，各機關得視網頁應用軟體更新及異動之規模及風險，決定是否進行動態應用軟體安全測試之複測。
3. 動態應用軟體安全測試，通過標準如下：以自動化工具進行黑箱測試(Black-Box Testing)，模擬駭客之攻擊行為，測試系統有無漏洞，測試結果不得存在OWASP(The Open Web Application Security Project ，開放網站應用程式安全專案)歸納公布之最新版十大網路資通安全風險(OWASP Top 10)或其他中(Medium)、高(High)以上風險。

(三) 系統弱點掃描：

1. 網頁應用軟體完成安裝部署，於上線前應通過系統弱點掃描檢測標準。
2. 網頁應用軟體後續如有更新及異動，各機關得視網頁應用軟體更新及異動之規模及風險，決定是否進行系統弱點掃描之複測。
3. 系統弱點掃描檢測，通過標準如下：針對作業系統之弱點、網路服務之弱點、作業系統或網路服務之設定、帳號密碼設定及管理方式等進行弱點檢測，系統弱點掃描之檢測項目包含所有最新版(Common Vulnerabilities and Exposures，CVE)發布之弱點內容，不得存在中(Medium)、高(High)以上風險。

(四) 行動應用軟體基本資通安全檢測：

1. 行動應用軟體上架發行前，應辦理基本資通安全檢測，並取得「行動應用App基本資安自主檢測推動制度」之認證機構認證合格之檢測實驗室，依行動應用程式類別之「行動應用App基本資安檢測基準」檢測合格證明或「行動應用 App 基本資安標章」。
2. 行動應用軟體後續如有更新及異動，各機關得視行動應用軟體更新及異動之規模及風險，決定是否進行基本資通安全檢測之複測。

(五) 滲透測試：

1. 網頁應用軟體完成安裝部署，於上線前應通過滲透測試(Penetration Test，PT)。
2. 網頁應用軟體後續如有更新及異動，各機關得視網頁應用軟體更新及異動之規模及風險，決定是否進行滲透測試之複測。
3. 滲透測試通過標準為不得存在中(Medium)、高(High)以上風險。
4. 滲透測試應針對資通系統之伺服器或主機作業系統、應用軟體、網路服務、可直接進行連線(配有IP)之物聯網設備(如門禁設備、網路印表機、網路攝影機(IPCAM)、環控系統，如監控溫度或濕度之機房環控系統之伺服器主機或無線AP/無線路由器等安全弱點及漏洞，進行滲透或穿透跳躍主機之入侵測試，設法取得未經授

權之存取權限，並測試內部資訊是否有遭受不當揭露、竄改或竊取之可能性。

肆、 資通系統運行環境

四、 各機關開發或購置之資通系統，其運行環境應符合下列安全要求：

（一） 資通系統應使用臺北市政府資訊局(以下簡稱資訊局)電腦機房作為運行環境。

（二） 作業平臺應每月評估更新，並關閉不必要服務及埠口(Port)。

（三） 針對資通系統依賴之外部元件或軟體，應注意其安全漏洞通告，每月定期評估更新。

（四） 資通系統依賴之外部元件或軟體，密碼不得使用預設或空值。

（五） 應符合政府基準組態、本府或各機關訂定之安全基準。

（六） 各機關應至少每半年盤點運行環境所需之主機或資通系統管理者及使用者帳號、存取權限配置、主機與網路防火牆政策、網路位址(IP)、虛擬或實體主機資源、儲存空間、資料庫系統帳號與權限等。如無需使用應予以刪除、停用或釋出資源。

（七） 開發、測試及正式作業環境應作區隔；作業環境之資料、帳號、權限及網路開放等均應不同並區隔，且不得共用及連線。開發或測試環境亦應符合本點安全要求。

（八） 運行環境包含作業系統及應用系統等，應保存稽核紀錄(log)，除法規另有規定外，稽核紀錄(log)應留存至少六個月，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。

伍、 資通系統安全週期管理規定

五、 資通系統安全週期管理規定：

（一） 前三點所定資通系統安全需求、安全性檢測要求及運行環境安全要求，應於上線前及定期維護作業檢視合規情形，並應納入查驗或驗收付款之必要條件。

（二） 定期測試或檢測之時間規定如下：前次測試或檢測在上半年者，應於次年上半年至少辦理一次測試或檢測；前次測試或檢測在下半年者，應於次年下半年至少辦理一次測試或檢測。

（三） 資通系統經檢測為中(Medium)、高(High)以上之風險者，應於檢測後十個工作天內完成修復或回復因應之控制措施；個別資通系統得依需求調整限期修復之規定。

（四） 各機關得視個案狀況及需求，要求廠商委託第三方專業廠商或機構執行第三點所定安全性檢測。除另有規定外，廠商所委託之第三方專業廠商或機構不得與廠商為公司法規定之關係企業，亦不得為陸資企業或依政府採購法及其相關子法規定不得作為分包對象之廠商。

六、 運行環境相關軟體或系統平臺於原廠停止服務前，應完成升級、更新

或汰換作業。無法配合者，應將風險有效控制措施與後續處置規劃簽報各機關資通安全長同意後，始得持續運作，並應定期檢討追蹤；資訊局得提供相關軟體或資通安全防護停止支援服務之資訊供各機關使用。

七、 資通系統經檢測無法修補弱點者，應擬訂風險有效控制措施及後續升級規劃，於簽報各機關資通安全長同意後，始得持續運作，且應定期檢討追蹤。

八、 資通系統因異動或停止服務須進行部分或全面下架時，應清查運行環境所需之主機或資訊系統管理者及使用者帳號、存取權限配置、主機及網路防火牆政策、網路位址(IP)、虛擬或實體主機資源、儲存空間、資料庫系統帳號及權限等。如無需使用應予以刪除、停用或釋出資源，避免無人維運造成資通安全漏洞。

陸、 其他規定

九、 內部或對外服務之資通系統如有網域名稱申請之需求，應依臺北市政府各機關辦理「.taipei」頂級網域保留字作業要點辦理。

十、 各機關發展對外便民服務、使用公有雲端服務、社群、通訊平臺等第三方服務進行與民眾或其他單位互動或行銷者，應使用該平臺之相關資通安全設定及機制，並依臺北市政府各機關網站服務管理作業原則辦理。

十一、 各機關發展行動應用軟體者，應依臺北市政府行動應用軟體(App)服務發展作業原則辦理。

十二、 資通系統承包廠商應依資通安全管理法之規定，接受機關對其資通安全維護情形之監督。

柒、 附則

十三、 個別資通系統有不適用本指引之情形時，各機關得排除本指引部分規定之適用，但各機關應於採購文件中具體說明。

前項排除項目屬資通安全責任等級分級辦法所定應辦事項或控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得依資通安全責任等級分級辦法第十一條規定函請資訊局審查，經審查同意並送資通安全法主管機關備查後，始得免執行該事項或控制措施。

十四、 個別資通系統應使用威脅建模(Threat Modeling)根據系統功能及要求，識別可能影響系統之威脅(包括但不限於偽冒、竄改、否認、洩漏、拒絕、提權等威脅類型)，及進行風險分析及評估(包括但不限於可能損害、可重製、可利用、影響人數、可發現等風險因子)，將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。

十五、 各機關應落實資通系統開發、部署上版、變更、例行性檢核或內外部稽核等要求；相關執行紀錄並應妥善保存，以備查核使用。

十六、 違反本指引者，依本府資通安全管理相關規定懲處。委外契約並應納入懲罰性違約金之相關約定。

十七、 各機關得依業務需要，自行訂定其他執行管理規範。