

臺北市立景美女子高級中學資通安全事件通報應變程序

壹、目的

臺北市立景美女子高級中學(以下簡稱本校)為遵照資通安全管理法第14條及本校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

發生於本校之事件，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

- 一、本校所屬人員於發現資通安全事件時，應依本程序執行通報及應變事務。
- 二、本校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定之方式進行結案登錄作業。

肆、事件通報窗口及緊急處理小組

- 一、臺灣學術網路資通安全事件委託由臺灣學術網路危機處理中心之教育機構資安通報應變小組(簡稱通報應變小組)負責，聯繫資訊如下：
聯絡電話：(07)525-0211
網路電話：98400000
電子郵件：service@cert.tanet.edu.tw
- 二、本校應至少指派2位以上資安聯絡人員，並於「教育機構資安通報應變平台」(<https://info.cert.tanet.edu.tw>)登錄相關聯絡資料，如有異動亦應立即上網更新。
- 三、本校之資通安全事件通報窗口及聯繫專線為：
資訊組 02-29368847#251
圖書館 02-29368847#225
- 四、本校應以適當方式使教職員明確知悉通報窗口及聯絡方式。
- 五、本校所屬人員知悉資通安全事件後，應立即至教育機構資安通報平台(<https://info.cert.tanet.edu.tw>)通報登錄資安事件細節、影響等級及支援申請等資訊。
- 六、本校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。
- 七、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。
- 八、事件經初步判斷認為可能屬重大(第「三」級、第「四」級)資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立緊急處理小組，立即協助進行處理；接獲本校所屬

分校（機關）或受託廠商所通報之資通安全事件時，亦同。

九、緊急處理小組成員由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。

十、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、判定事件等級之流程及權責

本校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：

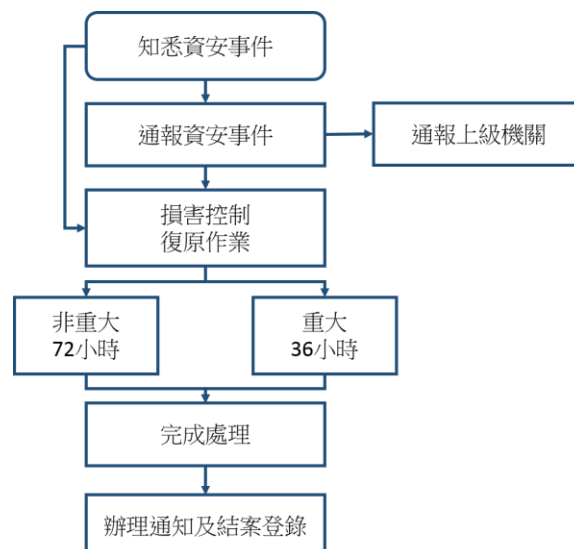
1. 事件涉及核心業務之資訊與否。
2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。
3. 事件所涉資訊是否屬於敏感資訊或一般公務機密。
4. 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。
5. 事件其他足以影響資通安全事件等級之因素。

二、除事件之等級外，本校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、本校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上級或監督機關及行政院所指定或認可之方式，進行事件通報。

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，並於事由解除後，依原方式補行通報。



陸、應變程序

一、事件發生前之防護措施規劃

本校應於平時妥善實施資通安全維護計畫，並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。

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. 重大(第「三」級、第「四」級)資安事件相關鑑識及其他調查作業。
 4. 重大(第「三」級、第「四」級)資安事件之調查與處理及改善報告之方式。
 5. 重大(第「三」級、第「四」級)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，本校應於知悉事件後72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，本校應於知悉事件後36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)本校完成資安事件處理後，須至教育機構資安通報平台填報資安事件處理辦法及完成時間。

柒、重大(第「三」級、第「四」級)資安事件後之復原、鑑識、調查及改善機制

- 一、本校若發生重大(第「三」級、第「四」級)資通安全事件時，於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、重大(第「三」級、第「四」級)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、本校應向所隸屬之上級機關及教育部提出前項之報告，以供監督與檢討。

捌、紀錄留存及管理程序之調整

- 一、本校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「教育機構資安通報平台」上填報完整之紀錄，該平台事件通報應變紀錄

由通報應變小組於年度彙整後，提交至本部資訊及科技教育司覆核備查。

- 二、本校於完成資通安全事件之通報及應變程序後，應依據實際處理之情形，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、本校應配合教育部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、本校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。
 - (二) 資安事件通報及應變
 - (三) 網路攻防
 - (四) 情境演練
 - (五) 其他資安演練

資通安全事件通報單

政府機關(構)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，惟待網路連線恢復後仍需上網補登通報。

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

注意事項

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 P1-P3，事件通報並結案的部分請根據事件分類回傳對應的頁碼(網頁攻擊 P1-P7、非法入侵 P1-P3,P8-P10、阻斷服務 P1-P3,P11-P12、設備異常 P1-P3,P13-P14、其他 P1-P3,P15-P17)

◎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：_____ ◎主管機關名稱：_____

◎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：

◎事件發生時間：____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：_____

◎事件說明及影響範圍：

◎是否影響其他政府機關(構)或重要民生設施運作：是 否

◎此事件通報來源：自行發現 警訊通知，發布編號：_____

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)

- 國家機密資料遭洩漏(4 級)
- 密級或敏感公務資料遭洩漏(3 級)
- 核心業務(含關鍵資訊基礎設施)一般資料遭洩漏(2 級)
- 非核心業務一般資料遭洩漏(1 級)
- 無資料遭洩漏(無需通報)

—完整性衝擊：(單選)

- 關鍵資訊基礎設施系統或資料遭嚴重竄改(4 級)
- 核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改(3 級)
- 非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改(2 級)
- 非核心業務系統或資料遭竄改(1 級)
- 無系統或資料遭竄改(無需通報)

—可用性衝擊：(單選)

- 關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作(4 級)
- 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(3 級)
- 非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(2 級)
- 非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(1 級)
- 無系統或設備運作受影響(無需通報)

Step4.評估是否需要外部支援

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）

Step5.請填寫機關緊急應變措施-網頁攻擊(請回傳 P1-P7)

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〉

《GoogleYahooYam(蕃薯藤) BingHinet

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】

STEP6.資安事件結案作業-網頁攻擊(請回傳 P1-P7)

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【請填寫其他安全處置】

◎完成修復時間：____年____月____日____時____分

Step5.請填寫機關緊急應變措施-非法入侵(請回傳 P1-P3、P8-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】

 影響評估補充說明【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】

Step6.資安事件結案作業-非法入侵(請回傳 P1-P3、P8-P10)

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〈複選〉

- 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(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【請填寫其他安全處置】

◎已解決時間：____年____月____日____時____分

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】

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〈複選〉

- 限制同時單一 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〈複選〉

- 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【請填寫其他安全處置】

◎已解決時間：____年____月____日____時____分

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】

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〈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【請填寫其他安全處置】

◎已解決時間：____年____月____日____時____分

Step5.請填寫機關緊急應變措施-其他(請回傳 P1-P3、P15-P17)

◎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】

- 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】

- 影響評估補充說明【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】

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〈複選〉

- 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【請填寫其他安全處置】

◎已解決時間：____年____月____日____時____分