

環球科技大學

資訊安全事件/事故處理單

表單編號	ISMS-04-035	機密等級	一般	版本	4.3
------	-------------	------	----	----	-----

資訊安全事件通報單(ISMS-04-034)事件編號：

文件編號：

1. 資安事件簡述(圖書資訊處填寫)

檢附： 檢舉函 網路流量記錄 其他_____

發生日期： 年 月 日 時間：

IP/帳號： (所屬單位：) 網路卡號：

發現方式： 校內偵測 校內外單位檢舉 教育部通知

事件類別： SPAM Attack 設備故障 個資外洩 侵犯智慧財產權 其他：_____

事件說明：_____

影響等級：0 1 2 3 4 其他：_____

應變措施： 停用網路 停用帳號 更改密碼 其他：_____

承辦人： 分機：

資訊安全組組長： 執行秘書：

處理完畢 請 敬會_____核定 送回圖書資訊處(本欄由資訊安全組組長填寫)

2. 事件調查(所屬單位處理)

所屬單位：

請說明該事件發生之原因和處理情形，以及防範補強措施。

該 IP/帳號使用者為_____ 姓名：_____ 學號或員工代號：_____ 電話：_____

使用者簽名：_____

※ 請協助查明上述 IP 之使用者，並確認是否為本人所為，若涉及侵犯智慧財產權或情節重大者，會請會辦單位依相關規定處理。

承辦人： 分機： 日期：

二級主管(或導師)：_____ 單位主管(或系所主任)：_____

※ 配合教育部訂定 7 天內回報處理結果，請於 月 日前完成，請敬會會辦單位或送回圖書資訊處。

3. 核定(會辦單位處理)

會辦單位：

承辦人： 分機： 日期： 單位主管：

※ 配合教育部訂定 7 天內回報處理結果，會辦單位請於 月 日前完成，送回圖書資訊處以利作業。

4. 結案(圖書資訊處處理)

是否問題解決與解除限制？是，已於 月 日解決與解除 否

是否轉送副本給秘書處？是，已於 月 日送出 否

是否需要回覆處理結果？是，已於 月 日回覆 否

承辦人：

資訊安全組組長： 執行秘書：

注意事項：

- 一. 環球科技大學(以下簡稱本校)資訊安全事件/事故處理單(以下簡稱本單)乃依據臺灣學術網路指導單位所制定之『校園網路使用規範』、『臺灣學術網路各級學校資通安全通報應變作業程序』、『學術網路保護智慧財產權之相關措施』與本校『校園網路使用規範』制定並進行網路事件流程管控。
- 二. 當圖書資訊處(以下簡稱本處)接獲臺灣學術網路管理單位通知、外部單位檢舉或經本處網路流量數據判別有攻擊或不正常流量行為時，將立即中斷事由者網路使用權。
- 三. 請事由者在接到本處通知後，依所附之舉發事證進行檢測處理。處理完後請填妥應填之欄位後送至會辦單位或圖書資訊處(存誠樓 MA308)。
- 四. 請各階段處理者務必簽名，以示此階段處理完畢。
- 五. 表單繳回後需 1~3 個工作天完成解除設定(若為臺灣學術網路管理單位來函者，尚需等待區網中心回覆處理，處理時間可能會較長)。
- 六. 依教育部資科司規定疑似違規 IP 需列入追蹤三個月。
- 七. 如故意使用工具更改 IP 或 Mac Address 逃避，經查獲後將送校方依校規處理。若因此而引發檢調單位調查，將有可能背負法律責任。
- 八. 若有相關問題請至本處資訊安全維護組或來電#2901~#2907 洽詢。
- 九. 請尊重智慧財產權，臺灣學術網路已建立偵測 P2P 監控機制管理違反智慧財產權事宜，請勿以身試法。
- 十. 請定期對使用電腦中的作業系統及軟體進行更新，並請安裝防毒軟體(需定期更新病毒碼)保護個人電腦安全，以杜絕駭客利用漏洞侵入電腦進行資料竊取或植入木馬成為攻擊他人電腦系統之跳板，如有需要亦可安裝個人防火牆。

影響等級說明：

- 『4』級：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。
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。
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。
- 『3』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。
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。
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。
- 『2』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。
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。
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。
- 『1』級：非核心業務資訊遭輕微洩漏。
非核心業務資訊或非核心資通系統遭輕微竄改。
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。
- 『0』級：違反校園網路使用規範。(不須通報教育機構資安通報平台)

其它說明：

- 一. 本表單需配合【資訊安全事件通報單(ISMS-04-034)】方得進行此項作業
- 二. 處理文件編號請依 ISMS-02-001 資訊安全文件與紀錄管理程序第 5.1.4 之規定為原則