國立高雄師範大學校園資訊安全事件暨個人資料事故緊急應變處理要點

109 年 11 月 12 日資安暨個資保護管理審查會議通過
109 年 12 月 16 日 109 學年度第四次行政會議通過

一、因應科技犯罪手法與時俱進，冒名電子郵件、通訊軟體之事件猖獗。鑒於以往僅能被動採取事後宣導，雖多數未造成實質損害，仍應制訂完善應變流程，提升主動預防能力，特定本校校園資訊安全事件暨個人資料事故緊急應變處理要點(以下簡稱本要點)。

二、本要點參考教育部「各級學校遭恐嚇詐欺作業說明及處理流程」與本校「ISMS 資訊安全管理系統」(以下簡稱 ISMS)資安事件處理相關程序及「PIMS 個資保護管理系統」個人資料保護應變處理作業辦法擬訂。

三、處理流程

(一) 通報階段：

1. 本校師生接收到疑似詐騙資訊，例如冒名傳送之可疑郵件、簡訊或通訊軟體等，發現意圖詐騙或遭騙屬實之情事，應檢附相關可疑資訊通報圖資處窗口：分機 1706、信箱<nh5@mail.nknu.edu.tw>。
2. 資訊安全及個人資料事故，分別依下列程序進行：
   (1)評估資訊安全等級，依循 ISMS-02-021 資訊安全事件管理作業程序書之標準，評斷資訊安全事件等級，若明確發生實質資料外洩，且內容足以影響本校資訊系統與資料之安全性、可用性及完整性，則發布校內資安通報，並依循 ISMS 四階文件相關程序辦理。
   (2)評估個人資料事故的問題，應依 PIMS-03-002-個人資料保護應變處理作業辦法進行，並依 PIMS-04-008-002 個人資料事故通報及處理流程先判斷是否為個資事故後，若是後續再依循 PIMS 四階文件相關程序辦理。

(二) 處理階段：

1. 由圖資處成立緊急應變小組，依事故性質召集資安/個資相關專責人員。圖資處處長為總召集人，小組成員視事件及影響層面調配組成，其中皆應至少包含一名資訊專長人員。若事件涉及法律層面，小組成員增列生輔組專責人員，進行相關備案程序與輔導。如情事重大，則召集一級主管協商是否循校安相關法規辦理。
2. 初步判定事件真偽，詳細記錄事件經過，彙整相關資料，評估是否納入專家，尋求專業單位協助(資安/個資顧問、警方、律師)。
3. 採取因應措施，透過資訊設備、軟體等方式，阻斷訊息來源以防止繼續擴散，例如封鎖仿冒者郵件地址。
4. 發布提醒資訊，透過全校信件、公告、官方粉絲頁等方式揭露最新詐騙手法，提醒師生民眾留意慎勿上當。

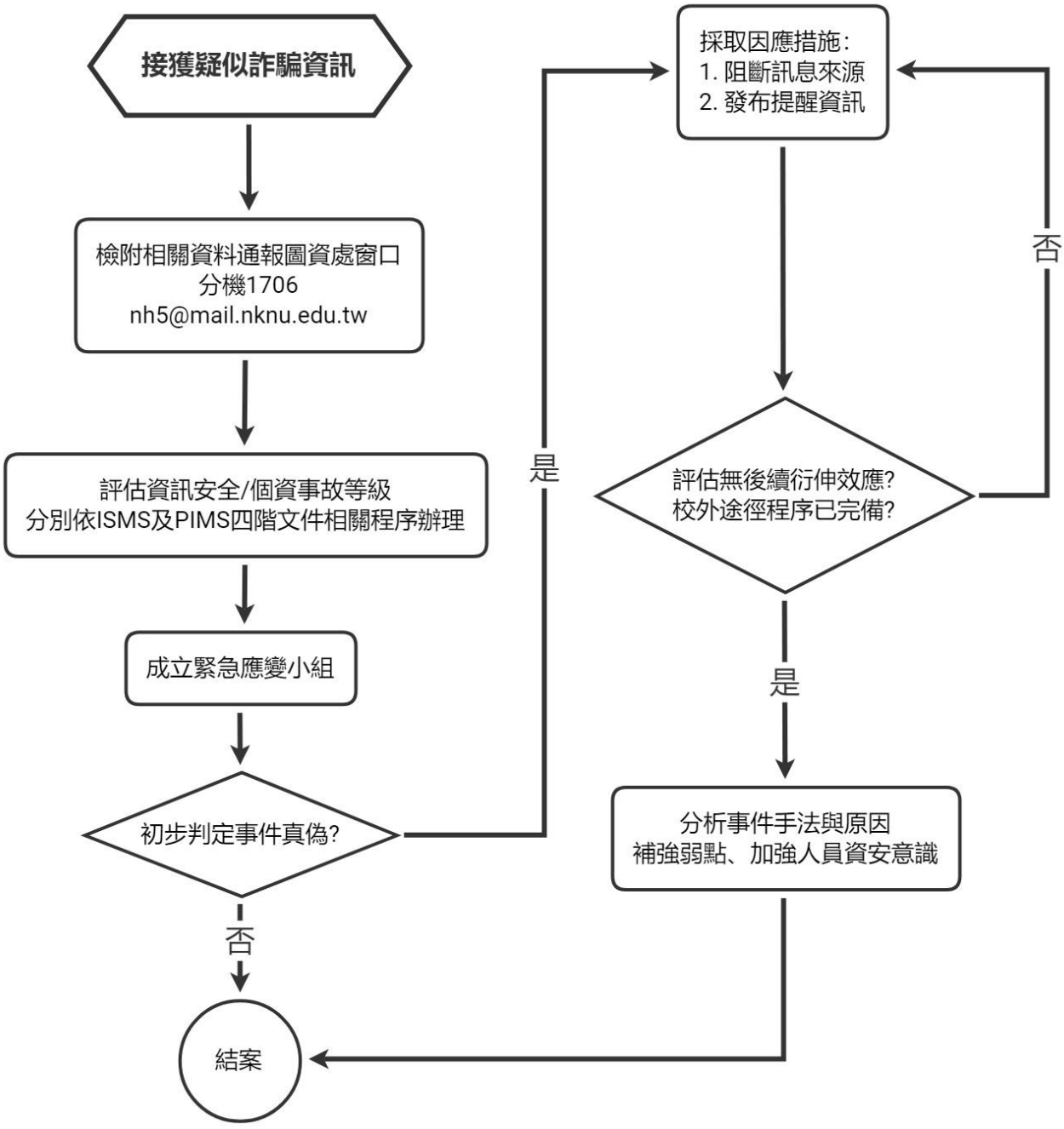
(三) 結案階段：

1. 由緊急應變小組評斷事件再無後續衍伸效應，且循校外途徑之程序均已完備，可宣告結案。
2. 分析事件手法與發生原因，檢討弱點進行補強，改善資訊環境不足、加強人員

資安意識，以達改善預防之功效。

四、如查獲事件發起者為校內人士，則學生依校規論處，職員依人事法規懲處，並循法律途徑辦理。

五、本要點經資訊安全暨個人資料保護管理審查會議審核、行政會議通過，陳請校長核定後實施；修正時亦同。



校園資訊安全事件暨個人資料事故緊急應變處理流程