臺北市立內湖高級中學資訊安全通報事件處理流程

一、 依據教育部學術機構分組資通安全通報演練計畫及教育機構資安通報應變手冊辦理。

二、 資訊安全事件包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等。當資安事件發生時，應循通報機制通報，以免後續影響擴大。

三、 本校的資訊安全事件等級，由輕微至嚴重區分等級如下：

-0 級：符合下列任一情形者，屬 0 級事件：

□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，但其正確性有待認。

□其他單位所告知教育部屬發生未確定之資安事件。

□教育部及區、縣網路中心檢舉信箱通告之資安事件 。

-1 級：符合下列任一情形者，屬 1 級事件：

□非核心業務資料遭洩漏。

□非核心業務系統或資料遭竄改。

□非核心業務運作遭影響或短暫停頓。

-2 級：符合下列任一情形者，屬 2 級事件：

□非屬密級或敏感之核心業務資料遭洩漏。

□核心業務系統或資料遭輕微竄改。

□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。

-3 級：符合下列任一情形者，屬 3 級事件：

□密級或敏感公務資料遭洩漏。

□核心業務系統或資料遭嚴重竄改。

□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。

-4 級：符合下列任一情形者，屬 4 級事件：

□國家機密資料遭洩漏。

□國家重要資訊基礎建設系統或資料遭竄改。

□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。

四、 本校任何人於校內發現異常情況或疑似資安事件及應立即向網管通報，網管應儘速進行處理並研判事件等級。

五、 網管當發生研判事件等級 3（含）以上之事件，應立即通報本校校長，並以電話聯絡臺北市教育網路中心資安承辦人，由校長儘快召集會議研商處理的方式。

六、 當本校發生內部無法處理之資通安全事件，應通報臺北市教育網路中心資安承辦人協助處理。

七、 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」事件通知由網管登入教育機構資安通報平台(國家資通安全通報應變網站 https://info.cert.tanet.edu.tw/)完成通報及應變作業。

八、 資安事件若為校內人員自行發現,由網管登入教育機構資安通報平台進行「自行通報」完成通報及應變作業。

九、 資安事件須於發生後 1 小時內進行通報，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。

十、 如有收到教育機構資安通報平台「資安預警情報」事件通知，由網管登入教育機構資安通報平台，進行資安預警事件單處理作業。

十一、相關通報應變流程依照「教育機構資安通報應變手冊」規定辦理。

本校資訊安全事件通報程序