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：110 年 6 月 16 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

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、事件通報窗口及緊急處理小組

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）及廖管理師英捷（07-7995678 分機 5257)。

(二)各機關資通安全事件通報窗口。

二、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。

三、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。

四、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。

五、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。

六、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，副轉知本局，由本局資通安全長成立緊急處理小組，立即協助進行處理；接獲本機關所屬機關或受託廠商所通報之資通安全事件時，

亦同。

七、緊急處理小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。

八、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

本機關之權責人員或緊急處理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。

(二)除事件之等級外，權責人員或緊急處理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。

(三)本機關權責人員或緊急處理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。

(四)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。

(五)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。

(六)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。

(七)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。

(八)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。

(九)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。

二、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。

三、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。

陸、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緊急處理小組，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。

柒、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前項之報告，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。

捌、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。

玖、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。

拾、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
高雄市殯葬管理處	彭韜	07-3816316	peng0730@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	呂百雅	07-6217389	re20000@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	劉榮豐	07-6812734	fon180@kcg.gov.tw
高雄市大寮戶政事務所	黃月英	07-7817516	s182630@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 P2-P4
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 P2-P6 、非法入侵 P2-P4,P9-P10、阻斷服務 P2-P4,P12-P13、設備異常 P2-P4,P14、其他 P2-P4,P16-P17）

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 P2-P8 、非法入侵 P2-P4,P9-P11、阻斷服務 P2-P4,P12-P13、設備異常 P2-P4,P14-P15、其他 P2-P4,P16-P18）

【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 P2-P6)

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 P2-P8)

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 P2-P4、P9-P10)

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 P2-P4、P10-P11)

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 P1-P3、P11-P12)

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 P1-P3、P11-P12)

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 P1-P3、P13-P14)

◎ 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 P1-P3、P13-P14)

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 P1-P3、P15-P17)

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 P1-P3、P15-P17)

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