資訊安全事件報告單					
文件編號	YUNTECH-ISMS-D-041	機密等級	限閱	版次	2.2

紀錄編號：_____　　填　表　日　期　：　年　月　日

通報單位聯絡資料			
單位名稱		通 報 人	
電　　話		電子郵件	

資訊安全事件通報事項	
發生時間	年　月　日　時　分
通報時間	年　月　日　時　分
事件分類	◎INT(入侵攻擊) □ 系統被入侵(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) □ 電子郵件社交工程攻擊(帳號遭盜用對外發動社交工程攻擊) □ 垃圾郵件(Spam)(資訊設備從事 Spam Mail 散播行為) □ 命令與控制伺服器(C&C)(主機疑似為駭客之 Botnet C&C Server) □ 殭屍電腦(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：_____ ◎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) □ 釣魚網頁(主機遭駭客置入釣魚網頁) □ 個資外洩(主機遭個資外洩) □ 其它類型的網頁攻擊
設備資料	IP 位址（無；可免填）： Web 位址（無；可免填）： 設備廠牌、機型： 作業系統名稱、版本： 已裝置之安全機制： 防毒軟體(名稱/版本)：　　防火牆(名稱/版本)： ＩＰＳ／ＩＤＳ(名稱/版本)：　　作業系統(名稱/版本)：

資訊安全事件資料					
資安事件判斷	□4 級	□3 級	□2 級	□1 級	□資安預警
破壞程度	□系統當機	□資料庫毀損	□網頁遭篡改	□其他	
事件說明					

資訊安全事件報告單					
文件編號	YUNTECH-ISMS-D-041	機密等級	限閱	版次	2.2

可能影響範圍及損失評估	
緊急應變措施	

期望支援項目
□ 是，期望支援方式： □ 電話告知 □ Email 告知 □ 否：通報單位自行解決
解決辦法
解決時間 ____年____月_____日____時____分
回覆通報時間 ____年____月_____日____時____分

權責（事件）單位		會辦單位	資訊中心		
承辦人	單位主管		資安承辦人	組長	主任

通報或諮詢資安事件，聯繫資訊如下：
資訊中心網路組電話：(05)5342601＃2655、2652 傳真：(05)5312044

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」、「3」、「2」及「1」級。

1、 4 級事件，符合下列任一情形者：
- 1.1 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。
- 1.2 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。
- 1.3 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。

2、 3 級事件，符合下列任一情形者：
- 2.1 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。
- 2.2 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。
- 2.3 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、 2 級事件，符合下列任一情形者：
- 3.1 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。
- 3.2 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。
- 3.3 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。

4、 1 級事件，符合下列任一情形者：
- 4.1 非核心業務資訊遭輕微洩漏。

4.2 非核心業務資訊或非核心資通系統遭輕微竄改。
4.3 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。

5、 資安預警，凡屬有待受害單位進行確認之資安事件皆屬於資安預警事件。