國立高雄師範大學

數位安全與治理執行辦法

目錄

第一章　通則……1
第二章　資訊安全管理……14
　第一節、 網路服務……14
　第二節、 系統服務……18
第三章　個人資料保護……24
　第一節、 個人資料蒐集……24
　第二節、 個人資料處理利用……25
　第三節、 個人資料傳輸銷毀……26
第四章　智慧財產權保護……26
第五章　人工智慧倫理……27
第六章　內部監督……28
第七章　附則……29

國立高雄師範大學 數位安全與治理執行辦法

114 年 11 月 25 日 114 年第 2 次資安、個資暨智財保護管理審查會議通過
115 年 5 月 27 日 115 年第 1 次數位安全與治理查會議修正通過
115 年 9 月 16 日 115 學年度第 1 次行政會議通過

第一章、 通則

章旨說明

本章係就資訊安全、個人資料保護、智慧財產保護及人工智慧倫理等章節中共同適用之基本事項與原則性規範，加以統整規定，作為本辦法各章適用之共同依據。凡性質上具共通性、原則性或需一致適用之事項，均集中列於本章，以避免各章重複規範，並利於使用者就特定主題進行整合查詢及整體理解，提升本辦法之體系性、明確性與適用便利性。

第一條、 使用者、各單位及租用單位使用本校提供之各項數位資源，應遵守本校資訊安全及隱私保護管理政策、本校數位安全與治理指引及數位安全與治理執行辦法(以下稱本辦法)，並應遵守教育部及其他主管機關所定相關規範，包括「臺灣學術網路管理規範」、「教育部校園網路使用規範」、個人資料保護法、智慧財產權保護及人工智慧相關法令，暨其他相關法律規定。如有本辦法未盡事宜，悉依相關法令、本校相關規定及其解釋辦理。

第二條、 使用者、各單位或租用單位違反前條規定、違反本辦法，或有其他足以影響校譽之行為者，應自行負擔因此所生之一切法律責任、損害賠償責任及其他相關責任，並依本校相關校規或人事獎懲規定辦理。單位於同一學期內屢次發生違規情事者，得通知該單位主管列席數位安全與治理委員會，並提出改善方案。

第三條、 應尊重隱私權：

一、不得任意窺視他人之個人資料、檔案、電子郵件。

二、不得未經授權截取、蒐集、處理、利用、儲存、竄改、刪除、散布或提供他人個人資訊。

三、不得利用數位資源或服務，從事其他侵害他人隱私權或個人資料保護之行為。

四、使用資通系統、雲端服務蒐集或利用個人資料者應注意：

(一)資料蒐集最小化：僅蒐集處理目的所必要之個人資料

(二)權限控管與設定檢查：檔案存取權限應採最小授權存取原則，且應詳閱設定內容，不宜使用者共同編輯個人資料檔案清冊，避免使用者能瀏覽其他使用者資料或作答內容，公佈前應確實做好相關設定檢查。

(三)傳輸與儲存安全：個人資料之傳輸應採加密機制辦理；資料儲存應符合相關安全維護規定，並依資料性質採取適當保護措施。

(四)資料保存期限：應訂定個人資料保存期限，並於期限屆滿或業務終止後，將所蒐集之個人資料刪除或銷毀。

(五)告知義務與權利保障：蒐集個人資料前，除法令另有規定外，應明確告知當事人個人資料保護法第八條第一項各款應告知事項及適當之申訴管道。

五、例外情形：本校應尊重數位資源使用者之隱私權，不得任意蒐集、處理、利用或窺視使

用者之個人資料；但有下列情形之一者，不在此限：

(一)為維護或檢查系統安全。

(二)依合理之根據，懷疑有違反校規之情事時，為取得證據或調查不當行為。

(三)為配合司法機關之調查。

(四)其他依法令執行之行為。

第四條、 應尊重著作權：

一、不得未經合法授權，下載、複製、安裝、使用、分享、散布、上傳、或提供他人下載有版權之程式、軟體、音樂、影片或其他受著作權法保護之著作。

二、不得利用網站、伺服器、檔案傳輸服務（如 FTP、雲端儲存空間）、點對點（Peer-to-Peer, P2P）連線軟體、tunnel 工具或其他類似技術，從事前款所列侵害智慧財產權之行為。

三、不得於 BBS、論壇、社群媒體或影像音訊內容分享平台，未經著作權人或權利人同意，或違反其明示之授權條件，任意轉載、散布或公開傳送其受著作權法保護之著作。

四、各單位或管理者提供網站、系統、伺服器或檔案分享服務時，應注意其服務內容或分享檔案、軟體之合法性，不得有猥褻、攻擊、商業性及侵犯智慧財產權之情形，並依規定標示合法授權來源及授權資料。

五、不得利用電子郵件、即時通訊軟體或其他通訊方式，從事違法傳送、散布或其他侵害他人智慧財產權之行為。

六、不得從事其他違反著作權法或相關智慧財產權法令之行為

第五條、 使用人工智慧工具、平台應注意：

一、 資料防護：應避免非必要之個人資料蒐集、處理或利用，涉及個人隱私資料、校務機密資料或其他具資通安全風險之機敏資料者，非經核准，不得輸入、上傳人工智慧工具或平台。如需進行模型訓練，應先落實去識別化處理。

二、內容審查義務：使用者應對 AI 產出內容之真實性、正確性及合法性負審查義務，並避免偏差與歧視。

三、風險分級與安全機制：

應依資料機敏性、個人隱私程度及業務影響範圍進行風險分級，並遵守相應之安全控管措施及防護機制，以兼顧業務數位創新與資訊安全。

（一）極高度風險：涉及機敏保密資料，禁止使用。除經核認之自建、非對外聯網之地端機房，或具同等級資安防護之自控機房，經確認系統安全性後，依個案評估使用。

（二）高度風險：涉及他人權益、隱私或具偏見歧視疑慮者，原則不予使用；確有必要時，應先完成去識別化或安全審核。

（三）中度風險：製作未具前述風險之對外正式文件，視需求建立核實與審核機制。

（四）低度風險：非屬上述單位內部之一般性應用，屬許可應用範圍。各單位可依其業務性質評估風險檢核原則或機制。

四、 人工智慧產出成果與權利歸屬：產出成果應注意其權利歸屬及使用責任，並保留必要生成歷程與證跡資料，以避免侵權、權利歸屬或學術倫理爭議。

（一）主體認定：基於國際人工智慧倫理基本框架認定，著作權與專利保護應以人類創作者為前提，由文字提示生成之 AI 圖像或其他作品，本身不享有版權保護，亦不得列為專利發明。惟著作權係屬私權，個別案例是否構成侵權行為，仍須由司法機關就個案具體事實調查認定。

（二）權利責任：應用 AI 工具產出成果僅於體現人類「實質性介入」、關鍵性修改或原創性引導之部分，始得依法主張權利。單純之文字提示（Prompts）不足以構成受保護之表達。

（三）透明度與證跡留存：利用 AI 工具生成之關鍵學術成果，應詳實記錄生成歷程（如 Prompts 紀錄、模型版本等），以保障權利取得並防範學術倫理爭議。

五、 涉及 AI 工具使用倫理、權責邊界或其他重大爭議事項，非單一單位所能裁決者，得由業務單位提案至本校「數位安全與治理委員會」研議。

第六條、帳號與通行碼原則

使用本校提供之各項數位資源和服務系統，其帳號密碼設定與更換應符合本校存取控制管理作業程序(ISP-02-014)之帳號與通行碼原則。

第七條、禁止商業用途

本校數位資源之使用，依「教育部臺灣學術網路管理規範」及其設置目的辦理，以教學、學術研究、教育行政及其他經本校核准之正當用途為限；除法令另有規定或經本校專案核准者外，不得提供、從事或供作任何營利性商業活動、商業性服務、商業廣告或其他與設置目的不符之商業用途。

第八條、禁用大陸廠牌資通產品

一、 本校為公務機關，依行政院規定不得下載、安裝、使用危害國家資通安全產品：

(一)本校各單位全面禁止採購及使用大陸品牌之資通訊產品，其範圍涵蓋硬體（含物聯網設備）、軟體、雲端服務及即時通訊服務。

(二)對本校出租場域，應於委外契約或租借規定中，明訂租用廠商或單位不得使用危害國家資安之產品及服務（含大陸廠牌軟體、硬體、雲端服務及資通訊設備）

(三)本校各單位禁止採購或使用大陸廠牌生成式 AI 服務產品（含雲端、APP 及地端下載方式）。

二、倘因業務需求且無其他替代方案，必須採購或使用前開產品時，應具體敘明理由，經本校資安長及教育部逐級核可，並函報《資通安全管理法》主管機關數位發展部核定後，以專案方式購置列冊管理。

第九條、數位採購外包：

一、本條所稱數位採購外包係指涉及資訊安全、個人資料保護、智慧財產保護及人工智慧管理等事項之軟硬體、網站、系統、平台及其他各類數位資源之套裝購置、委外開發、租用、維護委託或相關勞務委託。

二、執行單位與職責：

採購單位：總務處事務組負責採購作業

需求單位：各業務需求及使用部門，提出請購需求與驗收作業。

協助單位：圖資處資訊整合角色，對採購外包的規格提供諮詢，並提供驗收諮詢。

三、作業流程：依性質、規模及實際需要，分階段辦理需求規劃、請購、採購、驗收及維護等相關作業。

四、需求規劃：

(一)由需求單位提出需求規劃，若屬全校性、跨單位共用或整體性發展事項者，得由圖資處統籌規劃辦理。

(二)圖資處得定期就前開之供應商、受託廠商或服務提供者，就其服務品質、履約成效、成本效益、執行進度及其他相關管理情形辦理檢討或評估，作為後續採購外包之參考依據。

五、請購-數位設備採購：

(一)數位設備採購含各類電腦、伺服器、網路設備、監視設備、智慧設備、物聯網設備及其他硬體設備之採購、租用或建置。

(二)單位應要求廠商於報價單中提供資通訊設備之廠牌和型號，並於財產管理系統新增填報財產時正確填寫，以供每年填報教育部「資通訊設備清冊」之用。

(三)由提出請購需求之單位，本權責確認產品不得為大陸品牌。圖資處每年定期進行資訊資產盤點，請購單位須於資訊資產管理系統中填報各類資通訊硬體資產之廠牌、型號，以供稽核。數位採購外包之契約內應明訂禁止委外廠商使用大陸廠牌之資通訊產品，包含軟體、硬體及服務等。

(四)物聯網設備法遵事項：

1、 應優先採購取得資安標章之物聯網設備，且應與設備供應商簽訂資訊安全相關協議，其內容應包含服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案等事項，以明確約定相關責任。

2、 各單位請購各項裝設於本校場域之物聯網(IoT)設備時，應要求廠商不得以預設帳號、密碼或任何弱密碼完成設備設定，設備密碼長度及強度應符合本校資訊安全及隱私管理(ISP)之密碼安全性原則，廠商應於設備完成設定後，提供已更改密碼之相關證明文件(密碼設定佐證單)，本項要求應於規格需求書中明文載明，並作為驗收與付款之必要條件之一。

六、請購-套裝軟體與雲端服務採購

套裝軟體與雲端服務採購包含各類套裝軟體、雲端平台、線上服務、人工智慧服務、生成式人工智慧服務及其他非客製化數位服務之採購或租用。

七、請購-委外開發與資通系統建置

(一)委外案之規格建議書由需求單位自行研擬，若為圖資處統合性之資訊類採購案，則由圖資處協助需求單位研擬。

(二)委外資通系統之建置、維運，採購：

本校資通系統之採購及委外案件，應依行政院所定「資通系統籌獲各階段之資安強化措施」，納入請購審查、需求研擬、規格訂定、評選、履約管理及驗收程序。

1、 需求階段：

(1) 單位應於請購前，依「資通安全責任等級分級辦法」附表九之「資通系統防護需求分級原則」完成資通系統分級，

(2) 單位應於請購前，依系統等級對系統安全需求(含機密性、可用性、安全性)進行確認，填寫委外資通系統資安需求表。

2、 採購文件中載明以下事項：

(1) 前項資通系統分級結果及系統安全需求。

(2) 受託者應依前述分級結果，完成該辦法附表十所定「資通系統防護基準」之該等級全部適用項目要求。

(3) 受託者應依安全系統發展生命週期（Secure Software Development Life Cycle, SSDLC）進行系統開發程序，於 SSDLC 各階段依資通系統分級執行資

安要求。

(4) 受託者應協助單位填寫「資通系統安全等級評估表」及「資通系統安全防護基準檢核表」作為資安檢核依據。

3、 選任及監督受託者時應注意下列事項(採購文件中載明)：

(1) 受託者應具備完善之資通安全管理措施或通過第三方驗證，並就其開發及維運環境之資通安全管理接受評估。受託者應提供「委外廠商自我評估表」及佐證資料或通過第三方驗證之證明，以供評估。

(2) 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員，委託單位及受託者應指定專案管理人員，負責推動、協調及督導委外作業之資通安全管理事項。

(3) 受託者辦理受託業務如允許複委託，則對複委託之受託者其資通安全維護措施要求，應至少與受託者同等級。受託者應提供複委託之受託者相關之資安評估表或證明，以供確認。

(4) 受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。本要求應記載於招標公告、招標文件及契約；於辦理適任性查核前，並應經當事人書面同意。

4、 建置階段(採購文件中載明):

(1) 委託單位應監督、確認開發團隊於系統開發時遵循安全軟體開發生命周期(SSDLC)。

(2) 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；

(3) 受託者應提供資通系統之安全性檢測證明，涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

5、 維運階段(採購文件中載明)：

(1) 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

(2) 受託者需提供委託單位系統、資料庫等之管理者帳號與權限，以因應第一線面臨緊急狀況之初步處置。

(3) 發生資通安全事件時，受託者應立即通知本校，說明資安事件之原委、處置方式，相關異常處理紀錄與跡證保存原則應符合本執行辦之事件通報及應變規定進行跡證保存，本校得視需要查核。廠商需在採購單位訂定之復原時間目標(Recovery Time Objective，RTO)及復原點目標(Recovery Point Objective,RPO)時限內讓資訊服務恢復運作與資料損失量不超過規定的時間範圍。

(4) 受託者應訂定資通系統緊急應變與回復標準程序，以確保本校資訊業務之持續運作。

(5) 委託關係終止或解除時，受託者應返還、移交、刪除或銷毀履行契約而持有之資料，受託者應出具不再保留個人資料等相關切結書。

(6) 受託者應採取之其他資通安全相關維護措施。

(7) 委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，

以稽核或其他適當方式確認受託業務之執行情形。

(8) 受託者之專案成員進出本校安全限制區域及所攜帶或使用之資訊設備，應符合本校「ISP-02-15 實體及環境安全管理作業程序」。

(9) 受託者之專案成員對於資通系統存取程序及授權規定，應符合本校「ISP-02-14 存取控制管理作業程序」。專案人員調整及異動亦依前述作業程須調整其權限。

6、 各單位應要求廠商簽署「校外廠商保密切結書」，且管理相關委外專案人員及外部人員之各項個人資料存取權限，並要求外部人員應簽署「ISP-04-020-003 校外人員保密切結書」。若有委託他人蒐集、處理或利用個人資料時，委託單位應對受託者為適當之監督。

八、請購-數位勞務與技術服務

數位勞務與技術服務包含各類資訊安全服務、系統維護、顧問服務、安全性檢測、教育訓練、資料處理、人工智慧模型訓練及其他相關技術服務。

九、採購：採購方式依循採購管理辦法之規定辦理。

十、專案管理與驗收：

(一)數位採購外包應依其性質訂定完整之進度規劃要求外包廠商提報進度與執行成果，由採購單位會同圖資處協助執行，必要時可召開專案進度管制會議，統一追蹤並了解執行進度與成果。

(二)涉及客製化系統、平台建置或人工智慧應用開發者，應依照系統分析(SA)、系統設計(SD)、程式設計(Coding)、測試、驗證、試行及正式上線等階段管理。

(三)維護委託案或其他持續性服務者，得依契約約定辦理定期檢核、服務監控或分期驗收。

(四)數位採購外包之分期驗收或總驗收時，均應按採購約定之各期產出項目驗收，各項文件資料（含系統規格書、程式清單、操作說明等）須俱全，需求單位負責確認需求是否符合。

(五)系統委外案之委託單位應本權責訂定、監督、確認其資通系統維運作業確實依委託單位之資安管理措施落實辦理，圖資處協助委託單位作第二線勾稽確認。

十一、 保固與維護：

(一)採購或外包案於驗收之同時，應確認保固維護條款及系統轉移訓練計畫。若未檢附維護或訓練計畫，採購單位不得逕行驗收。

(二)涉及系統、設備或平台建置者，應訂定合理保固與維護期間(至少一年)，並應包含安全更新、漏洞修補及版本維護機制。

(三)涉及人工智慧或雲端服務者，應確認模型、服務或平台於契約期間內之維運、權限管理、資料保護及服務可用性。

十二、 系統介接與資料交換：

(一)數位採購外包如有與本校既有資訊系統、資料庫、身分驗證機制、資料交換平台或其他資訊架構進行 API 介接、資料交換、系統串接或架構對接之需求，受託者應配合本校資訊業務主管單位辦理相關技術作業，並提供下列服務：

1、 系統 API 介接諮詢及技術協作。

2、 資料庫欄位內容確認、資料內容、資料流向及交換規則之說明與確認。

3、 PI 介接、資料交換、資料庫交換作業或系統串接所需之帳號、權限、憑證、金鑰、資料表欄位說明或其他必要設定。

4、 自動化資料庫交換、批次介接、排程作業及相關監控、測試與異常排除服務。

5、 其他與系統自動化介接及架構對接有關之必要技術支援。

(二)本項要求應於採購文件中載明。

十三、 程式著作權：

(一)數位採購外包案件所產出之程式、文件、資料、模型、素材或其他成果，其智慧財產權、使用權限及授權方式，應於契約中明確約定。

(二)除契約另有約定外，受委託開發之應用系統、程式或相關成果，其著作財產權歸屬本校所有。

(三)廠商非經本校書面同意，不得將受託開發成果全部或部分移轉、授權或提供第三人使用。

(四)本項要求應於採購文件中載明。

第十條、通報及應變處理

一、本校數位安全與治理之通報及應變處理機制，涵蓋人工智慧倫理、資訊安全管理、個人資料保護及智慧財產權保護等四大面向。各單位於發生相關事件時，應依其所適用之中央法規、主管機關規定、本校相關制度或作業規範辦理通報、應變、調查、改善及紀錄保存等作業；如無相關法規或既有規範可資遵循者，則依圖書資訊處所訂之相關作業程序及管理規定辦理。

二、資通安全事件通報及應變處理

本校於發生資通安全事件時，應依「資通安全事件通報應變及演練辦法」相關規定，即時通報及應變，迅速完成損害控制或復原作業，降低資通安全事件對各機關業務之衝擊影響，並確保資通安全事件發生時之跡證保存。

三、本校應成立資通安全事件通報及應變小組(以下簡稱通報應變小組)，於平時進行演練，並於發生資通安全事件時，依事件等級進行通報及應變作業。通報應變小組組成及分組代表如下圖一及下表二，其任務如下：

(一)事件指揮官：為通報應變小組總召集人，綜理全般業務，直接督導各單位聯絡人員及機關新聞官/組。

(二)新聞官/組：視事件需要由事件指揮官或其授權人員擔任新聞官或分組代表，資通安全事件對外發布新聞或說明之單一窗口，綜整與定期更新訊息及擬定溝通計畫。

(三)執行秘書：為事件指揮官幕僚，負責督辦通報應變小組各項業務。

(四)情資及計畫組：

1、 本分組負責辦理下列事宜：

(1)資通安全事件通報及情資分享：透過資通安全監控中心(SOC)、防毒軟體及系統釐清事件影響，並清查各單位受影響情形，據以完成資通安全事件各階段通報，分享惡意程式 IoC 等。

(2)應變策略及計畫研擬：於發生重大資通安全事件時，依據事件情況研擬損害控制、復原作業及跡證保存計畫。

2、 本分組由機關資通安全專責人員、資訊人員及委外廠商或外部專家組成，上級機關、中央目的事業主管機關或相關機關，亦應視情況或納入政風單位派員參與，以提供必要之支援協助。

(五)應變執行組

1、 本分組負責辦理下列事宜：

(1)執行損害控制：依據情資及計畫組研擬之應變策略及計畫，調度資訊及資通安全人員執行災害搶救及損害管制，防止次波攻擊及損害擴散。

(2)復原作業：依據情資及計畫組研擬之復原作業，完成系統重建、弱點掃描或漏洞修補等事宜。

(3)跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。

2、 本分組由機關資通安全專責人員、資訊人員、業務單位及委外廠商組成，上級機關、中央目的事業主管機關或相關機關得於機關申請支援時派員參與。

(六)後勤調度組

1、 本分組負責辦理下列事宜：

(1)事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。

(2)提出改善建議：依據事件調查根因，提出短、中、長期改善建議。

(3)彙整改善報告。

(4)撰寫調查、處理及改善報告。

(5)追蹤管考：針對機關單位已結案或未結案事項，如有未盡改善事宜，將另案追蹤管考。

2、 本分組由機關資通安全專責人員、資訊人員及委外廠商或外部專家組成，上級機關、中央目的事業主管機關或相關機關得於機關申請支援時派員參與。

(七)財務行政組

本分組視事件需要由主計室主任組成，負責辦理預算調撥及提供行政支援事宜。

(八)各小組成員聘期採學年制,每學年經本校資訊安全暨個人資料保護管 理審查會議檢視小組成員組成，於會議通過後陳請資安長同意後發聘函。

四、本校之資通安全事件通報及應變程序(如下圖三)：

(一)通報資通安全事件

1、 依本法及資通安全事件通報及應變辦法規定，由情資及計畫組依主管機關或中央目的事業主管機關指定方式完成事件通報。

2、 第三級或第四級資通安全事件，各機關除依前目規定通報外，應另以電話或其他適當方式通知上級機關或中央目的事業主管機關，無上級機關者，應通知主管機關；行政院資通安全處(數位發展部資通安全署成立後為該署)就第三級或第四級資通安全事件，依國土安全緊急通報作業規定轉報行政院國土安全辦公室。

(二)組成通報應變小組與召開事件應變會議

完成第三級或第四級資通安全事件之初步損害控制後應召開事件應變會議，會議形式不拘，由事件指揮官主持討論下列事項，並得視情況邀請上級機關、中央目的事業主管機關或主管機關出席：

1、 資通安全事件概況。

2、 評估受影響範圍。

3、 其他必要之討論事項。

(三)損害控制或復原作業

1、 由應變執行組執行損害控制或復原作業，並辦理下列事項：

(1)確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，防止次波攻擊及擴散情形。

(2)評估各系統是否於可容忍中斷時間內恢復服務及對利害關係人之影響，決定是否對外公告事件之相關內容。

(3)於完成損害控制或復原作業後，依主管機關或中央目的事業主管機關指定之方式完成通知作業。

2、 第三級或第四級資通安全事件，除依前目規定辦理外，並應辦理下列事項：

(1)定時向事件指揮官、通報應變小組成員、上級機關或中央目的事業主管機關回報控制措施成效；無上級機關者，應回報主管機關。

(2)倘涉及個人資料外洩，應評估通知當事人之適當方式，依個人資料保護法第十二條規定辦理。

(四)事件根因分析

後勤調度組執行，依資通安全事件等級，建議辦理事項如下：

1、 依第四點跡證保存之規定保存相關跡證，惡意程式建議得請防毒軟體或資安服務公司檢測，並上傳至 VirusCheck 網站(https://viruscheck.tw/)分析，以更新或強化相關偵測及聯防機制，不宜上傳至其他平臺。

2、 除設備故障外，後勤調度組應依據目前保存跡證，由組長督導委外廠商或外部專家進行根因調查，並提出紀錄分析；如發現惡意程式，應提出惡意程式分析。

3、 依據事件調查根因分析結果，機關應評估短、中、長期資安管理改善策略，其內容如下：

(1)短期：完成可立即性修補項目之調整，例如更換密碼或修補程式弱點等。

(2)中期：依據事件根因提出三至六個月內完成之強化作為，例如盤點機關老舊設備，並訂定汰換期程。

(3)長期：依據事件受害情形，視需要提出二年內完成之管理改善建議，例如培養機關資安人員能力。

4、 由執行秘書將事件調查根因及改善策略提報事件指揮官裁處，並由機關資通安全專責人員彙整送交上級機關或中央目的事業主管機關；無上級機關者，應送交主管機關。

(五)改善追蹤

進行事件改善追蹤時，應視需要召開會議，並據以辦理下列事項：

1、 評估改善作為期程。

2、 評估執行成效，並據以調整改善策略。

3、 配合上級機關、中央目的事業主管機關或主管機關辦理相關改善作為。

4、 第三級或第四級資通安全事件，應由執行秘書將各階段改善措施執行成效定期回報事件指揮官至完成各項改善措施為止，並由機關資通安全專責人員彙整送交上級機關或中央目的事業主管機關；無上級機關者，應送交主管機關。

5、 依主管機關或中央目的事業主管機關指定之方式，送交調查、處理及改善報告；第三級或第四級資通安全事件，應另以密件公文將該報告送交主管機關及上級或監督機關。

6、 機關送交調查、處理及改善報告後，相關改善事項應納入機關現行定期追蹤管考機制。

五、跡證保存

為確保資通安全事件發生時，機關所保有跡證足以進行事件根因分析，本校依資通安全事

件等級C 級，建議辦理下列事項，並應視事件情形辦理其他必要之跡證保存事項：

(一)日常維運資通系統時，應依自身資通安全責任等級保存日誌(log)，並建議定期備份至與原稽核系統不同之實體系統，其保存範圍及項目如下表三。

(二)發生資通安全事件時，機關應依下列原則進行跡證保存：

1、 進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。

2、 若系統無備援機制，應備份受害系統儲存媒介(例如硬碟、虛擬機映像檔)後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。

3、 若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供服務。

4、 若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。

(三)本校於簽訂資通系統或服務之委外契約時，應依前二款規定於契約中明定紀錄保存及備份規定。

六、網頁遭竄改緊急應變處理

(一)依據資通安全管理法及教育部要求，學校對外服務網頁應保持正確可供瀏覽狀態，若網頁遭竄改，影響網站可用性、機密性、完整性、法遵性其一，本校各單位應須迅速依以下原則應變：

1、 各網站管理人員知悉網頁遭竄改，須立即通報秘書室及圖書資訊處，非上班時間須立即通知校安人員。

2、 原網站立刻下架，並注意須完成跡證保全及留存。

3、 維護公告網頁：10 分鐘內上架。

4、 靜態資訊網頁：網站功能無安全疑慮的部分可先上架恢復服務，如純資訊公告、媒體播放等。

5、 逐步功能恢復：網站每次版更上線前弱點掃描，確認無重大安全性弱點，必要時加入人工測試。

6、 全面修復上架。

(二)依資安法及「臺灣學術網路各級學校資通安全通報應變作業程序」規定，本校須落實資安事件通報及應變作業，圖書資訊處負責資安通報同仁將於知悉事件 1 小時內完成通報。

(三)全校各行政、教學單位之校內對外服務主網頁、各行政單位、系所、核心業務等網站，皆需進行業務持續運作演練（BCP），並將過程以電子檔案或書面留存，作為資安稽核證據。

七、個人資料安全事件應變處理

（一）本校個人資料安全事件之應變及通知作業，應依「個人資料保護法」第十二條相關規定辦理。個人資料保有單位或個人，於知悉本校所保有之個資法第十二條所定個人資料有被竊取、洩漏、竄改或其他侵害情事時，應先行通報並進行緊急因應措施，其作業程序如下：

1、 個人或單位接獲個人資料安全事件通知。

2、 個人或單位主動通知執行小組。

3、 執行小組釐清資料保有、處理等作業程序與責任所屬。

4、 資料權責單位應即進行防禦或補救作業。

5、 經查明個人資料確有被竊取、洩漏、竄改或遭其他侵害情形，且足以影響當事人權益者，資料權責單位應依個人資料保護法施行細則相關規定，以適當方式通知當事人。

6、 資料權責單位應將改善與預防措施納入工作準則，以降低事件再發生機率。

7、 回報執行小組。

8、 執行小組依規定上網通報。

(二)若因個人、資料權責單位或業務辦理單位違反本校個人資料保護相關規定，導致個人資料安全事件發生，造成個人資料外洩或其他權益侵害者，應依情節輕重，由相關個人或業務辦理單位承擔相關責任。

八、電腦軟體侵權應變處理

(一)本校各機關採購電腦設備時，應考慮未來使用合法電腦軟體之需求，並編列預算進行採購，避免侵犯智慧財產權；如無力採購合法授權軟體時，建議教師使用自由軟體教學，並鼓勵學生使用。

(二)非法電腦軟體係指「未經授權而使用之電腦軟體及非公務用 P2P 分享軟體」，本校每季各單位進行自我例行查核乙次；本校每年內部稽核時將進行抽查，若發現有非法電腦軟體，將列入單位缺失並矯正改善，情節重大者將進行議處。

(三)若接獲檢舉，學生或教職員個人電腦有疑似侵權行為時，將依據「台灣學術網路智慧財產權疑似侵權處理程序」相關規定，按以下步驟處理：

1、 立即限制該違規電腦之網路使用權。

2、 立即以本校之 email 或電話通知該使用者。

3、 該電腦擁有(管理)者必須親自至圖資處說明，填寫 「疑似違反智慧財產權說明書」。

4、 依侵權被檢舉次數及侵權事實，處理如下：

(1) 第一次被檢舉侵權者，告知相關侵權法律責任後，恢復其使用資格。

(2) 第二次被檢舉侵權者，若有侵權事實，填寫「不再犯切結書」。

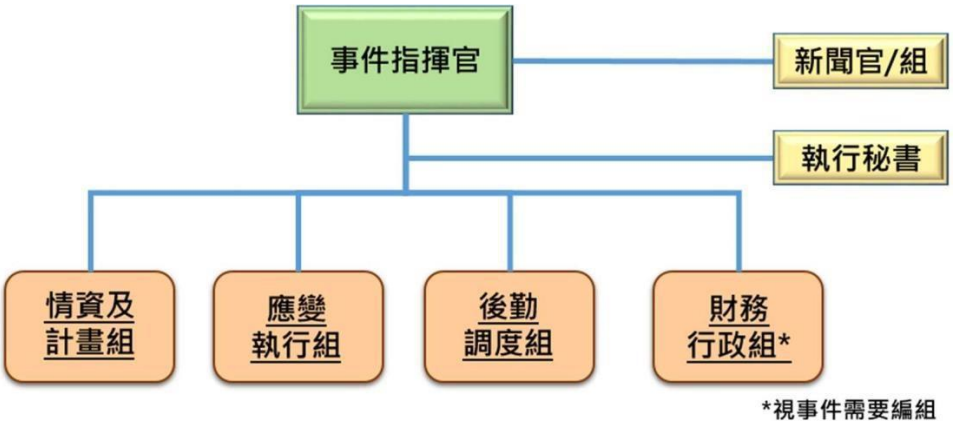
(3) 三次以上被檢舉者，若有侵權事實或無法取得誤判證明者，請學務處或人事室依情節懲處。

5、 圖資處將相關使用者所填寫「疑似違反智慧財產權說明書」、「不再犯切結書」及相關證明文件，送請學務處(學生)或人事室(教職員)備查。

對於上述宣稱無辜之使用者(被檢舉者)，圖資處將提供相關流量資料以茲佐證，並協助該使用者向檢舉單位說明，唯使用者必須提供詳盡之電腦使用習慣等資料以茲證明。

(四)若侵權情節重大者，由圖資處處長籌組工作小組進行調查及協助處理。

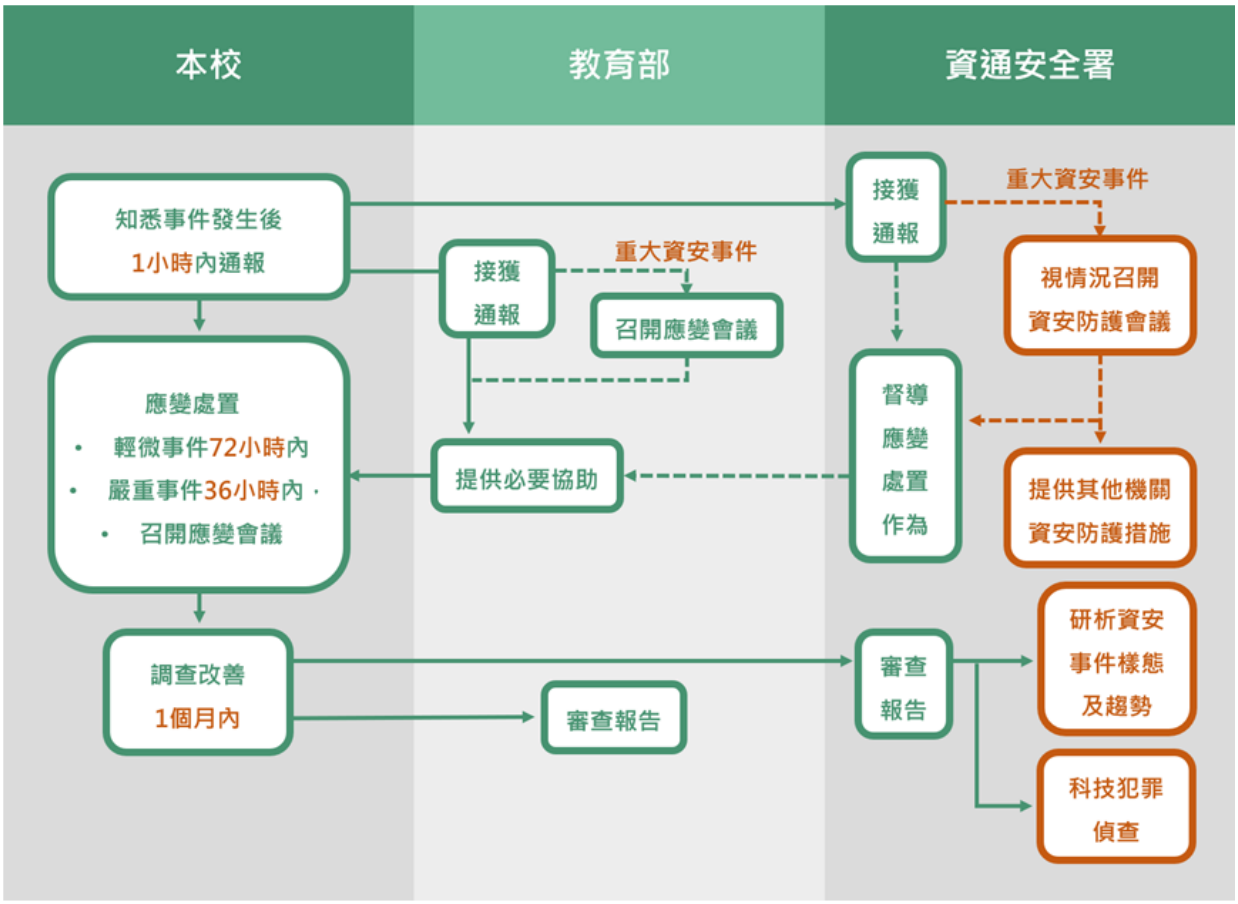
圖一、資通安全事件通報及應變小組組成圖



表二、通報及應變小組組成圖及各分組代表

	第一級、第二級資通安全事件	第三級、第四級資通安全事件
事件指揮官	機關資訊(安)單位主管 **圖書資訊處處長**	機關資通安全長 **校長**
新聞官/組	機關對外發言人員或單位主管 **副校長/主任秘書**	
執行秘書	機關資通安全專責人員或資訊人員 **資安專責人員** **（短期約聘僱/長期公務人員）**	機關資訊(安)單位主管 **圖書資訊處處長**
情資及計畫組組長	機關資通安全專責人員或資訊人員 **技術專員**	機關資訊(安)單位主管 或資通安全專責人員 **資安專責人員**
應變執行組組長	機關資通安全專責人員或資訊人員 **技術專員**	機關資訊(安)單位主管 或資通安全專責人員 **圖書資訊處處長**
後勤調度組組長	機關資通安全專責人員或資訊人員 **技術專員**	機關資訊(安)單位主管 或資通安全專責人員 **資安專責人員**
財務行政組組長	機關財務或秘書單位主管 主計室主任	

圖三、資通安全事件通報及應變程序



表三、跡證保存範圍及項目

資通安全 責任等級	保存範圍	保存項目
C	機關應保存全部核心資通系統最近六個月之日誌紀錄。	1.作業系統日誌(OS event log) 2.網站日誌(web log) 3.應用程式日誌(AP log) 4.登入日誌(logon log)

註：若資訊系統已向上集中者，則可由上級機關保存。

第十一條、<u>獎勵</u>

一、本獎勵辦法係針對本校推動「資訊安全管理、個人資料保護、智慧財產保護及人工智慧倫理」等數位安全與治理相關工作，具有具體績效或貢獻者，予以獎勵。

二、有下列「數位安全與治理」情形之一者，予以獎勵：

(一)依中央相關法規或機關內部規範，訂定、修正及實施數位安全與治理相關計畫(含資通安全維護計畫、個人資料保護安全計畫、智慧財產保護及人工智慧倫理相關計畫等)，績效優良。

(二)稽核所屬或監督機關之數位安全與治理實施情形，或辦理相關演練作業，績效優良。

(三)配合主管機關、上級或監督機關辦理數位安全與治理相關稽核或演練作業，經評定績效優良。

(四)辦理數位安全與治理業務切合機宜，防止資訊安全事件、個資外洩、智慧財產侵害或人工智慧使用風險之發生，避免本校教職員工生或其他機關遭受損害。

(五)主動發現新型態之資訊安全弱點、個資保護風險、智慧財產侵害問題或人工智慧應用風險，並進行相關分享或改善，防止事件發生或降低其損害。

(六)積極查察數位安全與治理相關異狀，即時發現重大事件，並辦理通報及應變，防止其損害擴大。

(七)對數位安全與治理業務提出具體建議或革新方案，並經採行。

(八)辦理數位安全與治理人才培育事務，有具體貢獻。

(九)辦理數位安全與治理相關軟硬體技術規範、服務及審驗機制發展等事務，有具體貢獻。

(十)辦理數位安全與治理政策、相關法規研析或制定，有具體貢獻。

(十一) 辦理數位安全與治理業務有具體功績。

(十二) 對本校數位安全與治理宣導與推動有實際作為。

(十三) 主動積極取得資訊安全、個資保護、智慧財產或人工智慧治理相關證照或證書。

(十四) 主動積極參與數位安全與治理相關培訓課程。

(十五) 積極參與本處辦理之相關研習、說明會、宣導活動等。

三、前項所列情形獎勵，由本校圖資處臚列具體事蹟，經數位安全與治理審查委員會審議後，製作獎狀乙幀，請校長於行政會議公開表揚獲獎單位及人員，並公告於本校官方網站以茲鼓勵。

第二章、資訊安全管理

第一節、 網路服務

第十二條、 校園網路

一、定義：本辦法所稱校園網路，係指由本校於教學、研究和行政區域建置並管理之有線及無線網路功能(以下簡稱校園網路)。惟學生宿舍網路已委託外部電信事業建設與營運，其架構、維修及使用者行為規範，其網路使用與管理權責另依相關合約、規範及法律辦理。

二、校園網路使用者應遵守以下項目：

(一)不得利用臺灣學術網路從事營利性商業活動，如電商營運、挖礦等。

(二)不得散布電腦病毒或其他干擾或破壞系統機能之程式。

(三)不得擅自截取網路與私自接用他人網路線路、接點傳輸訊息。

(四)不得以破解、盜用或冒用他人帳號及密碼等方式，未經授權使用網路資源或無故洩漏他人之帳號及密碼。

(五)避免將帳號借予他人使用。

(六)不得隱藏帳號或使用虛假帳號。但經明確授權得匿名使用者不在此限。

(七)不得以任何方式濫用網路資源，包括以電子郵件大量傳送廣告信、連鎖信或無用之信息，或以灌爆信箱、掠奪資源等方式，影響系統之正常運作。

(八)不得以電子郵件、線上談話、電子布告欄(BBS)、社群網站或類似功能之方法散布詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息。

三、校園網路管理

(一) 本校圖資處執行網路管理事項如下：

1、協助網路使用者建立自律機制。

2、對網路流量應為適當之區隔與管控。

3、對於違反本規範或影響網路正常運作者，得暫停該使用者使用之權利。

4、各網站系統設置專人負責管理、維護。對於違反網站系統使用規則者，系統負責人得刪除其文章或暫停其使用，情節重大、違反校規或法令者，並應轉請學校處置。

5、本校已加入 TANet 無線網路漫遊交換中心之校際無線網路漫遊計畫，凡屬於該計畫之成員學校人士，均可使用本校之無線網路。

6、訪客、廠商及其他校外人士若需要使用本校之無線網路，需由相關單位向圖資處申請提供臨時帳號予校園內活動或會議等場合使用，活動結束後，立即停止該帳號之臨時使用權。

7、為避免干擾無線網路之運作，無線網路使用頻道（channel）必須以圖資處設定為優先，私架設備不能干擾本校基地台之運作。

8、基於協助防治網路違規及犯罪之目的，於網路系統提供多人使用時，需採行適當之使用者認證機制，並記錄使用者登入帳號、使用起迄時間、使用之 IP 位址、MAC 位址等使用紀錄資料，以執行必要之系統管理與安全維護作業。

9、本校連入與連出的網路流量，需透過防火牆控管，使用白名單(已涵蓋常用連線需求，特殊連線開放單位個別申請)，未在白名單的流量一律被阻擋。

10、其他有關校園網路管理之事項。

(二)使用者若發現網路安全有任何缺陷，應盡速通報圖資處。

四、網路系統使用者如有違反本規範之情事，圖資處得停止其使用校園網路或相關網路資源。

第十三條、網路 IP

一、本校網路 IP 位址係以提供校內各系所與單位教學研究、辦理公務使用。

二、圖資處負責校園網路 IP 位址申請與設置，區分：

(一)行政區：凡本校教師、職員、助理，可經本校「單一登入平台」提出 IP 及網域名稱申請或填具「IP 申請表」，填妥申請用途、使用期限、管理者等資訊，經圖資處核可通過，即配發一個固定 IP 位址(與網域名稱)供使用。

(二)教學區(各院科系所教室/實驗室)：

1、 由圖資處統一規劃，依電腦數量透過系統自動派發 IP 位址，若管理單位有特殊需求得另行提出固定 IP 申請。

2、 各系所實驗室應指派一至二位網路管理人員。

(三)連網設備：除了需提供外界存取之伺服器之外，其餘印表機、網路攝影機、門禁、電控等連網設備，以設定虛擬 IP 位址為原則，若有使用實體 IP 之需求，得另行提出申請。

(四)IP 配額限制：

1、 個人 IP 上限： 2 個。

2、 教師實驗室與研究計畫合計 IP 上限：5 個。

3、 若有超過上限數量之需求需以專案方式向圖資處提出申請。若已逾上限數量規定者，不強制收回現有 IP，但不開放後續申請。

(五)圖資處定期盤點 IP 使用狀況，若已配發之 IP 超過一年未使用，將主動收回重新分配。

(六)經配發之 IP 將於後續每年透過系統自動詢問是否申請續用，圖資處仍保留回收之權利。

三、使用規範

(一)IP 使用者管理：

1、校內各單位 IP 位址發放給使用者後，一經網路卡(MAC Address)及 IP 位址註冊後，除重新於上述申請平台提出修改申請，不得自行更換或非法使用他人 IP。

2、若所申請 IP 用途為設備或系統，當管理者因職務交接、離職或其他原因發生更換，應於上述平台提出修改申請。

3、經查獲擅用未經申請之 IP 者，圖資處得封鎖其設備之網路連線能力。

(二)遠端連線需求：

1、定義：遠端連線是指於校外網路透過遠端存取方式，連線校內網路限定之服務系統或校內資訊設備(含微軟遠端桌面服務及其他遠端軟體)。

2、本校遠端連線由防火牆統一納管，需於校外進行遠端連線者，遵循下列規定辦理：

(1)教職員及學生：至單一登入平台下載並安裝「校外 VPN 連線認證」，完成設定後以 VPN 方式連線存取校內資源。

(2)委外廠商：因維運需要於校外進行遠端連線者，須向圖資處提出申請，經核准後，方得於核准期間開放指定 IP 之連線。

(3)遠端連線操作應謹慎執行，若因不當操作所引起之系統故障、損毀，由申請連線單位負責修復或賠償。

(三)特殊網路需求：若單位有大流量存取、開放特定服務連線、學術研究網路測試、架設 DHCP、DNS 等特殊網路需求，需向圖資處提出申請，於確認其配置方式與架構不影響整體網路後始可運行，後續架構調整仍需知會圖資處。若私自架設造成網路異常，影響他人者，圖資處得封鎖其設備之校內網路連線能力。

(四)申請之 IP 所屬設備發生下列情形，圖資處得先行封鎖該設備之網路連線，並通知管理者限期改善，經確認相關狀況改善後，始恢復連線使用：

1、遭惡意程式感染、入侵，或被植入後門程式者。

2、存在已知弱點或漏洞，未即時更新修補者，經通知後仍不處理者。

3、進行網路攻擊、連結不當或高風險網站、流量異常（含大量連線、掃描、濫發）等，或其他足認有資訊安全疑慮之行為者。

4、散佈、提供下載或協助傳播惡意軟體者。

5、經教育部或上級機關通報資安事件者。

6、管理人員聯繫方式失效、無法聯絡或不處理圖資處要求之改善通知。

7、其他可能影響網路及服務正常運作或有資安風險之情形者。

8、違反本執行辦法所定應遵守事項者。

第十四條、網路流量異常

一、流量係指本校進、出校外網路之流量，依據本校圖資處核心及重要交換器之網路流量進行每日流量統計。

二、電腦使用網路有下列之行為者，將被視為異常，將依資訊安全事件處理，並立即停止該電腦之網路使用權，須完成資訊安全事件處理流程後，方可恢復其網路使用，被停用 IP 名單公布於本處資訊安全專區-資安通報事件網頁以供查詢。

(一)單一 IP 位址如有異常大量上傳、下載或其他足以影響校園網路正常運作之使用情形。

(二)中毒、遭入侵或被植入惡意程式之情形，或有其他疑似資通安全事件之情形。

(三)未經授權進行連接埠（Port）掃描、IP 掃描、弱點探測，或其他類似網路探測行為。

(四)對外或對內進行網路攻擊、散布惡意程式、傳送異常或惡意封包，或其他危害網路與資訊安全之行為。

(五)異常發送垃圾郵件、廣告信函、詐騙訊息，或其他濫用網路資源之行為。

(六)經教育機構資安通報應變相關單位、其他機關（構）、校內外使用者或管理單位通報有異常情形，並經查證屬實。

第十五條、電子郵件

一、本校編制內教職員工及學生均配置一組電子郵件帳號，單位公務用、計畫、業務或臨時性公務用與短期兼任教師等特殊需求可另行申請信箱。

二、本校電子郵件信箱係提供本校教職員工生從事公務或學術活動使用，校內單位辦理公務業務或核心業務時，應使用本校配發之電子郵件信箱，不得使用非公務信箱進行收發。

三、電子郵件使用安全規則：

(一)為防範不可抗力因素導致資料遺失，重要資料由使用者負責備份，並且妥善維護信箱容量，以免超出容量限制，影響使用者電子郵件正常運作。

(二)使用者請勿開啟來路不明之電子郵件及其附件內的連結及執行檔，以免被植入木馬程式、病毒或勒索病毒。

(三)當使用電子郵件系統傳輸機密或敏感性資料時，應對附件進行加密後傳送，密碼請以其他管道告知收件者。

(四)使用電子郵件寄送 2 人以上之郵件應使用「密件副本」方式傳遞。

(五)電子郵件帳號疑似為垃圾信件發送者或侵害郵件系統正常運作，本校有權採取緊急停權處置。

(六)使用者辦理公務、及重要（或敏感）專案應使用本校提供之電子郵件信箱，不得轉至外部私人信箱收發公務資訊。

(七)教職員如轉任不得使用學校電子郵件信箱收發公務機關相關電子郵件。

(八)使用者如因故無法使用公務信箱讀取訊息，以致影響公務執行，得由直屬單位主管簽陳校長同意後委請圖資處電子信箱管理人員代為調閱信件讀取公務信箱相關內容。

第十六條、即時通訊軟體

一、本校同仁使用即時通訊軟體處理公務時，應注意駭客竊取資料、假冒詐騙和操作不慎致公務資料外洩等資安風險。

二、安裝與使用：

(一)安裝程式請由官方網站下載，勿透過未知來源連結或網站隨意下載使用。

(二)安裝時僅授權軟體必要使用權限，避免洩漏過多個人資訊。

(三)依各廠牌即時通訊軟體原廠建議進行安全設定。

(四)安裝即時通訊軟體之電腦、筆電請安裝防毒軟體且保持正常運作。

(五)行動裝置不宜取得超級使用者權限等破壞原廠安全機制之行為。

(六)裝置之系統及通訊軟體版本必須保持最新版本，確保使用安全。

(七)隨時注意工作群組是否有陌生人士加入，避免資訊外洩。

三、公務訊息傳遞：

(一)使用即時通訊軟體以傳送溝通訊息為主，內容避免涉及機密性、安全性、隱私性、敏感性或洩漏個人資料，以確保資訊資產受到適當等級之保護。

(二)不應使用即時通訊軟體傳遞之資料(訊)類型如下：

1、 依政府採購相關法規有保密必要者。

2、 決策形成前有保密必要者。

3、 具名或具體內容之檢舉、陳情案件。

4、 調(檢)查獲處理中有保密必要者。
5、 各項法規所列機密(保密)事項。
6、 為執行電腦系統安全管理相關作業事項。
7、 涉及隱私或個資。
8、 因承辦公務知悉或持有他人秘密。
9、 機關人事資料。
10、其他非機密，若不當公開或外洩可能造成決策困擾、個人或機關信譽非必要損害等負面效應事項。

(三)不隨意以任何形式散布通訊內容至任何公開或特定公開之網站。

第十七條、物聯網設備

一、定義：定義：物聯網設備係指處理公務具網路連線功能之設備，包含無線網路基地台/無線路由器、網路攝影機、網路印表機、門禁設備、環控系統、數位播放器、無人機等。

二、單位應建立物聯網設備管理清冊，並至少每年更新一次。

三、單位應訂定物聯網設備安全性更新機制，以維持設備之整體安全性。

四、單位應確認所屬物聯網設備皆具備身分驗證機制，且禁止使用設備預設帳密及弱密碼，密碼長度應配合中央主管機關規定，且應包含英文字母大小寫、數字與特殊符號要素之組合，並配合本校資安政策定期更換密碼。

五、單位應管制設備連線範圍，僅允許申請內部 IP 使用，不開放校外連線。惟若因業務需求需開放校外連線，應填寫 ISP-04-018-001 防火牆規則變更申請單，經圖書資訊處審核後始得開放連線。

六、若無法落實本條第三、四、五項之安全控管規範，應建立補償性管控機制，如：限制網際網路連線能力、加強存取控制或進行網路連線行為監控等。若設備存在已知弱點且無法修補或更新，應訂定汰換期程。

第十八條、資通安全教育訓練

一、一般使用者及主管：每年完成 3 小時資通安全通識教育訓練，搭配課後測驗合格者取得受訓時數。

二、資訊人員:泛指單位從事資通系統自行或委外開發、維運者，每人每二年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練，搭配課後測驗合格者取得受訓時數。

第二節、系統服務

第十九條、伺服器

一、為提升本校伺服器之資訊安全及網路服務品質，以符合智慧財產權等相關法令，訂定本條文。

二、適用對象：本校教學及行政單位（以下簡稱各單位）所有對外開放網路服務之伺服器。

三、本校各單位所架設之伺服器，其使用需遵守下列各項規定，並擔負與該伺服器有關一切行政及法律責任：

(一)本校相關網路使用規範

(二)台灣學術網路使用規範

(三)其他相關法律之規定

(四)對外連線原則禁止，例外開放(不含使用者端，採申請制)

(五)網站僅放行 HTTPS

四、申請、註銷：

(一)各單位欲架設伺服主機，須有專人進行維護管理，並需填具「ISMS-04-014-004-IP 申請表」，向圖書資訊處提出申請，經審查核准後始可架設。

(二)個人使用者不得私架伺服器，以避免不當資訊安全事件發生。

(三)已申請登錄伺服器如不需使用時，原申請單位或人員得向圖書資訊處辦理註銷。

(四)系統、資訊設備有對外連線需求，請填具「ISMS-04-014-004-IP 申請表」，向圖書資訊處提出申請，經審核查准後開放對外連線。

五、管理、維護

(一)各單位對外提供網際網路服務之伺服器，須有專人負責維護並進行相關資訊安全作業。

(二)各單位應負其單位內所提供伺服主機網路服務之督導責任。

(三)各單位伺服器管理者，須定期為所管理之機器進行相關安全性、漏洞、弱點等系統補強，圖書資訊處得不定期對列管之伺服器進行資訊安全檢測，以避免遭駭客入侵。

(四)管理者應注意提供服務內容的合法性，不得有猥褻、攻擊、商業性及侵犯智慧財產權之情形。

(五)各種服務系統中所提供之服務，如網頁瀏覽或軟體下載，內容較有爭議者，建議於首頁宣告通知使用者。

(六)單位內提供檔案傳輸伺服器(FTP)，應注意分享檔案之合法性，若由廠商或版權擁有者所提供合法分享軟體，應註明廠商或版權擁有者名稱及授權資料。

(七)台灣學術網路係提供各學校及研究單位學術用途，校園網路內不得提供商業性網路服務，亦不可提供具商業廣告性質之免費網路服務（含郵件伺服器、網頁伺服器及其他伺服器）。

(八)退（離）職人員應依資訊安全規定及程序，由伺服器管理人員取消存取網路權利。

(九)各單位伺服主機須有專人定期（每學期不得少於 1 次）清查伺服器資訊內容並記錄、追蹤處理情況。

(十)伺服器負責人員、維護人員應參加本校每年不定期所舉辦之資訊安全講習、演練及遵守相關規定。

六、各單位伺服器若有進行非所宣稱之服務、遭駭客入侵、發生異常流量、對外攻擊之資訊安全事件、發廣告信、違反智慧財產權或違反本條文第三點規定等情事時，依本校「校園網路使用規範要點」處理，圖書資訊處可依情節狀況停止該單位或該伺服器之網路連線權利。

第二十條、雲端虛擬主機

一、本服務係指使用者依其需要，向本校圖書資訊處(以下簡稱圖資處)提出雲端虛擬主機租用申請，以取得計算、網路、資料儲存等資源之服務模式。

二、本服務免費提供本校各單位與教師於研究、教學及公務上使用。亦提供收費的服務給計畫申請使用，視申請需求與當下硬體資源考量，圖資處得保留核發與否之權力。單位申請前述免費與收費空間，均需提供圖資處管理者權限，以於特殊情況時可第一時間介入處理。

三、本服務提供基本硬體運作平台、網路相關設定、網路故障排除與虛擬主機(VM)備份等基礎維運服務；租用單位應妥善管理虛擬主機內部之維護調整與服務建置。如租用單位有特殊維護需求，得向圖資處提出並視相關資源協調。服務租用期間，若遭遇不可抗力因素致使

服務停擺，應視權責分屬，由圖資處或租用單位窗口即刻於相關管道發布暫停服務訊息，並敘明估計災害復原時間與最新處理狀況。

四、圖資處備份服務將視空間資源調整備份保留天數，租用單位仍應自行做好資料備份工作，若因系統或設備障礙、阻斷、以致發生資料錯誤或毀損，本校不負損害賠償責任。

五、若遇不可抗力因素，圖資處保留與租用單位協調，進行網路或空間資源調整之權利，調整期間得暫時中止本服務運作。

六、為維持本服務有效性與設備運作效益，租用單位需指定專人管理租用主機，以作為服務聯絡窗口。租用單位之管理人員應對申請本服務所提供之內容負責，不得違反本執行辦法及相關法令規定，並應配合圖資處資通安全及隱私管理規範（ISP）相關稽核規定。

七、如發生相關情事或欠繳租用費，圖資處得依相關規定處理先行暫停本服務，並通知租用單位改善，改善期間仍列入租期。

八、校外計畫服務申請採使用者付費原則，申請者得以研究計畫中編列相關費用等支付，租用費用須於租用申請時支付。租用費收入納歸校務基金管理。

九、收費標準參考下表一。租用單位因租用方案不符需求，需以專簽方式申請特殊規格服務，圖資處得以專案方式辦理，價格另議。

十、本辦法租用收費，適用「國立高雄師範大學校務基金自籌收入收支管理辦法」第二條第五項「場地設備管理收入」之範圍，並依「國立高雄師範大學空間分配及管理要點」規定，提撥總收入之百分之七十充實校務基金，剩餘百分之三十用於支應本校資訊機房之設備擴充與維護，及例行汰換使用。

表一.國立高雄師範大學雲端虛擬主機租用收費標準如下表

- 收費標準：

租用方案	A方案	B方案	C方案
CPU（核心數）	1	2	4
記憶體（GB）	1	2	4
硬碟（GB）	20	40	60
租用費/月 （元）	1000	3000	5000

備註：租用費內含作業系統授權費用、防毒軟體授權費用、VANS 電腦組態工具授權費用及 5%營業稅。

- 租用方案與增購項目合計，不得超過總租用上限之限制。

增購項目	CPU	記憶體	硬碟
規格	1 核心	1 GB	10 GB
增購租用費／月(元)	400 元	400 元	600 元
租用上限	8 核心	16GB	甲、GB

第二十一條、多元繳費平台

一、為管理國立高雄師範大學(以下簡稱本校) 多元繳費平台服務(以下簡稱本服務)，特訂定本校多元繳費平台使用管理條文。

二、本服務係指使用者依其需要，向本校圖書資訊處(以下簡稱圖資處)提出多元繳費平台使用申請，以取得 ATM 虛擬帳號、臨櫃繳費單、國內外信用卡、行動支付等繳費通路之服務模式。

三、申請資格：凡本校各單位，均得依本辦法申請使用本服務。

四、申請方式：填寫申請單，說明使用需求，經圖資處審核通過得以使用網頁繳費入口與 API 串接等服務。

五、服務內容：

(一)網頁繳費入口，提供使用者進行繳費說明維護。

(二)API 使用及介接方法諮詢，可供委外開發之系統使用，須由使用者安排廠商進行介接。

(三) 繳費狀況查詢，支援使用者對帳作業。

六、本服務免費提供本校於招生、募款及公務上使用。亦提供收費之服務給予非屬前項使用、校外人士參加本校主辦活動與研討會等申請使用，視申請需求、交易對象與當下資源考量，本校得保留收費與否之權力。

七、本服務提供基本軟硬體運作平台、網路相關設定、故障排除與主機備份等基礎維運服務。服務使用期間，若遭遇不可抗力因素致使服務停擺，本校即刻於相關管道發布暫停服務訊息，並敘明估計災害復原時間與最新處理狀況。

八、圖資處備份服務將視空間資源調整備份保留天數。

九、為維持本服務有效性與平台運作效益，申請單位需指定專人作為服務聯絡窗口。

十、使用申請採交易付費原則，申請者得以編列相關費用(包括本使用費)，使用費收入納歸校務基金管理。

十一、收費標準：

(一)使用費：每筆成功交易酌收 15 元。

(二)使用單位因付費方案不符需求，需以專簽方式申請特殊需求服務，圖資處得以專案方式辦理，價格另議。

十二、本使用收費適用「國立高雄師範大學校務基金自籌收入收支管理辦法」第二條第二項「場地設備管理收入」之範圍，並酌予參照「國立高雄師範大學空間分配及管理要點」規定，提撥總收入之百分之七十充實校務基金，剩餘百分之三十用於支應本服務所需之平台系統擴充與維護，及例行汰換使用。

第二十二條、外部廠商教育版雲端服務

一、一般規範

若使用者有下述行為，本服務得隨時停止，毋須通知：

(一)違反「國立高雄師範大學校園網路使用規範要點」、教育部「臺灣學術網路使用規範」、以及國家所制定之各式法律規章。

(二)違反供應服務之公司之「服務條款」。

(三)利用本服務從事法律所禁止之侵害他人權利或違法行為。

(四)未經合法授權而截獲、竄改、收集、儲存或刪除他人個人資訊、電子郵件或其他資料，或將此類資料用於任何非法或不正當目的。

(五)冒用他人名義使用本服務或轉讓給他人使用。

(六)其他本校有正當理由認為不適當之行為。

二、服務使用

(一)個人身分必須為本校教職員工生，狀態為在職、退休或在校(含休學)、校友；單位身分必須為計畫/單位/中心/社團。

(二)休學生復學成功後身分同在校教職員生。

(三)有網路使用不良紀錄之使用者，本校得拒絕提供或停止提供服務。

(四)推廣班學生修課期間身分同在校教職員生，修課結束後帳號保留時間為 1 個月，屆期

進行帳號刪除。

(五)外部廠商之政策、服務內容或本校租用相關服務之管理規定有所變動調整或停止提供服務時，相關訊息將統一於本校網站公告。

(六)依服務使用規範合理使用，減少不當使用及降低資通安全威脅。

三、服務停用、復權與帳號刪除

針對個別使用者，以下項目任一要件成立時，本校將暫停或取消本服務：

(一)使用資格失效者，如離職或退學，離校前請務必自行備份相關資料，本校不提供備份或保留資料之服務。

(二)一年內從未登入者進行停用帳號，帳號保留三個月，未於保留時間提出復權申請者，屆滿後逕行刪除帳號。

(三)使用容量超過規定上限，經通知未改善而遭停用帳號者，帳號保留三個月，未於保留時間提出復權申請者，屆滿後逕行刪除帳號。

(四)未遵守供應服務之公司之服務條款，遭該公司停用帳號者請逕洽該公司聯繫反應，如三個月內未恢復使用權者，即刪除帳號。

四、資料刪除復原

本服務為供應服務之公司提供，當主動或誤刪資料、申請退出服務或帳號遭刪除後，資料將隨之刪除，無法復原。

五、服務終止

以下項目任一點成立時，本服務可能終止：

(一)供應服務之公司更改服務條款、授權範圍或收費方式，導致某些身份遭排除，或本校已不符合授權條款。

(二)供應服務之公司終止此項服務。

(三)本校終止提供此項服務。

六、免責聲明

(一)一、本服務隱私權與安全性義務由供應服務之公司負責，本校並無進行任何資料備份與保留。關於供應服務之隱私權與安全性的義務，請參考該公司之安全性與隱私權說明。

(二)使用者透過本服務所產出的資料係由供應服務之公司負責保管及維護，本校無法干涉資料被利用方式，也無法保障隱私權。使用本服務前，請先詳閱及同意該公司之安全性與隱私權政策。

(三)本服務的系統穩定性及資料保存，係由供應服務之公司維運提供，故本校無法保證服務穩定性及資料完整性，請使用者自行備份資料以避免風險。

(四)本服務涵蓋的應用種類繁多，本校僅協助帳號啟用之服務，恕無法提供各應用之正確諮詢，請使用者自行參閱供應服務之公司提供之使用說明。

(五)爾後若有使用疑問、記錄調閱、權利申覆或法律訴訟等需求，請逕洽供應服務之公司辦理。

七、本校保留因營運策略之調整，隨時更改或停止各項服務內容之權利，且毋須事先通知使用者。無論任何情形，就停止或更改服務之決定，對任何使用者或第三人均不負任何責任。本校建議您應自行留存備份。

第二十三條、機敏空間

一、為管理大樓內資訊安全與人員網路行為，特訂定本辦法。

二、進出大樓之機敏空間人員分為五類:

(一)A.大樓內機敏空間之管理人員。

(二)B 類：大樓內之工作人員，可以進出機敏空間。

(三)C 類：大樓內之工作人員，無法進出機敏空間。

(四)D 類：長期訪客，指駐留機敏大樓的期間會超過三個月。

(五)E 類：短期訪客，指駐留機敏大樓的期間會短於(含)三個月。

三、大樓(含機敏空間)應設置門禁及監視設備，均須具備不斷電系統，電力中斷時至少維 持三個小時以上的運作。

四、大樓若遇超過三小時之長時間停電，館內人員須於時間內撤離完畢。

五、大樓門禁規則：

(一)進出一律透過刷卡或輸入密碼。

(二)A、B、C、D 類人員，所攜帶可連網之所有計算機設備均須經過資安檢驗，以保障 本校機敏性資料無外洩疑慮。

(三)E 類人員，所攜帶可連網之計算機設備，須安裝防毒軟體，始可連網使用。

六、機敏空間門禁規則：

(一) 人員進出機敏空間須配合 ISMS 稽核，紀錄進出之相關資料(含 ISMS 稽核表及影像)並由 A 類人員全程陪同。

(二)所需攜帶進入機敏空間之物品，均須經過查驗，始得攜帶。

七、大樓內需建置無死角之監視環境，影像紀錄需儲存至少三個月。

八、資訊安全稽核

稽核內容為可連網之所有計算機設備中之帳號密碼強度、防毒軟體安裝及掃瞄、安裝作業系統更新與其他資訊安全要求。

(一)A、B 類人員之稽核週期為每週。

(二)C、D 類人員之稽核週期為每月。

(三)E 類人員則依進出狀況，由稽核人員不定期稽核。

(四)或經資安通報，需直接對該設備之使用者進行稽核，適用所有類別人員。

(五)上述相關稽核規則，受稽核者須配合辦理。

九、 上述相關規範若有違反事實者，將提報ISMS委員會進行檢討與修正。另有其他違法行為時，應依民法、刑法、著作權法或其他相關法令負法律責任。

第三章 個人資料保護

第一節、 個人資料蒐集

第二十四條、 個人資料範圍

一、本規範所稱個人資料、個人資料檔案、蒐集、處理、利用及傳輸等名詞，依個人資料保護法第二條規定。

二、適用範圍包含本校於蒐集、處理、利用、傳輸程序中所形成之各種形式個人資料檔案，包含書面、電子及個人生理特徵資料。

三、生物特徵個人資料包括指紋、臉部特徵、虹膜、聲音、掌紋、靜脈等；原始生物特徵資料，指以掃描器、相機等感測器蒐集之原始資料；特徵值，指經技術或演算法轉換後供比

對之不可逆資料。

第二十五條、 蒐集目的及核心原則

一、個人資料之蒐集，應有特定目的，並限於執行法定職務、行政管理、公共衛生與傳染病防治或其他合法目的所必要範圍內為之。

二、蒐集、處理、利用或傳輸個人資料，應遵循誠實信用、資料最小化、目的關聯性及不得逾越必要範圍等原則，並應尊重當事人權益。

三、因特定目的蒐集處理個人資料者，應符合個資法及相關法律規定，並以不侵害當事人權益為前提；涉及公共利益者，亦應以必要性為限。

四、各單位建立個人資料檔案後一個月內，應依規定報請個資主管單位，公開檔案名稱、保有機關名稱、業務主管單位及聯絡方式、保有依據與特定目的，於本校網頁供公眾查詢，其有變更者，亦同，以落實透明原則。

第二十六條、 蒐集方式

一、個人資料得以當事人親送、填寫、郵遞、資訊系統取得，或依法由校內相關電子系統支援匯入之方式蒐集。

二、蒐集前應明確告知當事人機關或單位名稱、蒐集目的、個人資料類別、利用之期間／地區／對象、當事人得行使之權利、申訴或諮詢管道，以及不提供資料可能影響之權益；法定免告知者，不在此限。

三、蒐集非由當事人提供之個人資料者，應於處理或利用前告知資料來源及前述應告知事項；法定免告知者，不在此限。

四、依法須取得同意者，應先取得當事人同意；使用生物特徵辨識技術蒐集個資時，應先取得當事人同意，未成年學生並應取得法定代理人同意。當事人不同意提供生物特徵資料時，應提供替代方案。

五、各單位因執行法定職務而需運用非主管之個人資料時，除另有規定外，應填具申請單，記載所需項目、運用方式及目的、屬於執行法定職務之說明、預估運用期間、個資運用後之處理方式，送請業務主管單位、個資主管單位核定後取得。

六、各單位所需運用之非主管個人資料，如屬全校性之個人資料，個資主管單位核定後應送請校長備查；如屬有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，應送請校長核准。

七、於當事人得自由選擇是否提供個資之情形下，應明示不提供之影響；防疫必要資料之蒐集，如拒絕提供，得影響入校或參與活動資格。

第二節、 個人資料處理利用

第二十七條、 處理利用一般原則

一、個人資料之處理與利用，應與原蒐集目的具有正當合理關聯，並應經適當審核及行政程序為之；其處理、利用歷程應做成紀錄並保存。

二、個人資料得以自動化或非自動化方式處理與利用，但不得任意公開上網、任意揭露，或以非業務必要方式處理。

三、公布名單、寄送資料或揭露資訊前，應審慎評估是否可能造成當事人困擾或權益受損，必要時採遮蔽、加密、個別寄送等措施。

四、生物特徵個人資料之處理，應以轉換為特徵值後再行處理為原則；特徵值如需連結其他個資，應採代號、代碼或其他假名化方式，並遵守資料最小化原則。

五、個人資料有錯誤或缺漏時，應儘速更正或補充，並通知曾利用該資料之單位；資料正確性有爭議時，應停止處理或利用，但法令另有規定或經當事人書面同意者，不在此限。

六、應設置申訴或諮詢窗口，保障當事人查詢、閱覽、請求複製、更正、刪除及停止蒐集、處理或利用之權利；查詢、閱覽及複製申請原則上應於十五日內准駁，更正、刪除及停止蒐集、處理或利用申請原則上應於三十日內准駁，必要時得依法延長。

第二十八條、 目的外利用

一、個人資料原則上不得逾越原蒐集之特定目的而利用。

二、生物特徵個人資料應與蒐集之特定目的相符，不得為目的外利用。

三、原蒐集特定目的範圍變更時，應先確認原合法要件是否仍然存續；其未存續者，應再取得當事人同意，並建立控制與紀錄機制。

四、個人資料如有公開需求或提供第三人之必要，除法令另有規定外，應先取得當事人同意。防疫蒐集資料如將來需作目的外利用，亦應依法先行取得書面同意。

五、違反法令蒐集、處理或利用個人資料者，應刪除或停止處理、利用，並保存相關紀錄。

第二十九條、 利用之期間、地區、對象

一、個人資料蒐集時，應明確告知其利用之期間、地區及對象。

二、一般個人資料之利用期間，應以達成特定目的所必要之期間為限，並依法定或核定之保存年限管理。

三、防疫蒐集資料屬特殊情形者，實聯制資料之利用期間自蒐集日起二十八日內；其餘防疫個資之處理及利用時間，以最長至防疫結束為限。

四、個人資料利用地區，以國內及與本校有業務往來之國內外機構所在地為限。

五、個人資料利用對象，以本校教學行政相關業務人員、依法有調查權機關、主管行政機關及法令所定必要受領者為限；防疫必要時，得提供衛生主管機關進行疫情調查及聯繫。

第三十條、 安全維護措施

一、本校設置數位安全與治理委員會，下設「個資保護執行組」及「內部稽核組」，辦理個資保護、安全維護、盤點、風險評估、稽核及教育訓練。

二、應依最小權限原則進行存取控制；涉及特種個資或敏感個資者，應採加密儲存，並符合個資法及相關資安規範。

三、生物特徵原始資料原則上不留存；如有留存必要，應與特徵值分別加密，儲存於不同媒體，並採嚴謹之存取管控措施。

四、紙本資料、隨身儲存設備及大型儲放個資空間，應有鎖櫃、門禁、環控、備份、防毒、螢幕保護、桌面淨空及資料屬性標示等安全措施。

五、不得蒐集、儲存、顯示非業務必要之個資，亦不得將個資隨意公開上網，或使用生成式 AI 處理個資。

第三節、 個人資料傳輸銷毀

第三十一條、 個人資料傳輸

一、 個人資料傳輸應遵守必要性、合法性及機密性原則，並以執行法定職務、核定目的或依法提供為限。

二、 網路傳輸應採 HTTPS 加密傳輸，並使用 TLS 1.2 以上版本；經圖資單位協助辦理之電子申請、資料審核與傳遞，應以加密或其他安全方式為之。

三、 含有個資之紙本資料傳遞時，應予密封，必要時於封口處彌封。

四、 跨系統匯入、系統間支援、或由非主管單位取得資料時，應經權責單位核准；涉及圖資單位協助者，應加會圖資處。所有個資相關公文亦需加會圖資處，以利資訊統一。

五、 對外傳輸或提供個人資料，除法令另有規定外，應以當事人同意或法定授權為依據。

第三十二條、 個人資料銷毀

一、 個人資料蒐集之特定目的消失、利用期限屆滿、業務終止、已無保存必要，或經認定有違法蒐集、處理、利用情形時，應刪除、停止處理或利用，並儘速銷毀。

二、 防疫實聯制等資料僅得保存二十八日，屆期應填具銷毀申請書主動刪除或銷毀。

三、 各單位經核准運用之非主管個資，於行政目的達成後，如無保留必要，應填具銷毀申請書並辦理刪除或銷毀；含有個資之廢紙，應以碎紙或專人方式銷毀。

四、 如仍有保留必要，應由該單位確實依照「大專校院類檔案保存年限基準表」暨校本校「國立高雄師範大學檔案分類及保存年限」訂定保管年限，各單位依實際需求訂定保存年限超過法定保存年限，應說明保存理由並訂定保存年限上限。

五、 刪除、停止處理利用及銷毀措施，均應留存相關紀錄，以供查核。

第四章 智慧財產權保護

第三十三條、 館藏資源、影音光碟暨影印服務規則

一、館藏資源

(一)使用館藏資源時，請確實依著作權法及相關規定，在合理使用範圍內從事重製（影印、列印、掃描、複製等）行為，不得大量複製散播。

(二)使用館藏資料或電子資源時，請確實遵守著作權法及相關規定。請勿大量下載或利用自動下載軟體擷取資料，下載之全文資料，請勿於網路上公開傳佈。

(三)於首頁建置相關著作權法規專區，讓使用者易於了解使用範圍與相關限制。

二、影音光碟

(一)嚴禁擅自拷貝或轉錄圖書館視聽資料及未經同意即移動各項多媒體設備。

(二)視聽資料區張貼，保障智慧財產權，合法影印，遵守著作權法與相關法令規定等宣導文字。

三、影列印服務

(一)圖書館的影印、列印服務旨在方便讀者研究與學習，但必須遵守著作權法之「合理使用」規定。

(二)請使用者確實遵守『著作權法』及『智慧財產權』之相關法律規定，勿影印盜版教科書，或進行非法影印。

(三)使用者委託影印之文件資料，僅供學術研究，不得擅自重製、出版、銷售，以免侵害著作人之權益。

(四)為保護環境資源，可多加利用電子掃描傳輸，以減少紙張之使用。

(五)圖書館加強張貼宣導標語，提醒尊重智慧財產權，違反相關規定者，一旦查證屬實，讀者需自行負擔相關法律責任。

第五章 人工智慧倫理

第三十四條、 教學人員研究與教學應用

一、教學人員得依課程目標及教學需求，適度運用人工智慧(AI)與生成式 AI 工具(以下簡稱 AI 工具)輔助教學設計、教材製作或反饋機制等教學用途，惟應履行人工審閱與校正義務，確保其正確性、專業性與符合教學倫理，並視必要性評估標註「本教材含 AI 生成內容」等說明。

二、課程對於 AI 工具之使用限制，應於教學大綱或作業說明中明確揭露。辦理各類考試評量時，應採取必要防護措施及多重評量設計，以維護評量公平。

三、運用 AI 技術協助教學診斷或個別化學習時，資料之蒐集、處理與利用應符合法規及本校數位安全治理政策。

四、研究流程使用 AI 工具應遵守研究倫理與論文投稿規範，並依所屬學術領域、出版機構及本校規範，覈實揭露使用情形及範圍，確保研究之可驗證性及信實度。

五、涉及不當使用 AI、偽造內容、抄襲或違反學術誠信者，依本校《學術倫理管理辦法》、《推動教師學術自律實施要點》、《教師違反送審教師資格規定及學術倫理案件處理要點》及相關規定辦理。

第三十五條、學生學習與評量使用

一、學生可於教學人員允許與規定範圍內使用 AI 工具作為學習、探索與創作輔助工具，惟 AI 工具生成內容非經教學人員明示允許，不得作為個人原創作品繳交，且應依教學規定註明引用來源及生成方式。

二、學生於測驗、評量、線上考試、遠距評量、學習診斷或其他需反映個人能力之範圍：

（一） 若教學人員或單位明示禁止使用 AI 工具，學生不得以任何形式（含隱匿操作、背景執行、外部裝置等）使用 AI 輔助作答。

（二） 若教學人員未明示允許使用，即視為不允許使用。

（三） 利用深偽技術(Deepfake)進行身分冒用或代考，視同重大舞弊。

（四） 違反前述規定者，依本校學術倫理或考試違規相關規定辦理。

三、 評量結果如具 AI 協助作答之疑慮，學生應負舉證責任，配合提交原始草稿、提示詞紀錄（Prompt Records）、推導歷程或參考資料，並得視需求參與口試以供查核。

四、 學生之作業、報告、論文或創作，經認定有不當使用 AI 工具之疑慮，應綜合審查以下要項：

(一)學術能力與過往作品之顯著差異。

(二)原始草稿、提示詞紀錄與生成歷程軌跡。

(三)資料引用、論述邏輯及內容一致性。

(四)AI 偵測工具之結果僅供查核參考，不得作為判定違規之唯一依據。

五、 經查證認涉及不當使用 AI 工具、偽造內容、抄襲或違反學術誠信者，依本校《學術倫理管理辦法》、《碩博士學位論文違反學術倫理案件處理要點》及相關規定辦理。

第三十六條、 行政人員與行政作業之應用

一、 行政單位使用 AI 工具於處理公務文書，應進行必要之人工審核與驗證，確保資訊正確性與適法性。

二、行政單位辦理採購時，如涉及 AI 技術、相關系統或取得含 AI 功能之服務，應於契約明訂 AI 人工智慧倫理規範、著作權歸屬及賠償責任等，並要求得標廠商遵守本校相關規範。

三、校內研究中心開發自有 AI 模型，應建立模型偏見監控機制，並揭露模型準確度、限制事項及資料來源。

第六章 內部監督

第三十七條、　資通安全及個人資料保護稽核

一、本校各單位辦理資訊安全稽核相關作業依本辦法之規定；本辦法未規定者，準用行政院及所屬各機關資訊安全管理要點之規定。

二、資訊安全稽核區分如下：

(一)外部稽核：指由機關或單位委託專家、學者或專業資安稽核廠商之公正第三方規劃辦理之稽核作業。

(二)內部稽核：指由本校對內部單位自行規劃辦理之稽核作業。

三、資訊安全稽核頻率如下：

(一)「外部稽核」得視本校資安業務實際需求定期或不定期辦理。

(二)「內部稽核」作業次數，依據本校內部稽核管理作業程序書規定每 2 年辦理 1 次，必要時可視需求不定期辦理，並就本校資通系統（保有個人資料）風險高低、教學單位特性訂定先後順序，規劃全校各單位分年分階段執行內部稽核。

四、各單位應指派資訊安全管控人員一至二名，作為所屬單位資訊安全稽核及其他應辦事項之聯繫與維護窗口。

五、各受稽核單位於稽核前均須填列資安稽核相關表單，並備妥相關文件，以利稽核；且實施稽核作業時，得調閱受稽單位有關資料、實地測試及檢查資訊軟、硬體設備使用情形。必要時，得由資訊相關人員或資訊安全稽核人員提供說明及專業諮詢意見。

六、資訊安全稽核作業實施範圍，應以系統存取控制管理為主，參酌本校資訊現況，針對下列事項，稽核其系統存取有無異狀及實施情形是否符合相關法令之規定：

(一)資產管理。

(二)人力資源安全。

(三)實體與環境安全。

(四)通訊與作業安全。

(五)存取控制。

(六)其他資訊安全管理事項。

七、資訊安全稽核作業程序如下：

(一)綜合分析機關資訊系統特性、系統存取政策、系統異常存取狀況及授權規定或其他使用管理規定，據以研（修）訂稽核項目，擬訂稽核計畫經管理審查會議通過後實施。

(二)計畫內容包括：計畫目的、稽核日期與行程、稽核範圍、稽核對象、稽核項目、稽核作業方式、評核原則與報告撰寫及處理等。

(三)依據稽核結果就優缺點及改進措施提出書面報告，陳報資安長，並協調缺失單位確實檢討改進，必要時得實施複查。

(四)前款報告內容包括：稽核時間、受稽核單位、稽核結果處理及建議事項等。

第七章、附則

第三十八條、本辦法經數位安全與治理委員會及行政會議通過，陳請校長核定後實施，修正時亦同。