國立清華大學作業程序說明表

項目編號	NNH-001
項目名稱	資通安全作業-01 資通安全事件通報及應變作業
承辦單位	計算機與通訊中心網路系統組
作業程序說明	一、 資通安全事件通報 （一）單位收到資安通報或發現資安事件後,負責人員應進行事件確認。 1. 經過查證後，應判斷事件是否屬實，並進行處理。 2. 如事件屬虛報者，應予結案；事件確實者應於一小時內登入教育機構資安通報平台進行通報，同時依據 IP 位址清單通知設備管理員進行處理並告知其系主任或單位主管。 3. 每件資安事件依等級不同，需於規定時間內處理完畢並完成結案通報 (1)4 級事件 符合下列任一情形者，屬 4 級事件： 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。 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。 ③ 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。 (2)3 級事件 符合下列任一情形者，屬 3 級事件： 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 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。 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，屬2級事件：

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。

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 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，屬1級事件：

① 非核心業務資訊遭輕微洩漏。

② 非核心業務資訊或非核心資通系統遭輕微竄改。

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)資安預警事件

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，說明如下：

① 未確定事件或待確認事件單：來自北區教育學術資訊安全監控中心（N-ASOC）、南區教育學術資訊安全監控中心（S-ASOC）、縣市網資訊安全維運中心（MINI-SOC）使用之新型技術所產生之事件單，但正確性有待確認者。

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。

(6)資安預警、1、2 級事件需於 72 小時內完成損害控制或復原；3~4 級事件需於 36 小時內完成損害控制或復原。

(7)發生資安事件之設備管理員必須確認事件原因，並提出改善及防範方法。

(8) 資安事件若違反國立清華大學校園網路使用規範應依校規給予處罰。

二、 資通安全事件應變

（一）緊急應變

1. 應就資安事件發生原因、影響等級、可能影響範圍、可能損失及是否需要支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。
2. 依訂定之緊急應變程序，實施緊急應變處置，並持續監控與追蹤管制。
3. 查詢臺灣學術網路危機處理中心網站、系統弱點(病毒)資料庫或聯絡技術支援單位(廠商)等方式，以尋求解決方案；如無法解決，應儘速向所屬區、縣（市）網路中心及通報應變小組反應，請求提供相關技術支援。
4. 評估資安事件對業務運作造成之衝擊，並進行損害管制。若未納入各單位防護範圍之資訊系統發生資安事件，為防止損害擴大影響他人或正常使用者之權益，依據「臺灣學術網路管理規範」,得先行中斷發生資安事件之系統網路連線,待該系統完成通報應變改善作為後,始得恢復其連線。
5. 資安事件損壞程度，請遵循各單位內部備份管理辦法，啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。
6. 資安事件如涉及刑責,應做好相關資料(含稽核紀錄)保全工作，以便聯繫檢警調單位協助偵查。
7. 各單位如發生重大(「4」、「3」級)資安事件，應主動提供相關設備系統日誌予所屬區、縣（市）網路中心及通報應變小組，俾提供相關協助。

（二）事後復原

1. 在執行復原重建工作時，應執行環境重建、系統復原及掃描作業，俟系統正常運作後，即進行安全備份及資料復原等相關事宜。
2. 在完成復原重建工作後，應將復原過程之完整紀錄(如資安事件原因分析與檢討改善方案、防止同類事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。

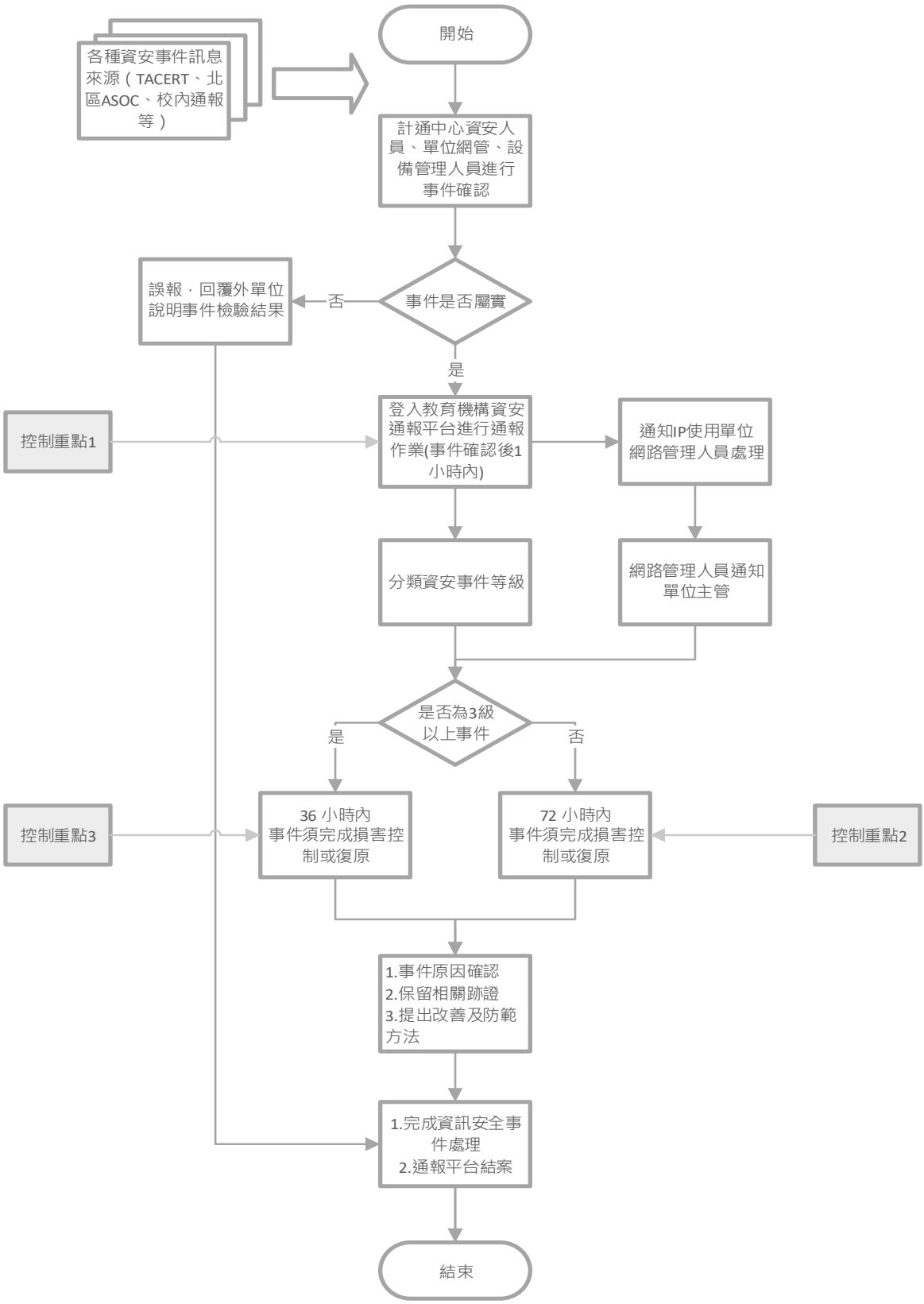
	3. 全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。 **※列明詳細步驟、作業時程、重要經驗及注意事項等**
控制重點 【預定完成日期】 【可量化標示】	一、 發生資安事件時，是否依資安事件等級，於規定的期限內，完成通報與損害控制或復原。 （一）事件確實者應於一小時內登入教育機構資安通報平台進行通報。 （二）資安預警、1、2 級事件需於 72 小時內完成損害控制或復原 （三）3~4 級事件需於 36 小時內完成損害控制或復原。 **※列明不可遺漏之程序、步驟或應予特別重視之作業或法令規定等重要環節並敘明**
法令依據	一、 資通安全管理法。 二、 資通安全事件通報及應變辦法。 三、 臺灣學術網路各級學校資通安全通報應變作業程序。
使用表單	一、 臺灣學術網路各級學校資通安全事件通報單(於無法網路回報時使用)

NNH-001

國立清華大學作業流程圖

資通安全事件通報及應變作業

一、 資通安全事件通報及應變流程



國立清華大學作業程序說明表

項目編號	NNH-001
項目名稱	資通安全作業-02 資通系統分級作業
承辦單位	計算機與通訊中心網路系統組
作業程序說明	一、 依據「資通安全責任等級分級辦法」附表三「資通安全責任等級 B 級之公務機關應辦事項」每年至少檢視一次資通系統分級妥適性。 二、 資訊系統負責人員收到檢視「資通系統分級」通知後，應進行以下作業程序如下： 甲、 盤點資訊系統 1. 盤點出需要進行分級之資訊系統，以自行或委外開發之資訊系統為主。 2. 套裝軟體、作業系統或防毒系統、防火牆系統、入侵偵測/防禦系統、弱點掃瞄系統、網頁/郵件內容過濾系統等屬資安防護處理相關控制措施，均不需進行資訊系統分級。 乙、 確認是否以列冊 1. 如未列冊，則填寫「安全等級評估表」，填寫程序如下： (1) 設定影響構面等級 ① 由資訊系統負責人員評估當發生資安事件時，對機密性、完整性、可用性及法律遵循性四大影響構面之衝擊程度，並參照「資通安全責任等級分級辦法」附表九「資通系統防護需求分級原則」(如附件 1)填寫影響構面安全等級，安全等級區分為【普】、【中】、【高】三級，對於不適用之影響構面，安全等級以 NA (Not Applicable)表示。 ② 資訊系統之安全等級，取其四大影響構面安全等級最高者。 (2) 識別業務屬性與檢視安全等級 ① 識別資訊系統之業務屬性，並由承辦單位主管檢視設定安全等級之合理性。 ② 資訊系統依其支援之單位及業務屬性，分為行政與業務二類，說明如下： ❶ 行政類： 指機關內部輔助單位之業務(如：人事、薪資等)，惟若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整其類別。

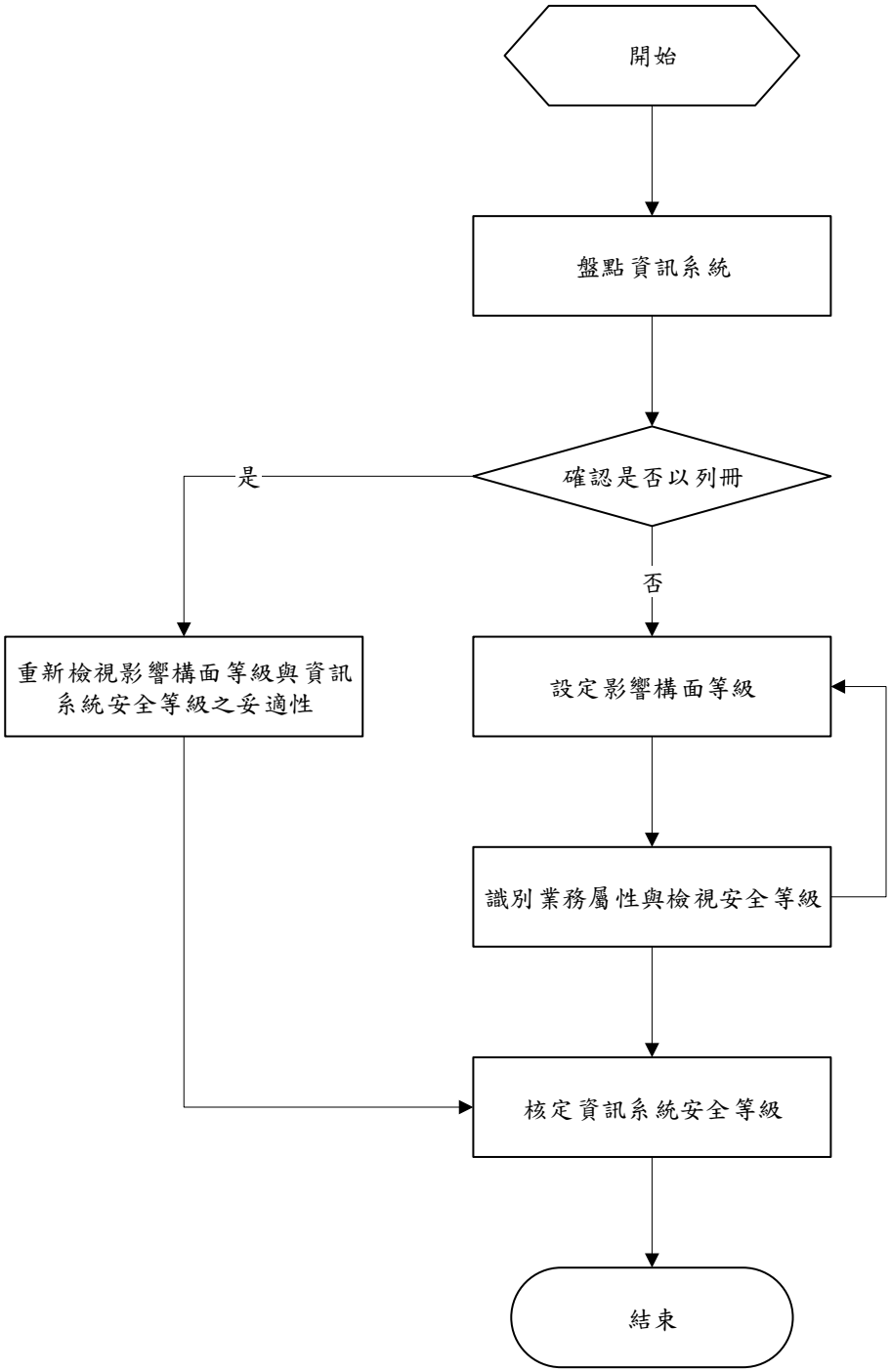
	❷ 業務類：指機關內部業務單位之業務（如：交通監理、便民服務等）。 ③ 本步驟所進行各項異動均須記錄異動原因。 2.如已列冊，則重新檢視影響構面等級與資訊系統安全等級之妥適性。 丙、 核定資訊系統安全等級 1.由計通中心綜整各資訊系統「安全等級評估表」中資訊，併同共同性系統(不需填安全等級)，彙整至「資訊系統清冊」，資訊系統安全等級經相關主管確認後，最後由資通安全長核定。共同性系統之分級，統一由開發管理之機關進行評估與鑑別。 2.本步驟所指之共同性系統，包含共用性系統與共通性系統，共用性系統指單一機關主責系統開發與資料管理，其餘機關僅涉及使用操作，如國稅系統。共通性系統指單一機關主責系統開發與規格制訂，其餘機關除使用操作外，資料主要儲存於使用機關，如公文電子交換系統。 三、 本作業程序所設定之資訊系統安全等級，將作為後續執行防護基準之依據。此外，資訊系統安全等級列【高】者，將納入本校資安維運計劃之核心業務。
控制重點 【預定完成日期】 【可量化標示】	各資訊系統是否依「資通安全責任等級分級辦法」附表九「資通系統防護需求分級原則」(附件 1)設定影響構面等級。
法令依據	一、 資通安全管理法。 二、 資通安全責任等級分級辦法。
使用表單	一、 「資通系統分類分級」內部控制制度作業層級自行評估表 二、 資通系統防護需求分級原則(附件 1) 三、 安全等級評估表(附件 2) 四、 資訊系統清冊(附件 3)

NNH-001

國立清華大學作業流程圖

資通系統分級作業

一、 資通系統分級作業流程



附件 1 資通系統防護需求分級原則

防護需求等級 / 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

國立清華大學作業程序說明表

項目編號	NNH-001
項目名稱	資通安全作業-03 個人資料保護管理機制作業
承辦單位	計算機與通訊中心校務資訊組
作業程序說明	**一、個人資料保護管理委員會** （一）成立「個人資料保護管理委員會」負責個人資料保護制度之建立及推動事宜，以確認本政策能被實施並配置相當資源。每學年開會一次為原則，必要時得召開臨時會議，以確保個人資料之安全維護整體持續改善。 （二）為確保本校之矯正措施有效運作，應確實落實管理審查機制，至少每學年舉行一次個資管理委員會會議，並確實討論下列議題： 1.個資保護政策與程序書之審查。 2.落實個資保護之評估項目。 3.不符合項目及矯正措施。 4.稽核結果。 5.個資保護目標之達成。 6.風險評鑑結果及風險處理計畫辦理情形。 7.持續改善之可能議題。 **二、個人資料檔案清查與風險管理程序** （一）各單位應就業務之流程，屬於個人資料作業、流程及範圍內進行個人資料識別、清查與盤點。 （二）各單位每年進行個人資料盤點作業時，應依據各單位處理個人資料之業務流程及內容，進行個人資料鑑別與盤點作業，並將所鑑別之個人資料，填具於「保有及管理個人資料之項目彙整表」中列管。 （三）個人資料風險評鑑作業於每年辦理個人資料內部稽核活動前執行，並於作業後彙整各單位之風險評鑑結果完成「個人資料風險評估表」，並撰擬「風險評估報告」，陳報「個人資料保護管理委員會」審議。 **三、個人資料事件管理** （一）事件等級主要依據個人資料發生之性質及對本校、當事人（個人資料主體）造成影響程度分類。 （二）本校所有人員發現疑似個人資料事件，應依個人資料事件通報流程通報權責人員，進行後續處置。

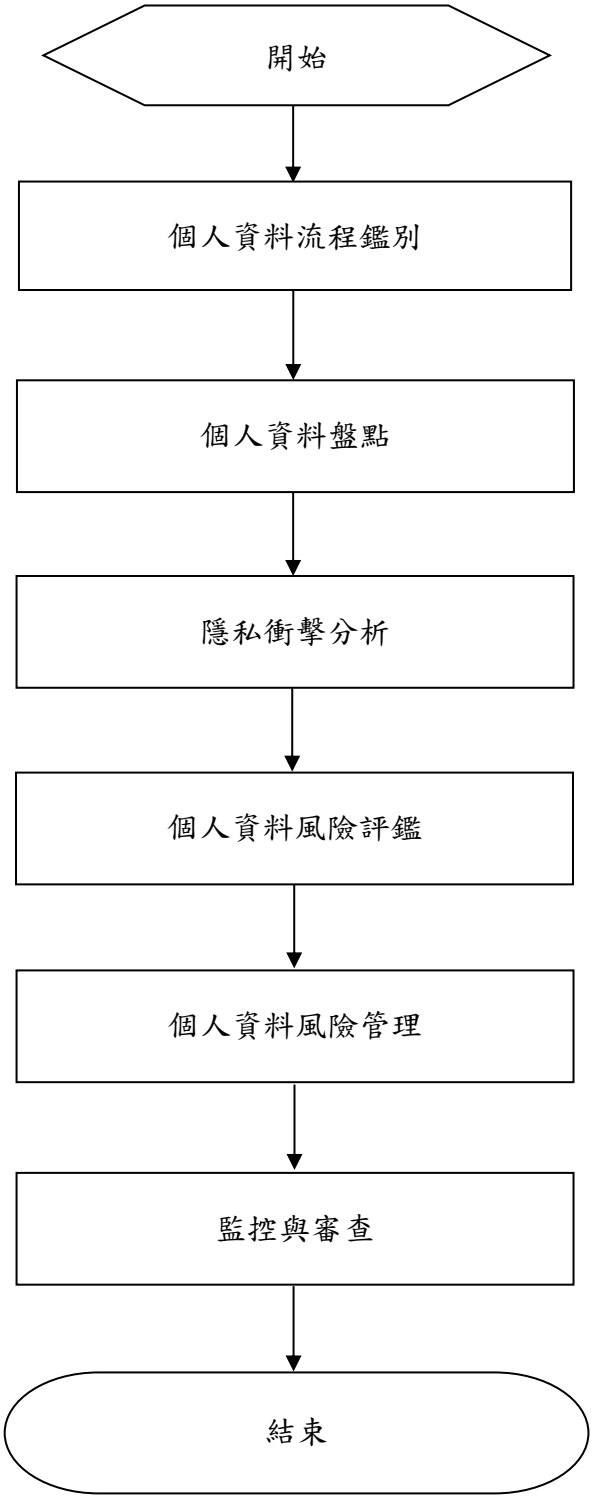
控制重點	一、每年是否至少舉行一次個人資料保護管理委員會。 二、每年是否辦理個人資料檔案清查與風險管理程序。
法令依據	一、個人資料保護法。 二、個人資料保護法施行細則。 三、國立清華大學個人資料保護管理要點。 四、個人資料保護政策。
使用表單	一、國立清華大學個人資料保護管理機制相關表單

NNH-001

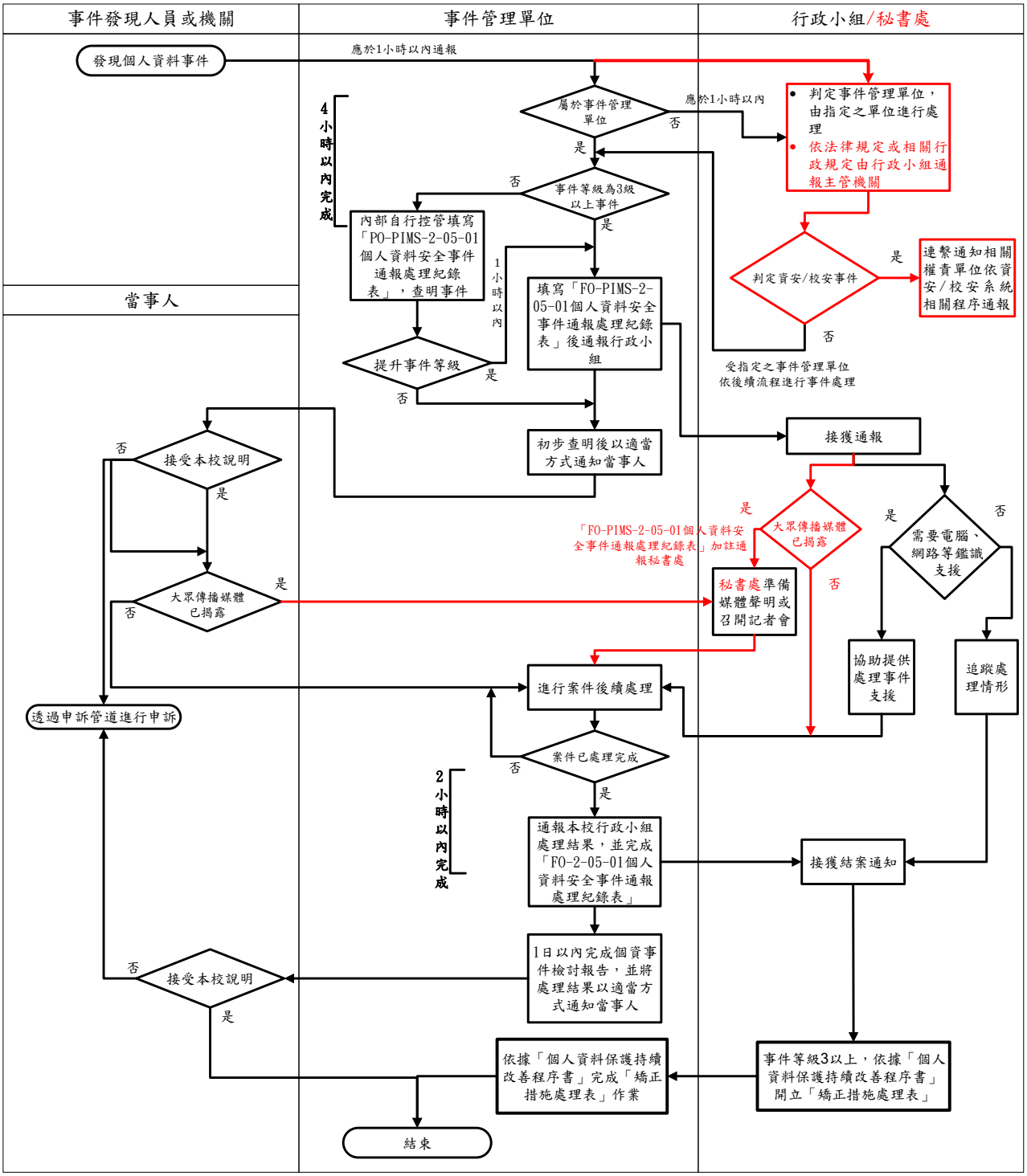
國立清華大學作業流程圖

個人資料保護管理機制作業

一、 個人資料檔案清查與風險管理程序



二、 個人資料事件管理


事件發現人員或機關
事件管理單位
行政小組/秘書處
當事人
發現個人資料事件
應於1小時以內通報
屬於事件管理單位
應於1小時以內
否
是
判定事件管理單位，由指定之單位進行處理
依法律規定或相關行政規定由行政小組通報主管機關
4小時以內完成
否
事件等級為3級以上事件
是
內部自行控管填寫「PO-PIMS-2-05-01個人資料安全事件通報處理紀錄表」，查明事件
1小時以內
填寫「FO-PIMS-2-05-01個人資料安全事件通報處理紀錄表」後通報行政小組
判定資安/校安事件
是
連繫通知相關權責單位依資安/校安系統相關程序通報
否
受指定之事件管理單位依後續流程進行事件處理
提升事件等級
是
否
初步查明後以適當方式通知當事人
接獲通報
否
接受本校說明
是
是
大眾傳播媒體已揭露
「FO-PIMS-2-05-01個人資料安全事件通報處理紀錄表」加註通報秘書處
秘書處準備媒體聲明或召開記者會
否
是
需要電腦、網路等鑑識支援
否
協助提供處理事件支援
追蹤處理情形
否
大眾傳播媒體已揭露
是
進行案件後續處理
透過申訴管道進行申訴
案件已處理完成
否
是
2小時以內完成
通報本校行政小組處理結果，並完成「FO-2-05-01個人資料安全事件通報處理紀錄表」
接獲結案通知
1日以內完成個資事件檢討報告，並將處理結果以適當方式通知當事人
否
接受本校說明
是
依據「個人資料保護持續改善程序書」完成「矯正措施處理表」作業
事件等級3以上，依據「個人資料保護持續改善程序書」開立「矯正措施處理表」
結束