真理大學資安事件通報與處理作業原則

民國 104.06.08 資通安全管理委員會訂定

第一條 目的及依據

為因應資訊化社會網路之普及應用，建立起完善之資通安全防護措施，以避免遭受電腦駭客入侵或受病毒感染，在資訊安全事件發生時，能迅速依程序進行通報，並採取必要之應變措施與建立事件學習機制，以降低事件所造成之損害，故擬定此作業程序。資安通報處理流程依據『教育機構資通應變手冊』訂立，規範依實際作業需求訂定之。

第二條 資安事件訊息來源

一、 教育機構資安通報平台，以手機簡訊及 Mail 通知資安連絡人。

二、 教育部資訊及科技教育司，以 E-mail 通知。

三、 警察局來函，以電子公文管理系統或實體紙本公文傳遞。

四、 校園內部防火牆偵測。

第三條 資安事件分類

一、INT(入侵攻擊)

- 系統入侵(資訊設備遭惡意使用者入侵)
- 對外攻擊(對外部主機進行攻擊行為)
- 針對性攻擊(針對特定個人的資訊洩漏與身分盜取)
- 散播惡意程式(主機對外進行惡意程式散播)
- 中繼站(主機成駭客之中繼站，接收惡意程式連線)
- 社交工程攻擊(帳號遭盜用對外發動社交工程攻擊)
- Spam(資訊設備從事 Spam Mail 散播行為)
- C&C(主機疑似為駭客之 Botnet C&C Server)
- Bot(資訊設備疑似成為駭客所控制之 Botnet 成員)
- 其它類型的入侵攻擊

二、 DEF(網頁攻擊)

- 惡意網頁(網頁遭駭客置換或放置不當內容)
- 惡意留言(網頁遭駭客放上惡意留言)
- 網頁置換(網頁遭駭客置換)
- 釣魚網站(主機遭駭客置入釣魚網站)
- 其它類型的網頁攻擊

第四條　資安等級區分

資訊安全事件依影響等級區分為 4 個級別，由重至輕分別為「4 級」、「3 級」、「2 級」及「1 級」。

4 級事件，符合下列任一情形者：

- 機密資料遭洩漏。
- 關鍵業務系統或資料遭嚴重竄改。
- 關鍵業務系統運作停頓，無法於可容忍中斷時間內回復正常運作。

3 級事件，符合下列任一情形者：

- 敏感資料遭洩漏。
- 關鍵業務系統或資料遭竄改。
- 關鍵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。

2 級事件，符合下列任一情形者：

- 限閱等級資料之關鍵業務系統或資料遭洩漏。
- 關鍵業務系統或資料遭輕微竄改。
- 關鍵業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

1 級事件，符合下列任一情形者：

- 非關鍵業務系統或資料遭洩漏。
- 非關鍵業務系統或資料遭竄改。
- 非關鍵業務運作遭影響或短暫停頓可立即修復。

第五條　資安事件處理方式

一、　依據資安事件訊息來源，電子計算機中心(以下簡稱本中心)判斷 IP 是否為本校所使用，確認為本校 IP 後，中心會視主機情形及攻擊類型判別是否於第一時間內封鎖其 IP，並通知發生資訊安全事件之權責單位，立即填寫「資訊安全事件報告單」，待權責單位處理完成應變措解決問題後，本中心再行放行通網動作。

二、　本中心若檢測到相關之校內資安事件，會以此作業原則做相關因應處理之方式。

三、　為保護校內人員個資避免爭議，警方來函須與該單位網管協助查證過後，IP 使用人瞭解涉及資安事件之實情，再配合提供資訊。

四、　若教育部資訊及科技教育司通知或警察局來函直接聯絡發生資訊安全事件之權責單位，務必回報本中心，並填寫「資訊安全事件報告單」以利本校校內資安事件之處理。

五、　通報國家資通安全會報：

1、2 級資安事件屬一般事件，事件處理須於 72 小時內完成。

3、4 級資安事件屬重大事件，事件處理須於 36 小時內完成。

第六條　此作業原則經資通安全委員會議通過，陳請校長核定後實施，修正時亦同。