臺北市政府資通安全事件通報及應變作業指引

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)為遵照資通安全管理法第十四條及本府資安全維護計畫之規定，建立本府資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變作業指引(以下稱本指引)。

貳、 適用範圍

二、 發生於本府各機關之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

參、 責任

三、 各機關所屬人員於發現資通安全事件時，應依本指引或權責人員之指示，執行通報及應變事務。

四、 各機關應於資通安全事件發生前，確保所屬或所監督之公務機關及所管之特定非公務機關是否制定及落實資通安全事件通報及應變管理程序，並依規定指定其知悉資通安全事件之通報以及完成應變作業後之結案登錄方式。

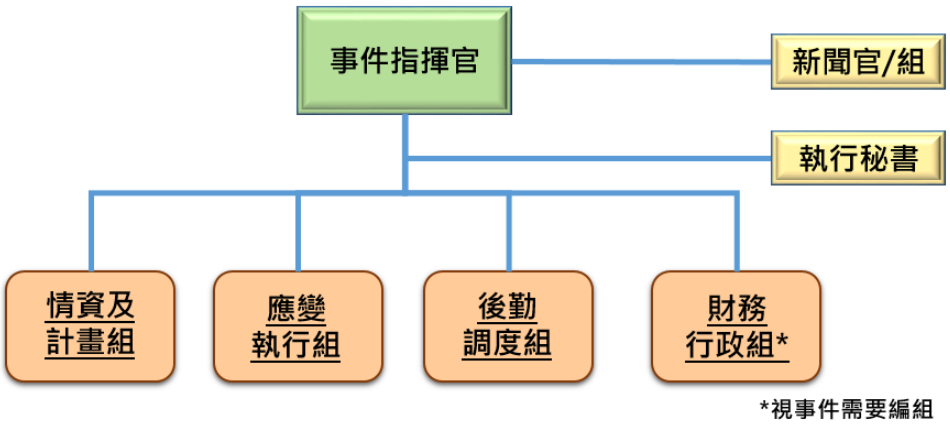
五、 各機關應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變管理程序，並於知悉資通安全事件後向本府進行通報，於完成事件之通報及應變程序後，依本府指示提供相關之紀錄或資料。

六、 各機關應於知悉資通安全事件後，應依本指引之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依本府、上級或監督機關及資通安全管理法主管機關指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

肆、 資通安全事件通報及應變小組

七、 各機關應成立資通安全事件通報及應變小組(以下簡稱通報應變小組)，於平時進行演練，並於發生資通安全事件時，依事件等級進行通報及應變作業；本府資通安全事件通報及應變小組則因應各機關事件處理之支援需求，成立本府情資及計畫組、應變執行組、後勤調度組。

通報應變小組組成如圖一，各分組代表如表一，其任務如下：



圖一、資通安全事件通報及應變小組組成

表一、資通安全事件通報及應變小組各分組代表

	第一級、第二級 資通安全事件	第三級、第四級 資通安全事件
事件指揮官	資訊(安)單位主管	資通安全長
新聞官/組	對外發言人員或單位主管	
執行秘書	資通安全專責人員 或資訊人員	資訊(安)單位主管
情資及計畫組組長	資通安全專責人員 或資訊人員	資訊(安)單位主管 或資通安全專責人員
應變執行組組長	資通安全專責人員 或資訊人員	資訊(安)單位主管 或資通安全專責人員
後勤調度組組長	資通安全專責人員 或資訊人員	資訊(安)單位主管 或資通安全專責人員
財務行政組組長	財務或秘書單位主管	

（一） 事件指揮官

為通報應變小組總召集人，綜理全般業務，直接督導各單位聯絡人員及機關新聞官/組，並確保機關處理資通安全事件通報及應變作業時各成員均落實相關程序配合各組組長辦理。

（二） 新聞官/組

為資通安全事件對外發布新聞或說明之單一窗口，負責綜整與定期更新訊息及擬定溝通計畫。

（三） 執行秘書

為事件指揮官幕僚，負責督辦通報應變小組各項業務。

（四） 情資及計畫組

1. 本分組負責辦理下列事宜：
   （1） 資通安全事件通報及情資分享：透過本府或機關資通安全監控中心(SOC)、內外部情資、資安或網路設備釐清事件影響，並清查各單位受影響情形，據以完成資通安全事件各階段通報，分享惡意程式或中繼站等。
   （2） 應變策略及計畫研擬：於發生重大資通安全事件時，依據事件情況研擬損害控制、復原作業及跡證保存計畫。
2. 本分組由機關資通安全專責人員、資訊人員及委外廠商或外部專家組成，本府、上級機關、監督機關或其他相關機關，亦應視情況派員參與，以提供必要之支援協助。

（五） 應變執行組

1. 本分組負責辦理下列事宜：
   （1） 執行損害控制：依據情資及計畫組研擬之應變策略及計畫，調度資訊及資通安全人員執行災害搶救及損害管制，防止次波攻擊及損害擴散。
   （2） 復原作業：依據情資及計畫組研擬之復原作業，完成系統重建、弱點掃描或漏洞修補等事宜。
2. 本分組由機關資通安全專責人員、資訊人員、事件發生之業務單位及委外廠商組成，本府、上級機關、監督機關或其他相關機關得於機關申請支援時視事件需要派員參與。

（六） 後勤調度組

1. 本分組負責辦理下列事宜：
   （1） 跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。
   （2） 事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。
   （3） 提出改善建議：依據事件調查根因，提出短、中、長期改善建議。
2. 本分組由機關資通安全專責人員、資訊人員及委外廠商或外部專家組成，本府、上級機關、監督機關或其他相關機關得於機關申請支援時視事件需要派員參與。

（七） 財務行政組

本分組視事件需要由機關財務或秘書單位組成，負責辦理預算調

撥及提供行政支援事宜。

八、 各機關得以現有相關資安任務分組為基礎，依各機關編制及業務分工，經機關資通安全長同意後調整小組組成及各分組代表，另得視資通安全事件或機關資通環境需要調整各分組任務。

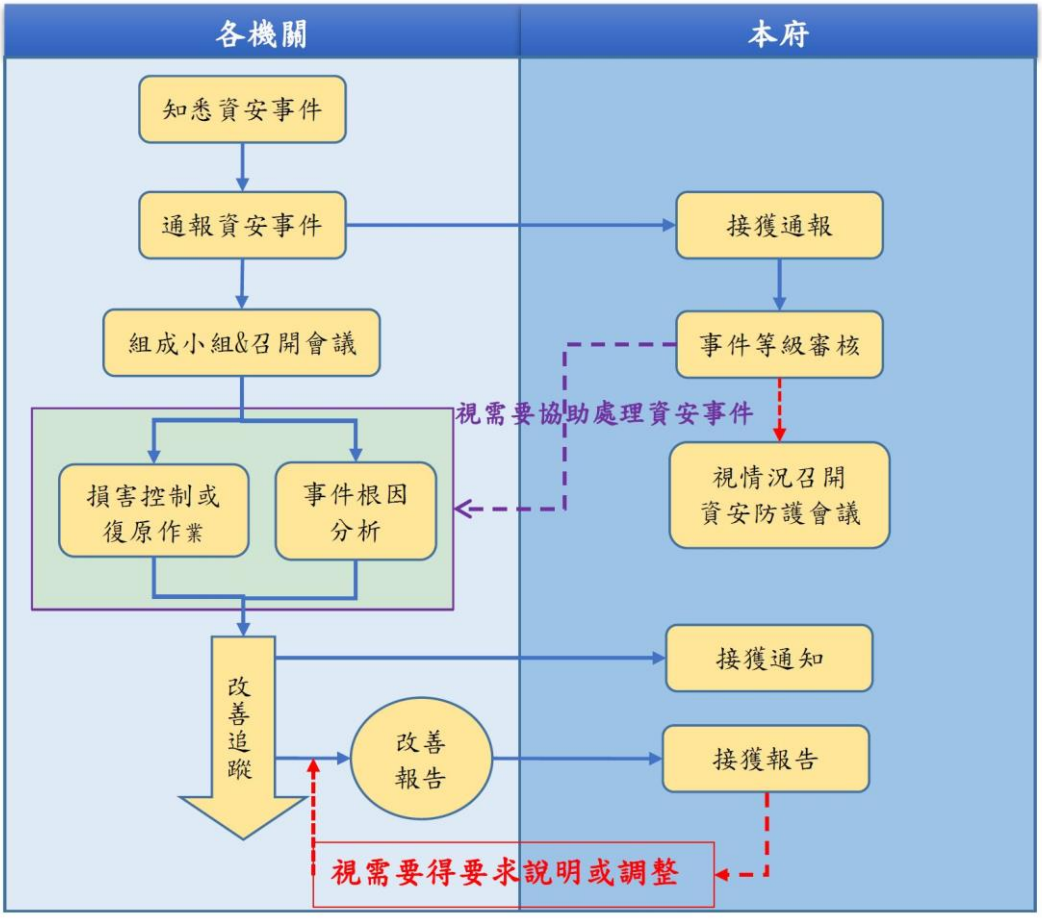
九、 小組成員除應變執行組中事件發生之業務單位，屬事件發生時方確定之成員，與財務行政組視事件需求方成立外，均屬常設組成。

十、 小組之事件指揮官、執行秘書、情資及計畫組等成員，應至國家資通安全通報應變網站登錄聯繫資訊，以利即時掌握資通情資與通報案件，成員如有異動應即更新，並應落實代理機制。

十一、 各機關應公告本小組成員與聯繫方式，確保全機關人員周知以利即時通報資安事件，並確保本小組各成員聯絡管道全天暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

伍、 通報程序

十二、 各機關之資通安全事件通報及應變程序，應包含通報資通安全事件、召開事件應變會議、損害控制或復原作業、事件根因分析及改善追蹤等項目(如圖二)，並依資通安全管理法施行細則第六條第一項第九款規定納入資通安全維護計畫中，各項程序如下：



圖二、資通安全事件通報及應變程序

十三、通報作業程序

（一） 通報資通安全事件

1. 各機關應依資通安管理法、資通安全事件通報及應變辦法及本指引規定，於知悉資通安全事件後，由權責人員應或通報應變小組依資通安管理法主管機關指定方式完成事件通報；如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，權責人員或通報應變小組應於知悉資通安全事件後一小時內，將該事件依本府或資通安全管理法主管機關所指訂或認可之方式，通知該機關。
2. 知悉資通安全事件之時間點，係指事件影響範圍或時間長度符合資通安全事件通報及應變辦法第四條所列各類等級資通安全事件，且機關人員已確認影響符合事件等級之時間點。
3. 第三級或第四級資通安全事件，各機關除依上述規定通報外，應另以電話通知本府、上級機關及監督機關。

（二） 判定事件等級之流程及權責

各機關之權責人員或通報應變小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

1. 事件涉及核心業務或關鍵基礎設施業務之資訊與否。
2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。
3. 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。
4. 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。
5. 事件其他足以影響資通安全事件等級之因素。

（三） 除因網路或電力中斷等事由，致無法依資通安全管理法主管機關所指定或認可之方式通報外，應於知悉資通安全事件後一小時內資通安全管理法主管機關所指定或認可之方式，進行事件通報。

（四） 各機關因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於知悉資通安全事件後一小時內以電話或其他適當方式，將該次資安事件應通報之內容及無法依規定方式通報之事由，分別告知本府、上級、監督機關及資通安全管理法主管機關，並於事由解除後，依原方式補行通報。

（五） 召開事件應變會議

各機關於完成資通安全事件之初步損害控制後應召開事件應變會議，會議形式不拘，就下列事項進行討論：

1. 資通安全事件概況。
2. 評估受影響範圍。
3. 其他必要之討論事項。

第三級或第四級資通安全事件得視情形邀請本府、上級或監督機關出席。

（六） 資通安全事件等級如有變更，權責人員或通報應變小組應告知通報窗口，使其續行通報作業。

（七） 各機關於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向機關之權責人員或窗口，以指定之方式進行通報。

十四、 接獲自身、所屬或所監督之公務機關通報之評估作業程序

（一） 本府之權責人員或通報應變小組，於接獲所屬或所監督之公務機關之資通安全事件通報後，應於以下時限內，完成資通安全事件通報等級及相關事項之審核：

1. 通報為第一級或第二級之資通安全事件，於接獲通報後八小時內。
2. 通報為第三級或第四級之資通安全事件，於接獲通報後二小時內。

（二） 本府之權責人員或通報應變小組進行本條第一項之審核過程中，得請求通報之公務或特定非公務機關提供級別判斷所需之資料或紀錄。

（三） 本府於必要時得依據審核之結果，逕行變更資通安全事件之等級或修正通報內容(如事件發現時間等)，並應於決定變更後一小時內，將審核結果及級別變更之決定通知資通安全管理法主管機關，並提供做成決定所依據之相關資訊。

十五、 對所屬或所管特定非公務機關之協助

各機關知悉資通安全事件，向本府、上級或監督機關為通報時，本府、上級或監督機關資通安全長應視必要性於以下時限內，決定是否組成通報應變小組，以協助所屬機關執行通報及應變程序，並視情形提供必要之支援或協助：

（一） 通報為第一級或第二級之資通安全事件，於完成複核後二小時內。

（二） 通報為第三級或第四級之資通安全事件，於接獲通報後一小時內。

陸、 應變程序

十六、 事件發生前之防護措施規劃

各機關應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

十七、 損害控制機制

（一） 由應變執行組執行損害控制或復原作業，並辦理下列事項：

1. 確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，

防止次波攻擊及擴散情形。

2. 評估各系統是否於可容忍中斷時間內恢復服務及對利害關係人之影響，決定是否對外公告事件之相關內容。
3. 於完成損害控制或復原作業後，依資通安管理法主管機關指定之方式完成通知作業。
4. 第三級或第四級資通安全事件，除依上述規定辦理外，並應辦理下列事項：
   (1) 定時向事件指揮官、通報應變小組成員及本府、上級與監督機關回報控制措施成效。
   (2) 倘涉及個人資料外洩，應評估通知當事人之適當方式，依個人資料保護法第十二條規定辦理。

（二） 負責應變之權責人員或通報應變小組，應完成以下應變事務之辦理，並留存應變之紀錄：

1. 資安事件之衝擊及損害控制作業。
2. 資安事件所造成損害之復原作業。
3. 資安事件相關鑑識及其他調查作業。
4. 資安事件之調查與處理及改善報告之方式。
5. 資安事件後續發展及與其他事件關聯性之監控。
6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據各機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。
7. 其他資通安全事件應變之相關事項。

（三） 對於第一級、第二級資通安全事件，各機關應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，各機關應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

（四） 各機關於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

柒、 資安事件後之跡證保存、事件根因分析及改善追蹤

十八、 各機關完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

十九、 發生資通安全事件時，各機關應依下列原則進行跡證保存：

（一） 機關進行跡證保存時，應優先採取隔離機制，包含網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方

式，以降低攻擊擴散。

（二） 若系統無備援機制，應備份受害系統儲存媒介（如硬碟、虛擬機映像檔）後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。

（三） 若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份份後重建系統，經系統測式後切換至原系統提供服務。

（四） 若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。

二十、 事件根因分析，辦理事項如下：

（一） 依跡證保存之規定保存相關跡證，相關採證與可疑之惡意程式應交付至本府指定之鑑識採證檔案交換區，另如有惡意程式應配合資通安全管理法主管機關規定上傳至 Virus Check 網站(https://viruscheck.tw/)進行檢測。

（二） 除設備故障外，應依據前目保存跡證，督導委外廠商或外部專家進行根因調查，並提出紀錄分析；如有發現惡意程式，應提出惡意程式分析。

（三） 依據事件調查、處理及改善報告，機關應評估短、中、長期資安管理改善策略，其內容如下：

1. 短期：完成可立即性修補項目之調整，例如：依本府「資安事件調查與復原檢核表」進行安全檢測與修補。
2. 中期：依據事件根因提出三至六個月內完成之強化作為，例如：盤點機關老舊資通系統或設備，並訂定汰換期程。
3. 長期：依據事件受害情形，視需要提出二年內完成之管理改善建議，例如：培養機關資安人員能力或納入風險議題進行風險管控措施。

（四） 由執行秘書將事件調查根因及改善策略提報事件指揮官裁處，並由機關資通安全專責人員彙整送交本府、上級及監督機關。

二十一、 資通安全事件調查、處理及改善報告應包括以下項目：

（一） 事件發生、完成損害控制或復原作業之時間。

（二） 事件影響之範圍及損害評估。

（三） 損害控制及復原作業之歷程。

（四） 事件調查及處理作業之歷程。

（五） 為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

（六） 前款措施之預定完成時程及成效追蹤機制。

二十二、改善追蹤

各機關進行事件改善追蹤時，應召開會議，並據以辦理下列事項：

（一） 評估改善作為期程。

（二） 評估執行成效，並據以調整改善策略。

（三） 配合本府、上級機關或監督機關辦理相關改善作為。

（四） 第三級或第四級，或本府、上級機關或監督機關指定之資通安全事件，應由執行秘書將各階段改善措施執行成效定期回報事件指揮官至完成各項改善措施為止，並由機關資通安全專責人員彙整送交本府、上級機關及監督機關。

（五） 依會議決議及資通安全管理法主管機關指定之方式，送交調查、處理及改善報告；第三級或第四級，或本府、上級機關或監督機關資通安全事件，應另以密件公文將該報告送交本府、上級機關或監督機關。

（六） 機關送交調查、處理及改善報告後，相關改善事項應納入本府威脅與弱點管理系統與機關現行定期追蹤管考機制，並於府資安長會議定期檢討改善進度。

二十三、本府針對資安事件提供相關鑑識與調查處理工具，並訂定「資安事件調查與復原檢核表」，檢核結果各機關應納入調查、處理及改善報告。

二十四、如資通安全事件由本府資通安全事件通報及應變小組支援者，將於事件調查完成後提交請求支援機關事件報告，內容包含事件發生時間、來源與目標 IP、駭客所在位置、攻擊方法與路徑及影響分析，以及系統復原、事件排除、修補及防禦等措施建議(含：系統重新安裝與設定、系統隔離修護、調整防火牆、更新系統安全或防毒軟體修正檔、弱點修補或新增防禦設備等建議)以提供予機關設置防禦措施等改善建議，機關得參考本報告製作調查、處理及改善報告。

捌、 紀錄留存及管理程序之調整

二十五、各機關應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「資安事件調查與復原檢核表」上留存完整之紀錄，該文件並應經承辦之權責人員、資通安全長簽核。

二十六、各機關於完成資通安全事件之通報及應變程序後，應依據「資安事件調查與復原檢核表」之內容及實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

玖、 情資分享

二十七、各機關處理資安事件後應依「資通安全情資分享辦法」分享以下情資：

（一） 資通系統之惡意偵察或情蒐活動。

（二） 資通系統之安全漏洞。

（三） 使資通系統安全控制措施無效或利用安全漏洞之方法。

（四） 與惡意程式相關之資訊。

（五） 資通安全事件造成之實際損害或可能產生之負面影響。

（六） 用以偵測、預防或因應前五款情形，或降低其損害之相關措施。

（七） 其他與資通安全事件相關之技術性資訊。

二十八、各機關應依資通安全管理法主管機關與本府指定之情資分享方式提供情資。

壹拾、演練作業

二十七、各機關應每年依資通安全事件通報應變辦法之規定辦理兩次社交工程演練、一次資通安全事件通報及應變演練，並於完成後一個月內，將執行情形及成果報告依資通安全管理法主管機關指定方式提報。

二十八、各機關應配合資通安全管理法主管機關與本府依資通安全事件通報應變辦法之規定所辦理之社交工程演練、資通安全事件通報及應變演練，二級以下機關應配合一級機關辦理前揭演練。

二十九、社交工程演練基準依「臺北市政府資通安全維護計畫」肆、資通安全政策及目標所訂，如單次演練未達標之機關應辦理加強教育訓練並檢討，如連續兩次均未達標之機關應再次辦理演練。

三十、 資通安全事件通報及應變演練應依資通安全事件通報應變辦法規定之各級事件通報、損害控制與改善結案時效進行通報處置，如逾期者機關應檢討並再度辦理演練。

三十一、各機關應配合資通安全管理法主管機關與本府依本指引之規定，所辦理之下列資通安全演練作業：

（一） 社交工程。

（二） 資安事件通報及應變。

（三） 資安事件處理報告。

三十二、 本指引相關系統與工具如下：

（一） 威脅與弱點管理系統(TVMS)。

（二） 鑑識採證檔案交換區。

（三） 離線版與連線版端點偵測及回應軟體(EDR)。

（四） 防毒軟體。

（五） 內網進階持續性威脅攻擊(APT)偵測設備。

（六） 鑑識採證工具(CDIR)。