基隆市武崙國中資訊安全通報事件處理流程

**資訊安全事件包括：系統被入侵、對外攻擊、針對性攻擊、散播惡意程式、中繼站、電子郵 件社交工程攻擊、垃圾郵件、命令或控制伺服器、殭屍電腦、惡意網頁、惡意留言、網頁置換、 釣魚網頁、個資外洩以及通訊中斷等。 本校資訊安全事件等級，由輕微至嚴重區分等級如下：**

1. 符合下列任一情形者，屬 0 級事件：

(1) 未確定事件或待確認工單:來自不同計畫所使用新型技術(A-SOC， miniSOC,… )所產 生之工單，但其正確性有待確認。

 (2) 其他單位所告知教育部所屬單位所發生未確定之資安事件。

 (3) 教育部及區、市網路中心檢舉信箱通告之資安事件。

2. 符合下列任一情形者，屬 1 級事件：

 (1) 非核心業務資料遭洩漏。

(2) 非核心業務系統或資料遭竄改。

(3) 非核心業務運作遭影響或短暫停頓。

3. 符合下列任一情形者，屬 2 級事件：

 (1) 非屬密級或敏感之核心業務資料遭洩漏。

(2) 核心業務系統或資料遭輕微竄改。

 (3) 核心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。

4. 符合下列任一情形者，屬 3 級事件：

 (1) 密級或敏感公務資料遭洩漏。

(2) 核心業務系統或資料遭嚴重竄改。

(3) 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。

5. 符合下列任一情形者，屬 4 級事件：

(1) 國家機密資料遭洩漏。

(2) 國家重要資訊基礎建設系統或資料遭竄改。

 (3) 國家重要資訊基礎建設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。

本校任何人於校內發現異常情況或疑似資安事件，應立即向資訊組長通報，資訊組長儘速處理並研判事件等級。資訊組長當發生研判事件等級 3（含）以上之事件，應立即通報資訊業務主管及校長，並以 電話聯絡教育局(處)資訊安全管理單位，由校長儘快召集會議研商處理的方式。(資安事件通報

程序，附件 1) 本校發生內部無法處理之資通安全事件，應通報基隆市市網

中心協助處理。

資安通報依情報來源分為「告知通報」與「自行通報」，若收到「告知

通報」事件通知，由資 安業務承辦人登入教育機構資安通報平台，完成通報

及應變作業。 資安事件須於發生後 1 小時內進行通報，0、1、2 級事件於事

件發生後 72 小時內處理完 成並結案(包括通報與應變)，3、4 級事件於事件

發生後 36 小時內完成並結案。

資安發生緊急聯絡資訊

|  |  |  |  |
| --- | --- | --- | --- |
| 資安業務承辦人 | 資訊組長 | 李福祉 | 24342456#12 |
| 資安業務 | 教務主任 | 賴昱瑄 | 24342456#10 |
| 資安長 | 校長 | 辜雅珍 | 24342456#80 |
| 教育處資安承辦人 | 臨時人員 | 陳莞華 | 24591311#836 |
|  |  |  |  |
| 資安通報平台 | <https://info.cert.tanet.edu.tw/prog/index.php> |

