



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	1/20

管理系統文件

文件類別	第一階文件
文件編號	IMS-1-001
文件名稱	資通安全與個人資料保護政策
發行單位	圖書資訊處
發行日期	113年2月7日
版次	1.2



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	3/20

1. 目的

1.1 作為本校資訊安全管理制度 (Information Security Management System, 以下簡稱 ISMS) 與個人資料管理制度 (Personal Information Management System, 以下簡稱 PIMS) 相關管理辦法作業程序之參考依據。同時沿用國際標準組織 (ISO) 所訂定之持續改善 P.D.C.A. 循環流程管理模式，整合及強化資通安全管理體系及確保個人資料之保護及管理，建立制度化、文件化及系統化之管理機制，持續改進、監督及審查管理績效，以落實資通安全管理及個人資料保護之理念，並達到以下之目標：

1.1.1 建立、落實及維護資通安全暨個人資料保護政策。

1.1.2 全面導入 ISMS 與 PIMS。

1.1.3 培訓資訊人員在資訊及通訊領域之安全專業能力。

1.1.4 強化資通安全環境及資通安全應變能力。

1.1.5 達成資通安全與個人資料保護政策之量測指標。

1.2 確保本校資訊資產之機密性、完整性及可用性，並符合相關法令之要求，使其免於遭受內、外部的蓄意或意外之威脅，以保障本校利害關係人之權益。

2. 適用範圍

2.1 本校 ISMS 與 PIMS 所涵蓋範圍內皆適用之。

3. 資通安全管理及個人資料保護政策要求

為貫徹執行本校 ISMS 與 PIMS，確保其運作有效性並持續監督管理，以維護重要資通系統之機密性、完整性與可用性，特訂定資通安全與個人資料保護政策 (以下簡稱本政策)。本政策旨在提供校內人員資通作業之明確指導原則，所有校內人員皆有義務積極參與推動，以確保本校之資料、資通系統、設備、網路安全維運及個人資料保護，達持續營運的目標。

3.1 落實資通安全，強化服務品質

全體校內人員應落實執行 ISMS 之所有資通作業相關措施，確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	4/20

當的管理，而遭受洩密、破壞或遺失等風險，應選擇適切的保護措施，將風險降至可接受程度並持續進行監控、審查及稽核，以強化服務品質，提升服務水準。

3.2 加強資安訓練，確保持續營運

因應資通安全威脅情勢變化，每年持續進行適當的資通安全及個人資料保護教育訓練，以提高校內人員之資通安全意識，校內人員亦應確實參與訓練，建立校內人員「資通安全，人人有責」的觀念，促使校內人員了解資通安全及個人資料保護重要性，遵守資通安全及個人資料保護規定，提高資通安全緊急應變能力，降低資通安全風險，達持續營運之目標。

3.3 做好緊急應變，迅速災害復原

應訂定重要資訊資產及關鍵性業務之緊急應變計畫及災害復原計畫，並定期執行各項緊急應變流程的演練，以確保資通系統失效或重大災害事件發生時，能迅速復原，確保關鍵性業務持續運作，並將損失降至最低。

3.4 基於施行單位合法目的下，進行必要之個人資料處理。

3.5 僅針對特定目的蒐集最少的個人資料，且不處理過多的個人資料。

3.6 明確提供自然人其個人資料使用方式與對象的資訊。

3.7 確保處理直接由未成年人蒐集的資訊受到特別保護。

3.8 僅處理相關且適當的個人資料。

3.9 公平與合法地處理個人資料。

3.10 維護施行單位處理的個人資料分類清冊。

3.11 保持個人資料的正確性，並依需要保持最新。

3.12 僅依法律法規或施行單位合法目的的要求下，保存個人資料。

3.13 尊重自然人之個人資料行使權利，包含資料調閱權。

3.14 確保所有個人資料的安全。

3.15 僅在被適當保護之下，才能將個人資料傳輸至國境之外。



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	5/20

3.16 如對歐盟其他國家的自然人提供貨物和/或服務，應在適當時，提出處理應對歐盟監管機構的策略。

3.17 個人資料保護法律所允許之例外情形的應用。

3.18 發展與實施 PIMS，使政策得以實施。

3.19 適當時，識別內部與外部利害相關團體，以及其對施行單位 PIMS 治理參與的程度。

3.20 明確界定工作人員在 PIMS 中之責任與歸責性。

3.21 維護個人資料處理紀錄。

4. 資通安全及個人資料保護目標

本校執行 ISMS 及 PIMS 需達成之資通安全及個人資料保護目標，應依據「IMS-2-004 資通安全及個人資料保護目標管理程序書」之相關規定辦理。

5. 資通安全責任

5.1 本校管理階層負責審查資通安全與個人資料保護政策。

5.2 資訊安全管理執行小組及個人資料保護管理執行小組應透過適當的標準和程序推動資通安全與個人資料保護政策。

5.3 所有人員與廠商皆應遵守相關安全管理程序以維護資通安全與個人資料保護政策。

5.4 所有人員與廠商均有責任通報資通安全事件。

5.5 任何蓄意違反資通安全的行為將受到相關懲處或法律行動。

5.6 資通安全長(個資管理長)應瞭解近期教育體系重大資通安全政策，如「私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法」、全國大專校院資安長會議相關指示等，並督導協助相關事宜。

6. 資訊安全管理制度(ISMS)

6.1 一般要求



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	6/20

本校因應 ISO/IEC 27001 資訊安全管理系統之要求，特制定本政策作為整體 ISMS 之建置開發、實施操作、監控審查及持續改善之規定，並依據本校業務活動與風險，以建立資通安全政策及管理目標。

6.2 組織全景之鑑別

6.2.1 本校應決定與營運目的相關，且會影響 ISMS 預期成果之內部與外部議題，鑑別出相關之利害關係者，以及這些利害關係者對本校的需求與期望，並於資通安全委員會知悉以取得共識，用以客觀決定本校 ISMS 之範圍。

6.3 ISMS 之建置開發

6.3.1 建立 ISMS

6.3.1.1 過程簡要說明

本校係依照 ISO/IEC 27001 標準之步驟建立 ISMS，其過程簡要說明如下：

- 6.3.1.1.1 依據標準建議與主管機關之要求，成立本校「資通安全委員會」，並經核准公告。
- 6.3.1.1.2 本校資訊安全管理制度(ISMS)全部核心資通系統已完成 ISMS 導入，並逐步完成全機關實施範圍。
- 6.3.1.1.3 頒布「資通安全與個人資料保護政策」，以說明本校資通安全與個人資料保護政策、管理目標與執行方式。
- 6.3.1.1.4 進行風險評估作業，發掘資產與組織之安全弱點及其威脅與影響，並評估其風險等級，彙整成「風險評鑑報告」後，執行及追蹤「風險處理計畫」。
- 6.3.1.1.5 依據「資通安全與個人資料保護政策」與風險評估的結果，設定風險管理之實施範圍。
- 6.3.1.1.6 選擇適合實施之資通安全管制目標與措施，並檢討確認其可行性與有效性。
- 6.3.1.1.7 將所選定之安全管制目標、管制措施、選用原因等資料記載於「適用性聲明 (Statement of applicability)」文件



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	7/20

中。

6.3.1.1.8 為貫徹資通安全並持續改善，本校將依實際需求適時檢討上述步驟，並做必要之變更修正。

6.3.1.2 本校所有校內人員與廠商派駐人員均須遵循本校「資通安全與個人資料保護政策」與資通安全目標，恪守 ISMS 各項作業流程、管理規定及相關法令之要求。故意或過失違反者，將視其違反情節及所造成之衝擊，依人事規章或委外契約予以懲處。

6.3.1.3 廠商在執行本校委外業務時若有複委託之需求，應評估複委託業務相關之資安風險，並要求廠商依法令及本校相關規定，對複委託廠商進行適當之監督與管理。

6.3.1.4 對內部及外部專案管理的過程中，應明定及陳述與專案相關之各項資通安全要求，並由風險評鑑之結果用以決定及實作資通安全控制措施，確保內部及外部專案資訊之機密性、完整性及可用性，降低機敏資訊（含個人資料）外洩及違反法令之風險。

6.3.2 ISMS 之實施操作

6.3.2.1 應視風險之程度制定風險處理計畫，有系統地鑑別及陳述適當的管理措施、權責及優先順序，以便管理資通安全風險。

6.3.2.2 實施風險處理計畫中所選定之控制措施，以對各項風險加以防禦與控制，包含實施既定管理計畫，以達到所設定之資通安全目標。

6.3.2.3 應擬定安全控制措施有效性之量測指標與使用方法，以判斷所選控制措施以達資安目標所要求之程度。

6.3.2.4 人員所需實施訓練與認知計畫參閱第 8.2.2 節。

6.3.2.5 各項作業需遵照作業規定與程序執行，並不定期檢視與管理各項作業執行之狀況。

6.3.2.6 須定時衡量各項計畫目標執行狀況，並依據衡量結果適時調整相關控制措施與目標。



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	8/20

6.3.2.7 執行時所需之各項資源管理參閱第 8.2 節。

6.3.2.8 單位主管利用不定期巡視、內外部稽核或是單位人員所提出之建議事項回報，加速偵知各種安全事件並予以回應處理。

6.3.3 ISMS 之監控審查

6.3.3.1 本校採用下列監控方式確保 ISMS 所涵蓋範圍皆能安全無虞：

6.3.3.1.1 人員應定期及不定期巡視檢查各項設備及環境是否皆屬正常狀態。

6.3.3.1.2 利用攝影機監視管制區域人員出入狀況並錄影存證。

6.3.3.1.3 應設定、定期檢查及記錄各項監控指標，以協助判斷安全事件，預防及立即處理安全事故之發生。

6.3.3.1.4 單位主管應隨時注意各項通報事件或校內人員執行狀況，進而決定相應的控制措施，必要時可將人員職務進行短期調動，避免發生系統失效或人為破壞事件。

6.3.3.1.5 配合定期執行之內部稽核，確認各種安全措施及控制程序是否如預期般實施。

6.3.3.1.6 隨時注意本校所發生之資安事件，針對事件發生之成因及後果詳加評估，並配合矯正預防措施之執行，改善整體資安環境，降低資安事件發生之機率。

6.3.3.1.7 管理階層利用定期執行之「資通安全委員會」內部會議，討論目前可能存在的安全漏洞，並決定解決之道。

6.3.3.2 於「資通安全委員會」中定期審查 ISMS 之有效性，並考慮安全稽核、事件、有效性量測及利害關係團體之建議及反映意見。

6.3.3.3 於「資通安全委員會」中審查資通安全風險、殘餘風險與可接受風險等級，並考慮組織、技術、單位營運目標及程序、已鑑別之威脅與外部事件（包括法令、契約及社會環境）之變化。



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	9/20

6.3.3.4 每年至少召開一次資通安全管理審查會議，執行正式的 ISMS 審查，以確保範圍適當及 ISMS 過程之各項改善措施均已鑑別與實施。

6.3.3.5 應依據監控審查結果，適時修訂「資通安全維護計畫」，以符合資安政策、資安目標與各項資通安全要求。

6.3.3.6 所有對 ISMS 有效性或績效有衝擊之活動與事件均須加以記錄。

6.3.4 ISMS 之變更管理

6.3.4.1 確定需要對資訊安全管理體系進行變更時，應以預先規劃的方式進行變更。當有變更需求時應依各流程、系統及相關程序書要求提出相應之變更申請，如：文件變更、人員變更、權限變更、系統變更、組態變更...等。

6.3.4.2 評估變更。

6.3.4.3 審查變更要求。

6.3.4.4 協調變更執行。

6.3.4.5 檢視變更結果。

6.3.4.6 必要時修正程序書、系統文件、操作手冊...等。

6.3.4.7 結束變更程序。

6.3.5 ISMS 之持續改善

本校將定期進行下述工作：

6.3.5.1 利用風險評鑑及內外部稽核之結果進行整體資通安全環境之改善。

6.3.5.2 採取適當矯正及預防措施，採用從其他單位或內部發生事件之安全經驗汲取教訓。

6.3.5.3 與相關機構就結果及各項措施進行溝通並徵詢意見。

6.3.5.4 必要時修改 ISMS。



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	10/20

6.3.5.5 確保各項修改措施達到預期目標。

6.4 文件化要求

6.4.1 一般要求

本校 ISMS 文件包括下列各項：

- 6.4.1.1 「資通安全與個人資料保護政策」與安全管理目標之書面聲明。
- 6.4.1.2 ISMS 適用範圍及各項作業程序。
- 6.4.1.3 風險評鑑報告。
- 6.4.1.4 風險處理計畫。
- 6.4.1.5 組織為確保有效規劃、操作及控制資通安全過程所需之文件。
- 6.4.1.6 ISO/IEC 27001 標準要求及主管機關要求之紀錄。
- 6.4.1.7 「適用性聲明書」。

6.4.2 文件管制

ISMS 所需之文件應受保護及管制。紀錄是文件之一種特殊型態，應依第 6.4.3 節所定的要求予以管制，並建立文件化程序，以界定所需之管制，用以：

- 6.4.2.1 在文件發行前核准其適切性。
- 6.4.2.2 必要時，審查與更新並重新核准文件。
- 6.4.2.3 確保文件之變更與最新改訂狀況已予鑑別。
- 6.4.2.4 確保在使用場所備妥適用文件之相關版本。
- 6.4.2.5 確保文件易於閱讀並容易識別。
- 6.4.2.6 確保文件於需使用時能隨時取用，並且於文件傳遞、保存及毀棄時皆能遵守文件管制規定辦理。
- 6.4.2.7 確保外來原始文件已加以鑑別。



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	11/20

6.4.2.8 確保文件分發有適當管制。

6.4.2.9 防止作廢（失效）文件被誤用，作廢文件為任何目的需保留時，應予以適當鑑別。

6.4.3 紀錄管制

6.4.3.1 為確保 ISMS 符合本校要求及提供有效運作之證據，應建立及維持執行 ISMS 各項作業程序之各項紀錄，並予以管制，並將相關法令及契約要求列入考量。

6.4.3.2 紀錄應清晰易讀，容易識別及檢索。紀錄之鑑別、儲存、保護、檢索、保存期限及作廢，應建立文件化程序，以界定所需之管制。

6.4.3.3 紀錄應妥善保存。

6.4.3.4 所需之紀錄及其範圍應由管理過程加以決定。該過程應記錄重大決定，並將紀錄之用途及缺少紀錄時相關之風險列入考量。

7. 個人資料管理制度(PIMS)

7.1 本校只基於法令要求及合法之目的，且在確實必要範圍內使用個人資料。

7.1.1 本校因營運所需取得或蒐集之包括但不限於個人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動..等個人資料，應遵循「個人資料保護法」等法令。

7.1.2 不過度且符合目的、相關且適當並公平與合法地從事個人資料之蒐集與處理。

7.1.3 在公務活動的過程中僅於特定目的及個人資料類別內取得個人資料，並且只進行合於組織目的之蒐集、處理及利用。

7.1.4 本校之廠商與本校業務合作時，均應簽訂保密契約，使其充分瞭解個人資料保護之重要性及洩露個資之法律責任。倘有違反保密



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	12/20

義務之情事者，將依法追究其民事及刑事責任。

7.1.5 本校因業務上所擁有之個人資料負有保密義務，除當事人之要求查閱或有下列情形外，應符合「個人資料保護法」第二十條及相關法令規定，並以內部作業流程查詢外，本校不得對第三人提供當事人個人資料：

7.1.5.1 司法機關、監察機關、檢察機關、調查機關或警政機關因偵查犯罪或調查證據所需者。

7.1.5.2 其他政府機關因執行公權力並有正當理由所需者。

7.1.5.3 與公眾生命安全有關之機關（構）為緊急救助所需者。

7.2 本校僅使用目的所需之最低限度的個人資料

7.2.1 僅蒐集最少量的個人資料，不處理過多的個人資料，且僅依原始蒐集之特定目的使用個人資料。

7.3 將如何使用個人資料及處理者資料，清楚提供給當事人（包含孩童）。

7.3.1 對於個人資料之保護，將明確告知並設置諮詢管道，提供當事人有關個人資料將如何被使用及被誰利用的清楚資訊。

7.3.2 為保持個人資料正確性，依作業性質及個人資料主體之請求，予以保持最新，確保當事人權利。

7.4 公平且合法的使用處理個人資料。

7.4.1 本著合法、公平、公正、公開的合理處置原則，進行蒐集、處理及利用必要之個人資料，且建立相關管理制度合理地處理所取得之個人資料。

7.5 維持正確的個人資料，在必要時保持更新。

7.6 對於所取得之個人資料，應建立個人資料檔案清冊並適當維護相關內容。

7.7 只有在基於法令的要求或合法的組織目的時留存個人資料，且確保即時與適當的處置。

7.7.1 個人資料保存期限，僅在合乎法律或組織規定、利用目的內進行。



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	13/20

7.8 尊重自然人對其個人資料的權利。

7.8.1 當本校應依「個人資料保護法」、「教育體系資通安全暨個人資料管理規範」、ISO/IEC 27701 國際標準及本校所訂之程序，於合法、標準規定範圍內接受當事人行使請求查詢、閱覽、複製、補充、更正、傳輸電子檔、刪除、停止蒐集、處理、利用、反對特定用途、可攜帶至其他組織、限制處理及利用（發生爭議、不合法待釐清前暫時停止處理及利用）權利，並依「個人資料保護法」規定時限內完成辦理。

7.8.2 尊重當事人權利，建立相關處理流程。

7.9 保障所有個人資料的安全。

7.9.1 確保所有個人資料安全，建立相關安全控管措施。

7.9.2 個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規定。

7.9.3 為確保所有個人資料安全，應強化個人資料檔案資訊系統之存取安全，防止非法授權存取，維護個人資料之隱私性，應建立安全保護機制，並定期查核。

7.9.4 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身分之登入通行碼，並視業務及重要性，考量其他輔助安全措施。

7.9.5 個人資料輸入、輸出、存取、更新、銷毀或分享等處理行為，應釐定使用範圍及調閱或存取權限。

7.9.6 本校各單位如遇有個人資料檔案發生遭人惡意破壞、毀損或作業不慎等安全事件，應進行緊急因應措施，並依本校緊急應變通報程序辦理。

7.9.7 本校係以嚴密之措施、政策保護當事人之個人資料，包括本校之所有人員，均受有完整之「個人資料保護法」及隱私權保護之教育訓練。倘有不當揭露個資之情事者，將依法追究其民事、刑事及行政責任。

7.10 本校於利用個人資料時，除需依「個人資料保護法」之特定目的必要



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	14/20

範圍內為之外，如需為特定目的以外之利用時，將依據「個人資料保護法」二十條之規定辦理；倘有需取得當事人同意之必要者，本校應依法取得當事人之同意。

7.11 本校所蒐集、處理之個人資料，應遵循「個人資料保護法」及本校 PIMS 之規定，且個人資料之使用為本校營運或業務所需，方可為本校承辦校內人員利用。

7.12 本校取得之個人資料，如有進行國際傳輸之必要者，謹遵「個人資料保護法」及相關規定且不違反國家重大利益、不以迂迴方法向第三國傳遞或利用個人資料規避「個人資料保護法」之規定等原則辦理。如為因應國際條約或協定有特別規定或資料接受國對於個人資料之保護未有完善之法令致有損害當事人權益之虞，本校將於符合相關法令限制之情況下進行國際傳輸，以維護個人資料之安全。

7.13 本校校內人員若為海外其他國家人民時，適用「個人資料保護法」之規定。

7.14 「個人資料保護法」所允許的各種例外狀況之適用。

7.14.1 依據「個人資料保護法」第六條之規定，有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

7.14.1.1 法律明文規定。

7.14.1.2 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

7.14.1.3 當事人自行公開或其他已合法公開之個人資料。

7.14.1.4 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

7.14.1.5 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

7.14.1.6 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	15/20

同意違反其意願者，不在此限。

7.14.2 依據「個人資料保護法」第二十條之規定，本校對個人資料之利用，除「個人資料保護法」第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

7.14.2.1 法律明文規定。

7.14.2.2 為增進公共利益所必要。

7.14.2.3 為免除當事人之生命、身體、自由或財產上之危險。

7.14.2.4 為防止他人權益之重大危害。

7.14.2.5 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

7.14.2.6 經當事人同意。

7.14.2.7 有利於當事人權益。

7.15 發展並實施 PIMS 以落實資通安全與個人資料保護政策。

7.15.1 本校應建立與實施 PIMS，以落實本政策；全體校內人員及廠商應遵循 PIMS 之規定，並定期審查 PIMS 之有效性。

7.15.2 持續發展及實施個人資料保護管理工作，以確保政策得以落實。

7.16 識別內部及外部的利害關係者，並確認該關係者所涉及組織 PIMS 治理程度。

7.16.1 適當鑑別並諮詢利害關係人，以增加利害關係人的參與程度。

7.16.2 利害關係人之參與及期許。

7.16.3 為確保本校矯正預防措施之有效運作，應落實管理審查機制，本校每年至少召開一次管理審查會議。

7.17 識別對 PIMS 有特定職責且承擔責任之人員。

7.17.1 為有效執行個人資料保護與管理各項工作，已成立「個人資料保



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	16/20

護管理執行小組」，確保本校內所有人員之個人資料管理與保護之責任與義務，防止個人資料被竊取、竄改、毀損、滅失或洩漏，並遵循法令及持續有效地落實個人資料保護最佳實務。

7.17.2 確認相關人員在 PIMS 內之職責及責任。

7.18 維持個人資料處理使用之紀錄。

8. 管理階層責任

8.1 管理階層承諾

為使 ISMS 與 PIMS 推動順利，管理階層應確實執行下列事項：

8.1.1 審核資通安全與個人資料保護政策、資通安全目標及計畫。

8.1.2 成立「資通安全委員會」，以明定及文件化資通安全之角色與責任。

8.1.3 定期召開 ISMS 與 PIMS 之管理階層審查會議。

8.1.4 決定風險評鑑後之可接受風險等級。

8.1.5 提供充分資源，確保能建立、實施操作、監控審查及持續改善 ISMS 與 PIMS。

8.1.6 各單位主管應向所有人員宣達符合資通安全目標及法令要求之重要性，以及持續改善之需求。

8.2 資源管理

8.2.1 資源提供

為確保 ISMS 與 PIMS 執行無礙，應決定並提供下列工作之必要資源：

8.2.1.1 提供建置與維護 ISMS 與 PIMS 時所需的人力與資源設備。

8.2.1.2 提供實施 ISMS 與 PIMS 時必要之協助。

8.2.1.3 確定各項安全程序可配合營運需求。

8.2.1.4 當需要時，進行審查並針對審查結果作適當因應。



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	17/20

8.2.2 訓練、認知及能力

為確保所有校內人員皆有能力執行所要求之工作與符合各項安全要求，應藉由各種途徑取得協助校內人員執行教育訓練，包括下列方式：

8.2.2.1 提供各種能力訓練以滿足該需求。

8.2.2.2 藉由意見（滿意度）調查、測驗、繳交心得報告及證書取得等方式，評估所提供訓練之有效性。

8.2.2.3 確保校內人員認知其所從事的活動之相關性及重要性，以及如何對資通安全目標之達成有所貢獻。

8.2.2.4 應留下教育訓練、技能、經驗及評定資格等紀錄。

9. 內部稽核

每年定期執行內部稽核，確保 ISMS 與 PIMS 的各項管制目標、控制措施、運作過程以及各項程序是否皆：

9.1 符合 ISO/IEC 27001、ISO/IEC 27701 及「教育體系資通安全暨個人資料管理規範」相關法令之要求。

9.2 符合本校所制定之資通安全及個人資料保護目標與其他相關要求。

9.3 有效地實施與維持 ISMS 與 PIMS。

9.4 符合主管機關的期待。

10. ISMS 與 PIMS 之管理階層審查

10.1 概述

本校「資通安全委員會」至少每年召開一次會議，針對本校現行之 ISMS 與 PIMS 進行審查，以確保相關程序的適用性、適切性及有效性皆符合本校需求，並評估相關政策與目標的改善時機，或是其他的變更需求，且審查結果應留下相關文件與紀錄備查。

10.2 審查輸入（管理審查之範圍）

管理階層審查至少應包含下列項目：

10.2.1 先前管理審查決議事項之跟催狀況。



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	18/20

10.2.2 有關可能影響 ISMS 與 PIMS 的外部與內部問題之變更。

10.2.3 與 ISMS 與 PIMS 有關的利害關係方的需求和期望的變化。

10.2.4 資通安全的及個人資料保護績效回饋，包含下列趨向：

10.2.4.1 不符合事項與矯正措施之執行狀況。

10.2.4.2 監督與量測結果。

10.2.4.3 內部稽核的結果。

10.2.4.4 資通安全及個人資料保護目標的實現。

10.2.5 資通安全維護計畫實施情形

10.2.6 個人資料檔案維護計畫實施情形

10.2.7 利害相關團體的回饋(包含客訴之處理與執行進度追蹤)。

10.2.8 風險評鑑的結果與風險處理計畫的狀態。

10.2.9 審查本政策之適切性。

10.2.10 資通安全與個人資料保護目標之適切性。

10.2.11 持續改善的機會。

10.3 審查輸出

10.3.1 管理審查的產出應包含持續改善機會與 ISMS 與 PIMS 的變更需求有關之決定。

10.3.2 管理階層審查之產出建議包含但不限於下列事項之任何決策與措施：

10.3.2.1 ISMS 與 PIMS 有效性之改善。

10.3.2.2 風險評鑑與風險處理計畫之更新。

10.3.2.3 影響資通安全之程序與控制之必要時的修改，以回應可能衝擊 ISMS 與 PIMS 之內部或外部事件，包括下列事項之變更：

10.3.2.3.1 各項營運要求。



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	19/20

- 10.3.2.3.2 各項安全要求。
- 10.3.2.3.3 影響既有各項營運要求之營運過程。
- 10.3.2.3.4 法律或法規各項要求。
- 10.3.2.3.5 契約的各項義務。
- 10.3.2.3.6 風險等級及/或風險接受準則。

10.3.2.4 資源需求。

10.3.2.5 控制措施的有效性如何量測之改善。

10.3.3 組織應保存文件化資訊及管理審查結果的證據。

11. ISMS 與 PIMS 之改善

11.1 矯正措施

本校採取適當控管措施，以減低 ISMS 與 PIMS 在建置、操作及使用時所產生的不符合事項，以防止再度發生。矯正措施之內容應包含下列各項：

- 11.1.1 鑑別各項不符合資安要求之事項。
- 11.1.2 判定各項不符合事項發生之原因。
- 11.1.3 評估各項矯正措施之需求，以確保各項不符合事項不復發。
- 11.1.4 決定及實施所需之矯正措施。
- 11.1.5 需記錄所採矯正措施之結果，紀錄保存之要求參閱第 6.4.3 節。
- 11.1.6 審查所採取之矯正措施。

11.2 預防措施

本校應採取適當的控管措施，以預防及降低潛在不符合事項發生之機會，預防措施應能預防潛在問題所可能發生之影響。

- 11.2.1 鑑別潛在的各項不符合事項及其原因。
- 11.2.2 評估預防措施的需求，以防止不符合事項的發生。



文件編號	IMS-1-001	文件名稱	資通安全與個人資料保護政策		
機密等級	一般	版次	1.2	頁次	20/20

11.2.3 決定及實施所需之預防措施。

11.2.4 記錄所採取措施之結果，紀錄保存之要求參閱第 6.4.3 節。

11.2.5 審查所採取之預防措施。

11.3 持續改善

本校經由資通安全與個人資料保護政策、安全目標、內外部資通安全稽核結果、事件監控之分析、矯正與預防措施以及管理階層審查，由單位主管負責所有風險發生或不符合事項之監控，並追蹤相關業務承辦人之改善情形，以持續改善 ISMS 與 PIMS 之有效性。

12. 審查

12.1 本政策每年應至少評估檢討一次，以反映本校資通安全及個人資料保護需求、政府法令、外在網路環境變化及資通安全技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力及個人資料管理實務作業之時效性。

12.2 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知相關單位及廠商，以利共同遵守。

13. 發布實施

本政策經資通安全委員會議通過，陳請資通安全長(個資管理長)核定後，自公布日起實施，修正時亦同。