內政部建築研究所資安事件通報應變標準作業程序

內政部建築研究所103年7月21日第15次所務會議通過

一、前言

本所為有效掌握資通訊及網路系統遭受破壞、不當使用等資安事件時，能迅速通報及緊急應變處置，並在最短時間內回復，以確保所內各項業務之正常運作，特參考「國家資通安全通報應變作業綱要」訂定本程序。

二、本所資安事件通報應變標準作業程序

依「國家資通安全通報應變作業綱要」規定，資安事件影響等級分4個級別，由重至輕分為「4級」、「3級」、「2級」及「1級」。進行資安事件處理時，「4級」、「3級」須於36小時內復原或完成損害管制；「2級」、「1級」須於72小時內復原或完成損害管制。

（一）各組室經由綜合規劃組通知有資安事件時，應依下列程序辦理：

1. 各組室於發生資安事件時，應即向該組室主管報告，並於半小時內填寫本所「資安事件通報應變標準作業程序單」（附件1）送綜合規劃組，說明該次事件相關資料及處理方法。

2. 綜合規劃組接獲通報單後，應即判定該事件之影響等級，屬風險性高者，應依本程序第(二)點辦理，其餘則依本所內部程序上報結案。

（二）本所經由國家資通安全會報技術服務中心或本部資訊中心通知發生資安全事件時，依下列程序辦理：

1. 綜合規劃組應即向本所資訊安全長或其職務代理人報告，並須 於1小時內至「國家資通安全通報應變網站」（https://www.ncert.nat.gov.tw)登錄通報，同時填寫「內政部暨所屬機關資通安全事件通報單」（附件2）經簽報核示後，以傳真方式向本部「資通安全處理小組」通報。

2. 資安事件處理時限，應按事件影響等級依前述「國家資通安全通報應變作業綱要」規定辦理。

3. 資安事件處理完成後，應另填寫「內政部暨所屬機關資通安全事件解除通報單」（附件2），並經簽報核示後，以傳真方式向本部「資通安全處理小組」辦理結案，同時至「國家資通安全通報應變網站」登錄資安事件處理辦法及完成時間。

三、本所資安事件通報承辦單位與各組聯絡窗口名單：

（一）綜合規劃組承辦單位窗口：

1. 阮文昌（02-89127890分機321、ivan@abri.gov.tw）

2. 嚴偉倫（02-89127890分機322、wlyen@abri.gov.tw）

（二）安全防災組窗口：

白櫻芳（02-89127890分機251、yingfang@abri.gov.tw）

（三）工程技術組窗口：

劉青峰（02-89127890分機305、xbr@abri.gov.tw）

（四）環境控制組窗口：

陳麒任（02-89127890轉281、chiren@abri.gov.tw）

（五）若聯絡窗口名單有異動，請即時通知承辦單位更新名單。

四、本程序經所務會議通過後實施，修正或廢止時亦同。

附件 1

內政部建築研究所
資安事件通報應變標準作業程序單

通報時間：_____年_____月_____日_____時_____分

一、發生資安事件單位資料：

組室名稱：_____ 聯絡人：_____ 分機：_____

二、資安事件通報事項：

1.事件發生時間：_____年_____月_____日_____時_____分

2.事件說明:

◎事件分類：□非法入侵 □感染病毒 □服務中斷 □其他 _____

◎破壞程度：□系統當機 □資料庫毀損 □網頁遭篡改 □其他_____

◎影響範圍及損失評估：_____

_____

3.設備資料：

◎IP 位址(IP Address)：內部 IP：_____外部 IP：_____

◎網際網路位置(Web-URL)：_____

◎設備廠牌、機型：_____

◎作業系統名稱、版本：_____

◎已裝置之安全機制：□防火牆□防毒軟體□其他_____

◎維護廠商：□無□有：_____

4.解決方式：□自行解決□請綜合規劃組支援□其他_____

通報組室、實驗中心	
承辦人	單位主管或其職務代理人

以下資料，由綜合規劃組填寫

本次資安事件處理方式：

□通報國家資通安全通報應變網站

□通報本部資通安全處理小組

□更新防毒軟體病毒碼、修補作業系統及應用程式漏洞，並進行掃描以清除病毒、漏洞

□更新入侵偵測系統攻擊碼與防火牆規則

□通報單位已自行處理完畢，所內結案

□其他：_____

解決時間：_____年_____月_____日_____時_____分

綜合規劃組	資訊安全長或其職務代理人

附件 2　　內政部暨所屬機關資通安全事件　　□ 通報單

□ 解除通報單

填報時間：____年____月____日____時____分　　編號：

一、發生資通安全事件之機關聯絡資料：

機關名稱：_____　通報人：_____

電話：_____　E-Mail：_____　傳真：_____

二、機關發生資通安全事件基本資訊：

1.事件發生時間：_____年_____月_____日_____時_____分

2.設備資料：

◎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：

□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: _____

◎資安監控中心(SOC)：

○無 ○機關自行建置 ○委外建置_____(請提供廠商名稱)

◎受害系統是否通過資安管理認證(ISMS)：○是 ○否

◎資安維護廠商：_____(請提供廠商名稱)

3.資通安全事件資料：

◎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：

A.機密性衝擊：(單選)

○國家機密資料遭洩漏

○密級或敏感資料遭洩漏

○核心業務（含關鍵資訊基礎設施）一般資料遭洩漏

○非核心業務一般資料遭洩漏

○無資料遭洩漏

綜合評估等級
○ 4級，重大資安事件
○ 3級，重要資安事件
○ 2級，一般資安事件
○ 1級，輕微資安事件

B.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

○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

○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

○非核心業務系統或資料遭輕微竄改

○無系統或資料遭竄改

C.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

○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

○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

○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

○無系統或設備運作受影響

◎事件分類與異常狀況(單選)：

○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

○設備異常

□設備毀損 □電力異常

○其他 _____

◎事件說明：_____

◎是否影響其他政府機關(構)或重要民生設施運作：

◆通報機關判斷：○ 是 ○ 否

◎此事件通報來源:

○自行發現

○警訊通知 □資安訊息警訊(ANA) □資安預警警訊(EWA) □網頁攻擊警訊(DEF)
□入侵事件警訊(INT) 發布編號 ：_____

◎應變措施

◎保留受害期間之相關設備紀錄資料：_____

◎事故分析與影響評估：_____

◎封鎖、根除及復原：_____

三、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：_____

四、資安事故結案作業：

◎事故發生原因：_____

◎補強措施：_____

◎其他相關安全處置：_____

五、完成修復時間：_____年____月____日_____時_____分

通報機關		主管機關	
承辦人	資訊安全長或授權人	承辦人	資訊安全長或授權人

備註：

一、發生資通安全事件時，須填妥本表進行內部通報，通報機關資訊安全長核示後，以傳真方式向本部「資通安全處理小組」通報。

二、事件影響等級達4、3級時，本通報單將陳報本部資訊安全長核定。事件影響等級達2、1級時，本通報單將陳報本部資訊中心主管核定。

三、本部緊急聯絡電話：(02) 25132255、(02) 25132254、(02) 25132257。傳真電話：(02) 25132262。

四、授權人須科長【不含】以上或課長【不含】以上