高雄市政府民政局暨所屬機關

資通安全事件通報及應變管理程序

發行日期：112 年 5 月 17 日

變更紀錄

版次	發行日	修訂者	說明	核准者
1.0	108 年 2 月 18 日	高雄市政府民政局	初版文件發行	民政局局長
1.1	108 年 6 月 27 日	高雄市政府民政局	配合行政院核定資通安全責任等級修正	民政局局長
1.2	109 年 11 月 5 日	高雄市政府民政局	配合本市戶政事務所組織整併及行政院審查意見修正	民政局局長
1.3	110 年 6 月 16 日	高雄市政府民政局	配合行政院核定三民戶政事務所資通安全責任等級為 D 級	民政局局長
1.4	111 年 4 月 27 日	高雄市政府民政局	1. 修正適用範圍格式 2. 修正第肆項事件通報窗口及緊急處理小組第一條本機關之「資通安全事件通報窗口及聯繫專線」第一點之人員 3. 修正第柒項資安事件後之復原、鑑識、調查及改善機制第三、四條內容 4. 修正附件表單 1.資通安全事件通報窗口及聯繫專線	民政局局長
1.5	111 年 9 月 27 日	高雄市政府民政局	配合行政院修正「各機關資通安全事件通報及應變處理作業程序」辦理	民政局局長
1.6	112 年 5 月 17 日	高雄市政府民政局	配合人員異動修正通報聯繫人員窗口及通報應變小組名單	民政局局長

目錄

壹、目的

高雄市政府民政局（以下簡稱本局）暨所屬殯葬管理處、兵役處、本市各戶政事務所全體機關（以下統稱本機關）為遵照資通安全管理法第 14 條、資通安全事件通報及應變辦法及本局資通安全維護計畫之規定，建立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管理程序（以下稱本管理程序）。

貳、適用範圍

發生於本機關之事件，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。

本管理程序適用範圍如下表：

責任等級	機關名稱	
C	高雄市政府民政局	
	高雄市殯葬管理處	高雄市兵役處
D	高雄市鼓山戶政事務所	高雄市左營戶政事務所
	高雄市楠梓戶政事務所	高雄市三民戶政事務所
	高雄市新興戶政事務所	高雄市苓雅戶政事務所
	高雄市前鎮戶政事務所	高雄市小港戶政事務所
	高雄市鳳山戶政事務所	高雄市岡山戶政事務所
	高雄市旗山戶政事務所	高雄市美濃戶政事務所
	高雄市大寮戶政事務所	高雄市仁武戶政事務所
	高雄市鳥松戶政事務所	高雄市路竹戶政事務所
	高雄市茄萣戶政事務所	高雄市梓官戶政事務所

參、責任

一、本機關所屬人員於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。

二、本機關應於資通安全事件發生前，確保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。

三、本機關應視必要性，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機關進行通報，於完成事件之通報及應變程序後，依本機關指示提供相關之紀錄或資料。

四、本機關應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依上級或監督機關及行政院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、事件通報窗口及資通安全事件通報及應變小組

一、本機關之「資通安全事件通報窗口及聯繫專線」為：

(一)本局資訊室王股長子評（07-7995678 分機 5252）、廖管理師英捷（07-7995678 分機 5257）及蘇分析師信宏（07-7995678 分機 5258)。

(二)各機關資通安全事件通報窗口。

二、本機關成立資通安全事件通報及應變小組，為任務編組，成員由本局資通安全長指派機關之資通安全相關技術人員擔任，或亦得由其他機關資通安全相關技術人員或外部專家擔任之。成員相關職掌如下：

（一）事件指揮官（由資安長擔任）

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。

（二）新聞官/組

視事件需要由事件指揮官或其授權人員擔任新聞官或分組代表，資通安全事件對外發布新聞或說明之單一窗口，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：透過資通安全監控中心(SOC)、防毒軟體及系統釐清事件影響，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 IoC 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，亦應視情況或納入政風單位派員參與，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。

(3) 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.本分組由機關資通安全專責人員、資訊人員、業務單位及委外廠商組成，上級機關得於機關申請支援時派員參與。

（六）後勤調度組

1.本分組負責辦理下列事宜：

(1) 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。

(2) 提出改善建議：依據事件調查根因，提出短、中、長期改善建議。

(3) 彙整改善報告。

(4) 撰寫調查、處理及改善報告。

(5) 追蹤管考：針對機關單位已結案或未結案事項，如有未盡改善事宜，

將另案追蹤管考。

(6) 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，上級機關得於機關申請支援時派員參與。

（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。

三、本機關應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。

四、本機關所屬人員發現資通安全事件後，應立即向所屬單位主管及本機關之通報窗口通報。

五、本機關應確保通報窗口之聯絡管道全天維持暢通，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。

六、負責事件處理之單位（該事件發生之單位）權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。

七、事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向各機關資通安全長報告，本機關所屬機關或受託廠商應副轉知本局，由資通安全事件通報及應變小組。

伍、資訊安全事件通報與應變作業流程

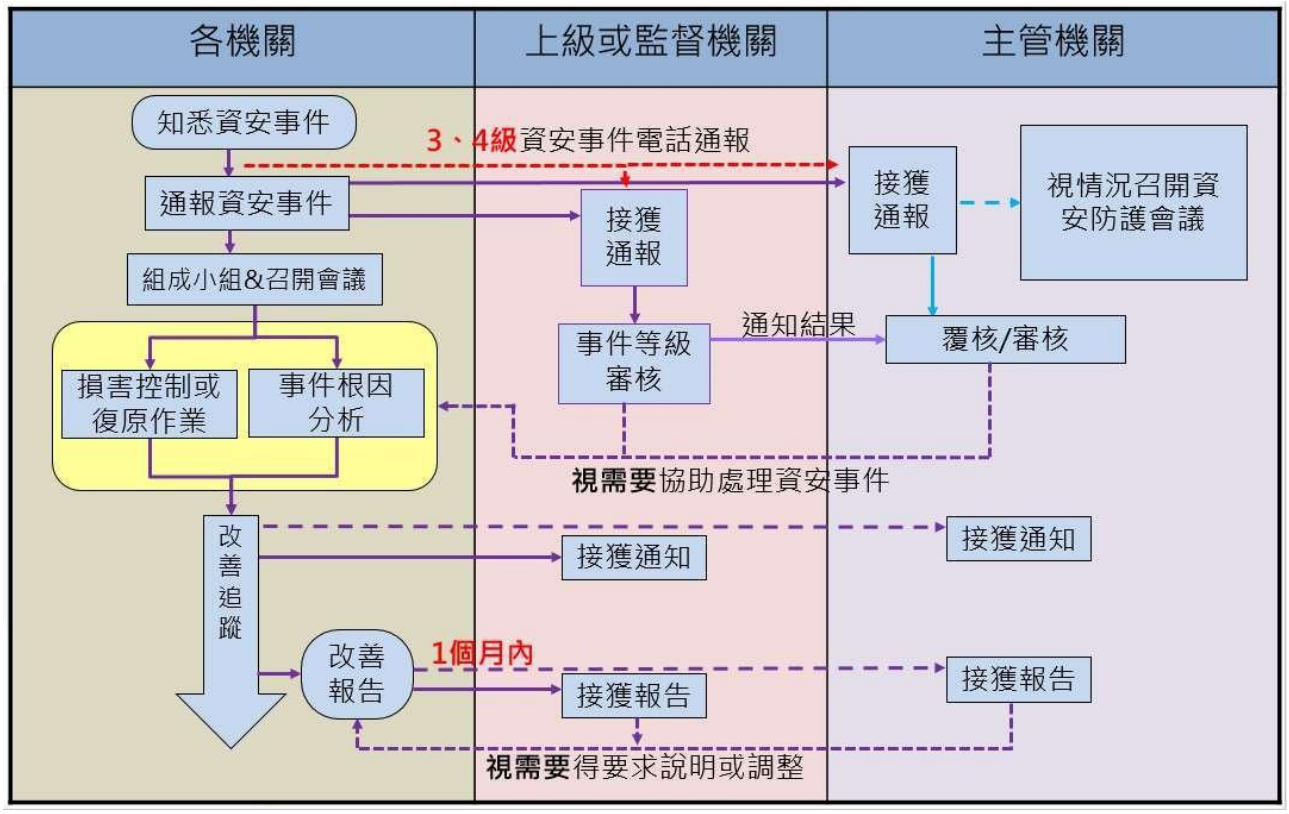
一、資安事件/故發生後應依「資訊安全事件通報與應變作業流程」處理(如下圖)，相關作業程序應注意下列事項：

（一）考量單位資源，於最短的時間內，確認回復後之系統及相關安全控制是否完整及正確。

（二）向管理階層報告處理情形，並檢討、分析資訊安全事件/故。

（三）限定僅授權之人員可使用回復後正常作業之系統及資料。

（四）緊急處理步驟應詳實記載，以備日後查考。



二、資訊安全事件通報與應變作業流程

（一）通報資通安全事件：

1. 各機關應依本法及資通安全事件通報及應變辦法規定，由情資及計畫組依主管機關指定方式完成事件通報。
2. 第三級或第四級資通安全事件，各機關除依前目規定通報外，應另以電話或其他適當方式通知上級機關，無上級機關者，應通知主管機關；行政院資通安全處(數位發展部資通安全署成立後為該署)就第三級或第四級資通安全事件，依國土安全緊急通報作業規定轉報行政院國土安全辦公室。

（二）組成通報應變小組與召開事件應變會議：

各機關於完成第三級或第四級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，由事件指揮官主持討論下列事項，並得視情況邀請上級機關或主管機關出席：

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。

（三）損害控制或復原作業：

1. 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，依主管機關指定之方式完成通知作業。

2. 第三級或第四級資通安全事件，除依前目規定辦理外，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、上級機關回報控制措施成效；無上級機關者，應回報主管機關。

(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。

（四）事件根因分析：

由後勤調度組執行，依資通安全事件等級，建議辦理事項如下：

1. 依第壹拾點跡證保存之規定保存相關跡證，惡意程式建議得請防毒軟體或資安服務公司檢測，並上傳至 Virus Check 網站 (https://viruscheck.tw/)分析，以更新或強化相關偵測及聯防機制，不宜上傳至其他平臺。

2. 除設備故障外，後勤調度組應依據前目保存跡證，由組長督導委外廠商或外部專家進行根因調查，並提出紀錄分析；如發現惡意程式，應提出惡意程式分析。

3. 依據事件調查根因分析結果，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，例如更換密碼或修補程式弱點等。

(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。

4. 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上級機關；無上級機關者，應送交主管機關。

（五）改善追蹤：

各機關進行事件改善追蹤時，應視需要召開會議，並據以辦理下列事項：

1. 評估改善作為期程。

2. 評估執行成效，並據以調整改善策略。

3. 配合上級機關或主管機關辦理相關改善作為。

4. 第三級或第四級資通安全事件，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上級機關；無上級機關者，應送交主管機關。

5. 依主管機關指定之方式，送交調查、處理及改善報告；第三級或第四級資通安全事件，應另以密件公文將該報告送交主管機關及上級或監督機關。
6. 機關送交調查、處理及改善報告後，相關改善事項應納入機關現行定期追蹤管考機制。

陸、通報程序

本機關之權責人員或資通安全事件通報及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、除事件之等級外，權責人員或資通安全事件通報及應變小組亦應對資通安全事件之影響範圍、損害程度及本機關因應之能力進行評估。

四、本機關權責人員或資通安全事件通報及應變小組於完成資通安全事件等級之判斷及相關評估後，應盡速報資通安全長核准。

五、除因網路或電力中斷等事由，致無法依上級或監督機關及行政院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依上級或監督機關及行政院所指定或認可之方式，進行資通安全事件通報。

六、本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通報依規定方式通報之事由，分別告知所屬之上級或監督機關及行政院，並於事由解除後，依原方式補行通報。

七、資通安全事件等級如有變更，權責人員或緊急應變小組應告知通報窗口，使其續行通報作業。

八、本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，應即向本機關之權責人員或窗口，以指定之方式進行通報。

九、本機關於知悉資通安全事件後，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，權責人員或緊急處理小組應於知悉資通安全事件後一小時內，將該事件依上級或監督機關及行政院所指定或認可之方式，通知該機關。

十、本機關執行通報應變作業時，得視情形向直屬上級機關提出技術支援或其他協助之需求。

十一、接獲自身、所屬機關通報之評估作業程序

(一)本機關之權責人員或緊急處理小組，於接獲所屬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)本機關之權責人員或緊急處理小組進行本條第一項之審核過程中，得請求通報機關提供級別判斷所需之資料或紀錄。

(三)本機關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，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行政院，並提供做成決定所依據之相關資訊。

十二、對所屬機關之協助

本機關之所屬機關知悉資通安全事件，向本機關為通報時，本機關資通安全長應視必要性於以下時限內，決定是否組成緊急處理小組，以協助隸屬本機關之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：

1.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。
2.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。

柒、應變程序

一、本局暨所屬機關資訊安全危機處理包括事前建置安全防護機制、事中主動預警與緊急應變，以及事後復原追蹤鑑識偵查等步驟。說明如下：

（一）事前建置安全防護機制

1. 建置資訊安全管理系統及整體防護架構。
2. 彙整及備妥資訊安全相關文件。

（二）事中主動預警與緊急應變

1. 事件辨識：辨識事件之歸屬及採取之對策，如內部危安事件、外力入侵事件、天然災害或重大突發事件等，並決定處理的方法與程序。
2. 事件控制：依據各類事件危機處理之程序，進行事件傷害控制，降低影響的程度及範圍。

3. 問題解決：事件處理權責單位或負責人須將問題解決。必要時，應向資訊安全委員會提出建議方案。
4. 恢復作業：問題解決後，系統需恢復至事件發生前之正常運作狀態。

（三）事後復原追蹤鑑識偵查

1. 後續追蹤之精神乃係檢討相關資訊安全事件是否會重複發生，並審視現有環境漏洞，透過研析相關資料，以釐清事件發生之原因與責任。
2. 受損單位依復原程序實施災後復原重建。
3. 重大資訊安全事件應保留事件發生之線索，如有需要得向國家資通安全會報技術服務單位或檢警單位申請數位鑑識（電腦、網路鑑識）。

二、損害控制機制

(一)負責應變之權責人員或資通安全事件通報及應變小組，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，應依據本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。

(二)對於第一級、第二級資通安全事件，本機關應於知悉事件後七十二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；於第三級、第四級資通安全事件，本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。

(三)本機關完成通報及應變程序之辦理後，應依所隸屬之上級機關或行政院所指定或認可之方式進行結案登錄。

(四)本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。

捌、資安事件後之復原、鑑識、調查及改善機制

一、本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。

二、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。

三、本機關應向所隸屬之上級機關及行政院提出第一項之損害控制或復原作業之報告，以供監督與檢討。

四、本機關指示隸屬於本機關之所屬機關提出第二項送交之報告之期限，若其逾期未提出，本機關除應使其盡速提出外，並應為其他必要之監督及指示。

玖、紀錄留存及管理程序之調整

一、本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「資訊安全事件通報單」上留存完整之紀錄，該文件並應經通報人員、通報主管、資通安全長簽核。

二、本機關於完成資通安全事件之通報及應變程序後，應依據「資訊安全事件通報單」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。

壹拾、跡證保存

為確保資通安全事件發生時，各機關所保有跡證足以進行事件根因分析，各機關依資通安全事件等級，建議辦理下列事項，並應視事件情形辦理其他必要之跡證保存事項：

一、各機關於日常維運資通系統時，應依自身資通安全責任等級保存日誌(log)，並建議定期備份至與原稽核系統不同之實體系統，其保存範圍及項目如下表。

資通安全責任等級	保存範圍	保存項目
A	機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄。	1. 作業系統日誌(OS event log) 2. 網站日誌(web log) 3. 應用程式日誌(AP log) 4. 登入日誌(logon log)
B	機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄。	
C	機關應保存全部核心資通系統最近六個月之日誌紀錄。	

註：若資訊系統已向上集中者，則可由上級機關保存。

二、發生資通安全事件時，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，包含設備關機、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(例如硬碟、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後重建系統，經系統測試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。

三、各機關於簽訂資通系統或服務之委外契約時，應依前二款規定於契約中明定紀錄保存及備份規定。

壹拾壹、演練作業

一、本機關應配合本府資訊中心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、本機關應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：

(一)社交工程演練。

(二)資安事件通報及應變演練。

(三)網路攻防演練。

(四)情境演練。

(五)其他資安演練。

壹拾貳、附件表單

1. 資通安全事件通報窗口及聯繫專線

機關名稱	姓名	電話	電子郵件
高雄市政府民政局	王子評	07-7995678 分機 5252	tzuping@kcg.gov.tw
高雄市政府民政局	廖英捷	07-7995678 分機 5257	warrickl@kcg.gov.tw
高雄市政府民政局	蘇信宏	07-7995678 分機 5258	jessesu@kcg.gov.tw
高雄市殯葬管理處	曾靖淇	07-3816316	jingchi@kcg.gov.tw
高雄市兵役處	尤良源	07-3373581	youdil2@kcg.gov.tw
高雄市鼓山戶政事務所	李德修	07-5510404	jamesli@kcg.gov.tw
高雄市左營戶政事務所	鄭玄明	07-5829803	jassua7@kcg.gov.tw
高雄市楠梓戶政事務所	李依純	07-3511895	e7382@kcg.gov.tw
高雄市新興戶政事務所	林倫旭	07-2364015	yiyo0904@kcg.gov.tw
高雄市苓雅戶政事務所	鍾玫宜	07-3302232	mable@kcg.gov.tw
高雄市前鎮戶政事務所	陳莠嬿	07-8115128	onlyr2@kcg.gov.tw
高雄市小港戶政事務所	翁玉如	07-8119784	rita1396@kcg.gov.tw
高雄市三民戶政事務所	張專明	07-3951246	t172052@kcg.gov.tw
高雄市鳳山戶政事務所	陳冠吾	07-7429784	cckity@kcg.gov.tw
高雄市岡山戶政事務所	吳鑫穎	07-6217389	hy0430@kcg.gov.tw
高雄市旗山戶政事務所	張宥嵐	07-6614461	youlan31@kcg.gov.tw
高雄市美濃戶政事務所	黃溥鈞	07-6812734	hpj0601@kcg.gov.tw
高雄市大寮戶政事務所	傅全佑	07-7817516	adi123@kcg.gov.tw
高雄市仁武戶政事務所	楊智欽	07-3711328	office@kcg.gov.tw
高雄市鳥松戶政事務所	曾裕仁	07-7316414	euntseng@kcg.gov.tw
高雄市路竹戶政事務所	林佩君	07-6962518	jjj12393@kcg.gov.tw
高雄市茄萣戶政事務所	張信慧	07-6902004	a1001215@kcg.gov.tw
高雄市梓官戶政事務所	黃富泰	07-6171538	ag9199@kcg.gov.tw

備註：本機關之所屬機關資通安全事件通報窗口異動，請立即通知本局資訊室修正。

2. 資通安全事件通報及應變小組

職務	職稱	姓名	電話	電子郵件
事件指揮官	副局長	蔡翹鴻	07-7995678#5021	a0623@kcg.gov.tw
新聞官	主任秘書	吳永揮	07-7995678#5026	yeonghui@kcg.gov.tw
執行秘書	主任	雒彬彬	07-7995678#5251	robin@kcg.gov.tw
情資及計畫組組長	股長	王子評	07-7995678#5252	tzuping@kcg.gov.tw
情資及計畫組組員	分析師	蘇信宏	07-7995678#5258	jessesu@kcg.gov.tw
情資及計畫組組員	管理師	廖英捷	07-7995678#5257	warrickl@kcg.gov.tw
情資及計畫組組員	資安廠商	沈國輝	02-29665138	shenneo@sdsgroup.com.tw
應變執行組組長	股長	王子評	07-7995678#5252	tzuping@kcg.gov.tw
應變執行組組員	分析師	蘇信宏	07-7995678#5258	jessesu@kcg.gov.tw
應變執行組組員	管理師	廖英捷	07-7995678#5257	warrickl@kcg.gov.tw
應變執行組組員	資安廠商	沈國輝	02-29665138	shenneo@sdsgroup.com.tw
應變執行組組員	區政科	陳育輝	07-7995678#5063	yiehway@kcg.gov.tw
應變執行組組員	宗禮科	謝雅玉	07-7995678#5113	monica724@kcg.gov.tw
應變執行組組員	自治科	陳俊豪	07-7995678#5078	ap2236@kcg.gov.tw
應變執行組組員	戶政科	張麗霜	07-7995678#5143	frost@kcg.gov.tw
應變執行組組員	基建科	陳文亮	07-7995678#5159	kxkomq@kcg.gov.tw
應變執行組組員	秘書室	盧致銘	07-7995678#5213	lewis@kcg.gov.tw
應變執行組組員	會計室	曾怡箋	07-7995678#5223	lg312@kcg.gov.tw
應變執行組組員	人事室	江淑芳	07-7995678#5172	beagle5@kcg.gov.tw
應變執行組組員	政風室	曾國裕	07-7995678#5092	guoyu@kcg.gov.tw
後勤調度組組長	股長	王子評	07-7995678#5252	tzuping@kcg.gov.tw
後勤調度組組員	分析師	蘇信宏	07-7995678#5258	jessesu@kcg.gov.tw

後勤調度組組員	管理師	廖英捷	07-7995678#5257	warrickl@kcg.gov.tw
後勤調度組組員	資安廠商	沈國輝	02-29665138	shenneo@sdsgroup.com.tw
財務行政組組長	會計室	吳芝穎	07-7995678#5229	j7291@kcg.gov.tw

3. 資通安全事件通報單

（機關名稱）

資通安全事件通報單

一、 遵照資通安全管理法，公務機關與特定非公務機關發生資安事件時，應於限定時間內辦理事件通報、損害控 制或復原通知，並於 完成事件損害控制或復原後一個月內完成資通安全事件調查、處理及改善報告。

二、 公務機關、公營事業或政府捐助之財團法人應至國家資通安全通報應變網站(http://www.ncert.nat.gov.tw）通報資安事件，若因故無法上網填報，可先填具本通報單以傳真或郵寄方式傳送至國家資通安全會報政府資通安全組， 俟網路連線恢復後 ，仍須至通報應變 網 站進行資安事件補登 作業 。

傳真專線：(02)27331655　　郵寄地址：台北市大安區 106 富陽街 116 號

諮詢專線：(02)27339922

三、資通安全事件通報單填寫注意事項如下：

1. ◎為必填項目。
2. 請依通報之資安「事件分類」填寫通報單，並依事件類別回傳通報單內容。
3. 事件通報的部分請回傳 P17-P19
4. 事件損害控制或復原的部分請根據事件分類回傳對應的頁碼
   (網頁攻擊 P20-P21 、非法入侵 P24-P25、阻斷服務 P28、
   設備異常 P30、其他 P32-P33)
5. 事件調查處理及改善報告的部分請根據事件分類回傳對應的頁碼
   (網頁攻擊 P22-P23 、非法入侵 P26-P27,P9-P11、阻斷服務 P29、
   設備異常 P31、其他 P34-P35)

【壹、事件通報】(通報階段)

◎填報時間：____年____月____日____時____分

STEP1. 請填寫事件相關基本資料

一、發生資通安全事件之機關(機構)聯絡資料：

◎ 機關(機構)名稱：_____◎審核機關名稱：_____

◎ 通報人：_____ ◎電話：_____ 傳真：_____

◎ 電子郵件信箱：_____

◎ 是否代其他機關(構)通報：□是，該單位名稱_____ □否

◎ 資安監控中心(SOC)： □無 □機關自行建置
□ 委外建置，該廠商名稱_____

◎ 資安維護廠商：_____

STEP2.請詳述事件發生過程

二、事件發生過程：

◎ 事件發現時間：____年____月____日____時____分

◎ 事件分類與異常狀況：(事件分類為單選項；異常狀況為複選項)

○網頁攻擊
□網頁置換 □惡意留言 □惡意網頁 □釣魚網頁
□網頁木馬 □網站個資外洩

○非法入侵
□系統遭入侵 □植入惡意程式 □異常連線 □發送垃圾郵件
□資料外洩

○阻斷服務(DoS/DDoS)
□服務中斷 □效能降低

○設備問題

□設備毀損 □電力異常 □網路服務中斷 □設備遺失

○其他：____年____月____日____時____分

◎ 事件說明及影響範圍

【請說明事件發生經過，如機關如何發現此事件、處理情形等】

_____
_____
_____
_____

_____

_____

◎ 是否影響其他政府機關 構 或重要民生設施運作：□是 □否

◎ 承上，影響機關 構 重要民生設施領域名稱：

□水資源 □能源 □通訊傳播 □交通 □銀行與金融
□緊急救援與醫院 □重要政府機關 □高科技園區

◎ 此事件通報來源： □自行發現 □警訊通知，發布編號：_____
□其他外部情資：_____

STEP3.評估事件影響等級

三、事件影響等級

◎ 請分別評估資安事件造成之機密性、完整性以及可用性衝擊：

*資安事件影響等級為機密性、完整性及可用性衝擊最嚴重者(數字最大者)

－機密性衝擊：(單選)

□一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭 洩漏(4 級)

□未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏(3 級)

□非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏(2 級)

□非核心業務資訊遭輕微洩漏(1 級)

□無資料遭洩漏(無需通報)

－完整性衝擊：(單選)

□一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改(4 級)

□未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心 資通系統遭輕微竄改(3 級)

□非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改(2 級)

□非核心業務資訊或非核心資通系統遭輕微竄改(1 級)

□無系統或資料遭竄改(無需通報)

－可用性衝擊：(單選)

□涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可

容忍中斷時間內回復正常運作(4 級)

□未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業 務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作(3 級)

□非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作 (2 級)

□非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響 (1 級)

□無系統或設備運作受影響(無需通報)

STEP4.評估事件影響等級

四、期望支援項目：

◎ 是否需要支援：

□是（請續填期望支援內容）□否（免填期望支援內容）

期望支援內容：（請勿超過 200 字）

_____

_____

_____

_____

【貳、損害控制或復原-網頁攻擊】(應變處置階段)

STEP5. 請填寫機關緊急應變措施-網頁攻擊(請回傳 P20-P21)

五、完成損害控制或復原

◎ 保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

□已保存遭入侵主機事件紀錄檔〈單選〉

〈□1 個月 □1-6 個月 □6 個月以上 □其他_____〉

□已保存防火牆紀錄〈單選〉

〈□1 個月 □1-6 個月 □6 個月以上 □其他_____〉

□已保存網站日誌檔〈單選〉

〈□1 個月 □1-6 個月 □6 個月以上 □其他_____〉

□已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共_____個

□其他保留資料或資料處置說明【如未保存資料亦請說明】

_____

_____

◎ 事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)，經分析已保存之紀錄，是否發現下列異常情形：

□異常連線行為【請列出異常 IP 與異常連線原因，如：存取後台管理頁面】

_____

_____

□異常帳號使用【請列出帳號並說明帳號權限 ，與判別準則，如非上班時間帳號異常登入 /登出】

_____

_____

□清查網頁目錄內容，網站內存在未授權之程式/檔案【請說明程式名稱或路徑、檔名】

_____

_____

□網站資料庫內容遭竄改

□發現資料外洩情況【如：異常打包資料，請說明外洩資料類型欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

_____

_____

□影響評估說明補充【請填寫補充說明】

_____

_____

◎ 封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)因應分析結果，執行處置措施：

□移除未授權存在之惡意網頁/留言/檔案 ，共____筆(必填)

【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】

_____

_____

□將異常外部 連線 IP 列入阻擋清單(必填)【請說明設定阻擋之資訊設備與阻擋之 IP，如無須阻擋，請填寫「無」】

_____

_____

□停用/刪除異常帳號(必填)【請說明停用/刪除之帳號，如無須刪除，請填寫「無」】

_____

_____

□移除網站外洩資料

□通知事件相關當事人，並依內部資安通報作業向上級呈報

□暫時中斷受害主機網路連線行為至主機無安全性疑慮

□已向搜尋引擎提供者申請移除庫存頁面〈複選〉

《□Google □Yahoo □Yam(蕃薯藤) □Bing □Hinet □其他搜尋引擎提供者___ 》

□修改網站程式碼，並檢視其他網站程式碼，完成日期_____

□重新建置作業系統與作業環境，完成日期_____

□應變措施補充說明【請填寫補充說明】

_____

◎ 應變處置綜整說明【請說明損害控制或復原之執行狀況】：

_____

_____

○已完成損害控制，未有擴大損害情形

○已完成損害控 制並復原，恢復資安事件造成的損害

完成損害控制或復原時間：____年____月____日____時____分

【參、調查、處理及改善報告-網頁攻擊】(結報階段)

STEP6.資安事件結案作業-網頁攻擊(請回傳 P22-P23)

六、 事件調查與處理

◎受害資訊設備數量：電腦總計____臺；伺服器總計____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址(Web-URL)(無；可免填) ：_____

◎作業系統名稱、版本：

□ Windows 系列 □ Linux 系列 □其他作業平台 版本：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎事件發生原因〈單選〉

〈□作業系統漏洞 □弱密碼 □應用程式漏洞 □網站設計不當

□人為疏失 □設定錯誤 □系統遭入侵 □其他_____〉

◎ 請簡述事件處理情況：

_____

_____

_____

◎ 補強措施〈複選〉

I.補強系統/程式安全設定

□已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密碼等)(必填)

□已完成評估變更受害主機中所有帳號之密碼(含本機管理者)(必填)

□已完成檢視更新受害主機系統與所有應用程式至最新版本(包含網站編輯管理程式，如： FrontPage)(必填)【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

_____

_____

□關閉網路芳鄰功能

□設定 robots.txt 檔，控制網站可被搜尋頁面

□已針對所有需要特殊存取權限之網頁加強身分驗證機制【請說明機制名稱或類別】

_____

□限制網站主機上傳之附件檔案類型【請說明附檔名】

□限制網頁存取資料庫的使用權限，對於讀取資料庫資料的帳戶身分及權限加以管制

□限制連線資料庫之主機 IP

□關閉 WebDAV(Web Distribution Authoring and Versioning)

II.資安管理與教育訓練

□重新檢視機關網路架構適切性

□機關內部全面性安全檢測

□加強內部同仁資安教育訓練

□修正內部資安防護計畫

◎ 其他相關安全處置【 請填寫相關處置、預定完成時程及成效追蹤機制 】

_____

_____

◎調查、處理及改善報告繳交(登錄結報)時間：

____年____月____日____時____分

【貳、損害控制或復原-非法入侵】(應變處置階段)

STEP5.請填寫機關緊急應變措施-非法入侵(請回傳 P24-P25)

五、 完成損害控制與復原

◎ 保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

□已保存遭受害主機事件紀錄檔〈單選〉

〈□1 個月 □1-6 個月 □6 個月以上 □其他_____〉

□已保存防火牆紀錄〈單選〉

〈□1 個月 □1-6 個月 □6 個月以上 □其他_____〉

□已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共_____個

□其他保留資料或資料處置說明【如未保存資料亦請說明】

_____

_____

◎ 事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)經分析已保存之紀錄，是否發現下列異常情形：

□異常連線行為【請列出異常 IP 與異常連線，如：存取後台管理頁面】

_____

_____

□異常帳號使用【請列出帳號並說帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

_____

_____

□發現資料外洩情況 【如：異常打包資料 請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

_____

_____

□影響評估說明補充【請填寫補充說明】

_____

_____

◎ 封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)因應分析結果，執行處置措施：

□移除未授權存在之 惡意網頁/留言/檔案/程式 ，共_____筆(必填)

【請說明程式名稱或路徑、檔名 如無須移除，請填寫「無」 】

_____

_____

□將可疑 IP/Domain Name 列入阻擋清單(必填)【請說明設定阻擋之資訊設備與阻擋之 IP，如無須阻擋，請填寫「無」】

_____

_____

□停用/刪除異常帳號(必填)【請說明停用/刪除之帳號，如無須移除，請填寫「無」】

_____

_____

□中斷受害主機網路連線行為至主機無安全性疑慮

□重新建置作業系統與作業環境 ，完成日期_____

□惡意程式樣本送交防毒軟體廠商，共_____個

□應變措施補充說明【請填寫補充說明】

_____

_____

◎ 應變處置綜整說明【請說明損害控制或復原之執行狀況】

_____

_____

○已完成損害控制，未有擴大損害情形

○已完成損害控制並復原，恢復資安事件造成的損害

完成損害控制或復原時間：____年____月____日____時____分

【參、調查、處理及改善報告-非法入侵】(結報階段)

STEP6.資安事件結案作業-非法入侵(請回傳 P26-P27)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計____臺；伺服器總計____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址(Web-URL)(無；可免填)：_____

◎作業系統名稱、版本：

□ Windows 系列 □ Linux 系列 □其他作業平台 版本：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎事件發生原因〈單選〉

〈□社交工程 □作業系統漏洞 □弱密碼 □應用程式漏洞 □網站設計不當
□系統遭入侵 □其他_____〉【請說明事件調查情況】

_____

_____

◎ 補強措施〈複選〉

I.補強系統/程式安全設定

□已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密碼等)(必填)

□已完成評估變更受害主機中所有帳號之密碼(含本機管理者)(必填)

□已完成檢視/更新受害主機系統與所有應用程式至最新版本 (必填)

【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

_____

_____

□關閉郵件伺服器 Open Relay 功能

□關閉網路芳鄰功能

II.資安管理與教育訓練

□重新檢視機關網路架構適切性

□機關內部全面性安全檢測

□加強內部同仁資安教育訓練

□修正內部資安防護計畫

◎ 其他相關安全處置【 請填寫相關處置、預定完成時程及成效追蹤機制 】

_____

_____

◎調查、處理及改善報告繳交(登錄結報)時間：

____年____月____日____時____分

【貳、損害控制或復原-阻斷服務(DoS/DDoS)】(應變處置階段)

STEP5.請填寫機關緊急應變措施-阻斷服務(DoS/DDoS)(請回傳 P28)

五、 完成損害控制與復原

◎ 保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

□已保存遭受害主機事件紀錄檔〈單選〉

〈□1 個月 □1-6 個月 □6 個月以上 □其他_____〉

□已保存防火牆紀錄〈單選〉

〈□1 個月 □1-6 個月 □6 個月以上 □其他_____〉

□已保存受攻擊主機封包紀錄〈□10 分鐘 □10-30 分鐘 □30-60 分鐘〉

□其他保留資料或資料處置說明【如未保存資料亦請說明】

_____

_____

◎ 事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)

□攻擊來源 IP 數量_____個

□確認遭攻擊主機用途【請說明主機用途】

_____

_____

□影響評估補充說明

_____

_____

◎ 封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)

□阻擋攻擊來源 IP(必填)【請說明設定阻擋之資訊設備與阻擋之 IP，如無須阻擋，請填寫「無」】

_____

_____

□調整網路頻寬

□聯繫網路服務提供業者（ISP）_____（請提供 ISP 業者名稱）

請其協助進行阻擋

□應變措施補充說明【請填寫補充說明】

_____

◎ 應變處置綜整說明【請說明損害控制或復原之執行狀況】

_____

_____

○已完成損害控制，未有擴大損害情形

○已完成損害控制並復原，恢復資安事件造成的損害

完成損害控制或復原時間：____年____月____日____時____分

【參、調查、處理及改善報告-阻斷服務(DoS/DDoS)】(結報階段)

STEP6.資安事件結案作業-阻斷服務(DoS/DDoS)（請回傳 P29）

六、事件調查與處理：

◎受害資訊設備數量：電腦總計____臺；伺服器總計____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址(Web-URL)(無；可免填)：_____

◎作業系統名稱、版本：

□ Windows 系列 □ Linux 系列 □其他作業平台 版本：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎ 補強措施〈複選〉

I.補強系統/程式安全設定

□限制同時間單一 IP 連線

□DNS 主機停用外部遞迴查詢

□已完成檢視/移除主機/伺服器不必要服務功能(必填)【請說明服務功能名稱 ，如無須移除，請填寫「無」】

_____

_____

□已完成檢視/更新受害主機系統與所有應用程式至最新版本（必填）

【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

_____

_____

II.資安管理與教育訓練

□重新檢視機關網路架構適切性

□修正內部資安防護計畫

◎ 其他相關安全處置【 請填寫相關處置、預定完成時程及成效追蹤機制 】

_____

_____

◎調查、處理及改善報告繳交(登錄結報)時間：

____年____月____日____時____分

【貳、損害控制或復原-設備異常】(應變處置階段)

STEP5. 請填寫機關緊急應變措施-設備異常(請回傳 P30)

◎ 保留受害期間之相關設備紀錄資料

□其他保留資料或資料處置說明【如未保存資料亦請說明】

_____

_____

◎ 事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)

□評估設備影響情況

〈□無資料遭損毀

□資料損毀，但可由備份檔案還原

□資料損毀，且資料無法復原

□資料損毀，僅可復原部分資料____%〉

□遺失設備存放資料性質說明

〈個人敏感性資料、機密性資料、非機敏性資料，請說明內容〉

_____

_____

□影響評估補充說明

_____

_____

◎ 封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)

□毀損資料/系統已恢復正常運作

□完成系統復原測試

□通知事件相關當事人，並依 內部資安通報作業向上級呈報**【如遺失設備存有敏感資料，此選項為必填】**

□應變措施補充說明【請填寫補充說明】

_____

_____

◎ 應變處置綜整說明【請說明損害控制或復原之執行狀況】

_____

_____

○已完成損害控制，未有擴大損害情形

○已完成損害控制並復原，恢復資安事件造成的損害

完成損害控制或復原時間：____年____月____日____時____分

【參、調查、處理及改善報告-設備異常】(結報階段)

STEP6.資安事件結案作業-設備異常(請回傳 P31)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計____臺；伺服器總計____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址(Web-URL)(無；可免填)：_____

◎作業系統名稱、版本：

□ Windows 系列 □ Linux 系列 □其他作業平台 版本：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎事件發生原因〈單選〉

〈□設定錯誤 □設備毀損 □系統遭入侵 □電力供應異常 □人為疏失

□其他_____〉【請說明事件調查情況】

◎ 補強措施〈複選〉

I.補強系統/程式安全設定

□檢視資訊設備使用年限

II.資安管理與教育訓練

□重新檢視機關網路架構適切性

□機關內部全面性安全檢測

□加強內部同仁資安教育訓練

□修正內部資安防護計畫

◎ 其他相關安全處置【 請填寫相關處置、預定完成時程及成效追蹤機制 】

_____

_____

◎調查、處理及改善報告繳交(登錄結報)時間：

____年____月____日____時____分

【貳、損害控制或復原-其他】(應變處置階段)

STEP5.請填寫機關緊急應變措施-其他(請回傳 P32-P33)

五、 完成損害控制與復原

◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

□已保存遭入侵主機事件檢視器〈單選〉

〈□1 個月 □1-6 個月 □6 個月以上 □其他_____〉

□已保存防火牆紀錄〈單選〉

〈□1 個月 □1-6 個月 □6 個月以上 □其他_____〉

□已保存未授權存在之惡意網頁/留言/檔案/程式樣本〉，共_____個

□其他保留資料或資料處置說明【如未保存資料亦請說明】

_____

_____

◎ 事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明) 經分析已保存之紀錄，是否發現下列異常情形：

□異常連線行為【請列出異常 IP 與異常連線，如：存取後台管理頁面】

_____

_____

□異常帳號使用【請列出帳號並說帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

_____

_____

□發現資料外洩情況 【如：異常打包資料 請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

_____

_____

□影響評估說明補充【請填寫補充說明】

_____

_____

◎ 封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)

□移除未授權存在之惡意網頁/留言/檔案/程式 ，共_____筆(必填)

【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】

_____

_____

□將可疑 IP/Domain Name 列入阻擋清單(必填)【請說明設定阻擋之資訊設備與阻擋

之 IP，如無須阻擋，請填寫「無」】

_____

_____

□停用/刪除異常帳號(必填)【請說明停用/刪除之帳號，如無須移除，請填寫「無」】

_____

_____

□暫時中斷受害主機網路連線行為至主機無安全性疑慮

□重新建置作業系統與作業環境 ，完成日期_____

□惡意程式樣本送交防毒軟體廠商，共_____個

□應變措施補充說明【請填寫補充說明】

_____

_____

◎ 應變處置綜整說明【請說明損害控制或復原之執行狀況】

_____

_____

○已完成損害控制，未有擴大損害情形

○已完成損害控制並復原，恢復資安事件造成的損害

完成損害控制或復原時間：____年____月____日____時____分

【參、調查、處理及改善報告-其他】(結報階段)

STEP6.資安事件結案作業-其他(請回傳 P34-P35)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計____臺；伺服器總計____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址(Web-URL)(無；可免填)：_____

◎作業系統名稱、版本：

□ Windows 系列 □ Linux 系列 □其他作業平台 版本：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎事件發生原因〈單選〉

〈□社交工程 □作業系統漏洞 □弱密碼 □應用程式漏洞 □網站設計不當

□人為疏失 □設定錯誤 □設備毀損 □系統遭入侵 □電力供應異常

□其他_____〉【請說明事件調查情況】

_____

_____

◎ 補強措施〈複選〉

I.補強系統/程式安全設定

□已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密碼等)(必填)

□已完成評估變更受害主機中所有帳號密碼之必要性(含本機管理者)(必填)

□已完成檢視/更新受害主機系統與所有應用程式至最新版本(必填)

【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

□關閉網路芳鄰功能

II.資安管理與教育訓練(複選)

□重新檢視機關網路架構適切性

□機關內部全面性安全檢測

□加強內部同仁資安教育訓練

□修正內部資安防護計畫

◎ 其他相關安全處置【 請填寫相關處置、預定完成時程及成效追蹤機制 】

_____

_____

◎調查、處理及改善報告繳交(登錄結報)時間：

____年____月____日____時____分