教育體系
資通安全暨個人資料
管理規範

中 華 民 國 105 年　　月　　日

本規範歷次變更紀錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目　　錄

壹、　緣起 4
貳、　簡介 4
參、　適用範圍 5
肆、　目標期程 6
伍、　引用標準 6
陸、　適用性聲明（Statement of Applicability） 7
柒、　建置步驟及需求 7

壹、緣起

資通訊科技的快速發展，對於作業效率之提供有所助益，惟其亦帶來了資通安全之挑戰。為能夠有效因應資通訊科技應用所帶來的資通安全挑戰，教育部(以下稱本部)於民國(以下同)96 年 5 月 30 日發布「教育體系資通安全管理規範」，供教育體系機關(構)與各級學校據以建立其資通安全管理系統，綜合考量其重要性、急迫性以及可分配資源等因素，建立其資通安全管理規範的設計與施測，透過持續改善的管理機制運行，大幅強化其資通安全的有效性。

「教育體系資通安全管理規範」自施行迄今已逾九年，其間經歷資通訊環境之變遷，諸如：網路之普及、資通訊科技之進步與廣泛應用、資通訊安全最佳實務標準於 102 年改版、以及組織架構與運作模式轉變等，有必要重新檢視與調整。復以我國於 99 年將電腦個人資料保護法修改為個人資料保護法，擴大保護標的，不限於經電腦處理之個人資料，且以任何形式存在之個人資料皆有該法之適用。其次則是擴大適用範圍，舉凡涉及個人資料蒐集、處理、利用之個人、法人或團體皆為該法之適用，且各行各業皆應適用該法。第三，新增個人資料蒐集、處理與利用之行為規範，諸如：告知義務之履行，並提高損害賠償之額度且導入團體訴訟之機制。此外，我國於 104 年針對 99 年修正之個人資料保護法，因應實務運作之需求，完成第二次修法，包括：將病歷納入特種個人資料之範圍，新增當事人書面同意為特種個人資料之蒐集、處理與利用依據等。前揭法令之更迭對於教育體系造成相當程度之影響，且教育體系發生個人資料遭不當揭露或利用之情況亦曾見聞。是以，於維護資通安全之際，尤有必要考量個人資料安全之維護。

爰此，為因應資通訊環境之變化，並考量我國個人資料保護法之修正與施行，以及最佳國際實務標準之發展與普及，如 ISO 27001:2013、ISO 27002:2013、ISO 29100:2011、BS 10012:2009 等，自 104 年起著手「教育體系資通安全管理規範」之研修，歷經數次之專家討論與教育體系意見諮詢，終而於 105 年完成之修訂，提出新版之「教育體系資通安全暨個人資料管理規範」。(以下稱本規範)

貳、簡介

本規範因應個人資料保護法之修正與施行，新增個人資料管理系統（Personal Information Management System，以下稱 PIMS）之相關要求，期以 PDCA (Plan-Do-Check-Act，規劃-實行-確認-行動)策略，協助教育體系機關(構)與各級學校完善其個人資料安全維護之工作，達到個人資料保護之目的，降低個人資料遭不當揭露或利用之風險。同時，本規範因應最佳實務標準 102 年之改版，新增資訊安全管理系統（Information Security Management System，以下稱 ISMS）之相關控制措施建議，期能夠協助教育體系機關(構)與各級學校有因應資通訊科技應用所衍生之新興資通安全議題。此外，為達資源有效運用之目的，本規範特別針對結合 ISMS 與 PIMS 之「資通安全暨個人資料管理系統」進行說明，期能夠協助教育體系機關(構)與各級學校評估其組織規模、管理需求、目標、結果等因素，建置能夠同時符合資通安全維護與個人資料保護目標

之管理系統。

本規範期望對教育體系機關(構)與各級學校之資通安全或個人資料管理產生引導作用，協助其有效率地建置與運行資通安全與個人資料管理系統，發揮「事前預防・事後抑制」之效果，有效落實個人資料保護法令之施行，並達維護資通安全之目的。是以，教育體系機關(構)與各級學校於參照本規範建立管理系統時，得衡酌組織規模、業務特性、所欲達成之資通安全維護或個人資料保護目的等因素，選擇適當之實施範圍，配置適當之資源與人員，規劃適宜之管理系統，持續有效地運行該系統，並定期檢視與改善該系統。然而，值得注意是個人資料保護法令之遵循係屬全組織應遵循之事宜，且資通安全之風險非僅肇因於系統風險，故教育體系機關(構)與各級學校宜逐步擴大實施範圍，以達維護資通安全與個人資料保護之目的。

除本規範另有規定，選擇單獨建置 ISMS 之單位，無須執行關於 PIMS 之要求，反之亦然；選擇建立「資通安全暨個人資料管理系統」，應同時符合二項管理系統之要求。意即，教育體系機關(構)與各級學校得就 ISMS 或 PIMS 擇一驗證，亦可就 ISMS 與 PIMS 同時驗證。然而，本規範之驗證作業目的係為協助導入機關(構)與學校確認其所建置資通安全或個人資料管理系統之有效性，如有發生個人資料保護之爭議，仍應依個案為具體判斷，非謂經驗證通過即可謂無法律責任。

參、適用範圍

本規範適用於教育體系機關(構)與各級學校，其得參照本規範所訂之管理要求與執行方法，針對資通安全與(或)個人資料安全之維護建立管理系統，就組織規模、業務特性等選擇適當之實施範圍，配置適當之資源與人員，規劃適宜之管理系統，持續有效地運行該系統，並定期檢視與改善該系統。

有鑑於教育體系機關(構)與各級學校之層級、組織規模、業務特性差異極大，為避免其因組織特性無法執行部分要求，本規範爰參考行政院國家資通安全會報訂定之「政府機關（構）資通安全責任等級分級作業規定」與教育部頒定之「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」，將適用機關(構)及學校分為 A、B、C 三級(各級涵蓋之對象請參閱教育部與所屬機關(構)及學校資通安全責任等級分級作業規定)，並依等級建議不同之適用範圍，如下：

一、 A 級：

ISMS：應至少包含組織內所有資訊管理作業與流程，全部核心業務應用資訊系統與網路系統，以及受委託執行國家安全與機密資訊或技術研究單位，或試務管理單位。

PIMS：應包含組織內全部所有涉及個人資料蒐集、處理與利用之流程。

二、 B 級：

ISMS：應至少包含資訊管理單位、學術網路系統、核心業務資訊系統。

PIMS：應至少包含涉及核心業務之個人資料蒐集、處理與利用流程之行政單位，以及資訊管理單位。

三、 C 級：

ISMS：應至少包含資訊管理單位及校務行政資訊系統。

PIMS：應至少包含組織內涉及個人資料處理蒐集、處理與利用流程之行政單位，以及資訊管理單位。

備註：欲建立「資通安全暨個人資料管理系統」之機關(構)與學校，得分別定義兩項管理系統之適用範圍，惟 PIMS 適用範圍所涉及之資通安全管理議題，應完整包含於 ISMS 之適用範圍內。

肆、目標期程

本規範之目標，係提供所有教育體系機關(構)與學校，考量自身資源及所對應之風險，並依其適用範圍建置適合與有效之資通安全或個人資料管理系統，進而建立整合的「資通安全暨個人資料管理系統」。

管理系統之建立、實作、維持及持續改善，需考量管理階層的支持、各單位的協調配合、人力、經費等各項資源因素，因此，建議各單位採階段式進行建置，自行設定合理的期程目標，逐步達成每年度預定的進程比例，藉由如此的模式，最終能建置合適、整合的「資通安全暨個人資料管理系統」。

伍、引用標準

本文架構主要採用 ISO 組織定義之 Annex SL 架構，條文內容則同時參考 ISO/IEC 27001:2013 及 BS 10012:2009 兩項管理標準，再依據教育體系機關(構)與學校的特性及需求，設計出較為合適的規範，希冀能有效提升各機關(構)與學校的資通安全及個人資料管理能力。參考文件如下：

個人資料保護法及個人資料保護法施行細則(法務部)

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實施辦法(教育部)

行政院及所屬各機關資訊安全管理規範(行政院)

政府機關（構）資通安全責任等級分級作業規定(行政院資通安全辦公室)

教育體系機關構及學校資通安全責任等級分級作業規定(教育部)

資訊系統分級與資安防護基準作業規定(行政院國家資通安全辦公室)

政府機關構資安事件數位證據保全標準作業程序(行政院國家資通安全辦公室)

教育體系個人資料安全保護基本措施(教育部)

103 年資安服務暨專案管理辦公室 安全控制措施參考指引（V2.0）

ISO/IEC 27001:2013 Information security management systems – Requirements。

ISO/IEC 27002:2013 Code of practice for information security controls。

BS 10012:2009 Data Protection Specification for a Personal Information Management System。

ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework。

ISO/IEC 29101:2013 Information technology - Security techniques - Privacy architecture framework。

ISO29191:2012 Information technology - Security techniques - Requirements for partially anonymous, partially unlinkable authentication

陸、適用性聲明（Statement of Applicability）

本規範適用於教育體系機關(構)與學校，其得考量各自分級屬性、類型、規模、資源、業務性質、以及組織內部有關 ISMS 與 PIMS 之施行狀況，選擇控制措施並產生相關之適用性聲明。

一、有關 ISMS 之建置與施行

擬建置 ISMS 之教育體系機關(構)與學校可依據前揭所提及之適用等級選擇控制措施，參考附錄 A 之控制措施，提出「ISMS 適用性聲明」。各等級機關(構)與學校適用之控制措施請參照「附錄 A 資訊安全管理規範 附件 1 各級教育機構適用控制項對照表」。附錄 A 控制措施之排除僅限適用範圍內資訊系統無需執行，且排除後不影響該機關(構)與學校提供資通安全能力與責任之控制措施。

教育機構如欲取得驗證，所有附錄 A 資訊安全管理規範內之控制項，除標註「建議」者外均應納入，同時應參考「資訊系統分級與資安防護基準作業規定」，鑑別適用範圍內資訊系統之安全等級，經資訊系統分級與鑑別後，識別出具有等級為「高」者之資訊系統，應加入 A.14 系統獲取、開發及維護與 A.15 供應者關係等控制領域所有控制措施，並於該控制措施中述明適用之資訊系統。

核心業務資訊系統：指經資訊系統分級後，等級為「高」者，資訊系統安全等級經鑑別為高者，則需進行風險評鑑以分析規劃實作控制措施之有效性。實際執行時，核心業務資訊系統或其他安全等級為高者，應依據適用安全等級高項目執行控制措施，其他中低安全等級系統，則僅依其等級選用控制措施即可。

二、有關 PIMS 之建置與施行

建立並運行 PIMS 之機關(構)與學校，應選用附錄 B 所有控制項。

三、有關資通安全暨個人資料管理系統之建置與施行

建立並運行整合的「資通安全暨個人資料管理系統」之機關(構)與學校，應同時遵循上述要求，並提出「資通安全暨個人資料管理系統適用性聲明」。

柒、建置步驟及需求

教育體系機關(構)與學校於建立、實作、維持及持續改善 ISMS、PIMS 或資通安全暨個人資料管理系統時，執行步驟及相關需求事項如下：

一、 組織全景

(一) 施行機關(構)或學校應依據相關法令要求、行政院及教育主管機關所下達之重要決定或指導(包括但不限於主管機關之行政指導、重要會議決議事項等)、組織透過相關會議所做成之決議(包括但不限於主管會報、行政會議或校務會議等

之決)，針對資通安全或個人資料安全之維護需求進行評估，並據此建立或調整資通安全與個人資料管理範圍與目標。

(二)　施行機關(構)或學校應依據決議事項確認其關注方(利害相關團體)與要求事項，並留存文件化紀錄。

(三)　上述事項之識別與分析應定期審查(每年至少一次)，或於施行機關(構)或學校遭遇重大變更、或有新增業務時重新檢視，並供管理審查時，評估管理系統及其適用範圍是否有調整之必要性。

二、 領導作為

(一)　領導及承諾

管理制度管理人或召集人應由施行機關(構)或學校之副首長以上擔任或指定，並藉由下列事項，展現對管理制度之領導與承諾：

1. 建立或核定機關(構)或學校之管理政策與目標。
2. 傳達管理制度要求事項之遵循與持續改善的承諾。
3. 提供管理制度運行所需資源及人力。

(二)　建立政策與目標

1. 管理人或召集人應確保建立文件化的管理政策，並於機關(構)或學校內進行公告或傳達，同時依需要提供予利害相關團體。
2. 管理政策應包含符合機關(構)或學校之管理目的與目標、滿足管理制度要求事項與、以及持續改善之承諾。
3. 施行機關(構)或學校應依規劃期間或重大變更時，於透過管理審查管理活動評估管理政策與目標，並配合變更需求修訂政策與目標。

(三)　指派角色、責任及權限

管理人或召集人應建立制度管理小組，依機關(構)或學校特性，指派人員並賦予其管理之責任與權限，以促進達成本規範之要求事項。受指派人員應定期(每年至少一次) 或於重大變更時向管理階層報告管理制度執行成效。ISMS 與 PIMS 所配置人員應依據附錄 A.6 資訊安全組織與附錄 B.2 個人資料管理組織派任。

三、 規劃

(一)　管理目標達成風險與機會之因應行動

為確保達成制度管理目標，並預防或減少非預期之影響，以達成持續改善，應依規劃期間或重大變更時，評估管理目標異動與達成情形，如有異動或未達成狀況，則應規劃因應風險與機會之行動，將各項行動整合及實作於管理制度中，並評估此行動之有效性。

PIMS 並應依附錄 B.4 個人資料之識別與風險管理要求執行。

(二)　建立風險管理程序

應參考「資訊系統分級與資安防護基準作業規定」，鑑別適用範圍內資訊系統之

安全等級。資訊系統經鑑別後，其安全等級屬最高等級者，應執行風險評估、擬訂與執行風險管理措施；其安全等級非屬最高等級者，應衡酌其風險程度，以決定是否進行風險評估、擬訂與執行風險管理措施。

風險評估與管理流程建立應符合下列要求事項：

1. 建立與維持風險準則
   包含風險評鑑執行時機與方法，以及風險接受準則，以確保重複之風險評鑑能產生一致、有效及可比較之結果。
2. 識別、分析並評估風險
   (1) 識別管理制度適用範圍內涉及資訊之機密性、完整性、可用性與適法性相關聯之風險與風險擁有者。
   (2) 所識別之風險可能導致之潛在後果與發生的實際可能性，並將所建立之風險準則與風險分析結果進行比較，訂定風險處理優先順序。
3. 選擇風險處理措施
   考量風險評鑑結果，選擇適切之風險處理選項，並依選項決定所有必須實作之控制措施。
4. 產生或評估適用性聲明書(資訊安全風險處理使用)
   執行資訊安全風險評鑑時，應依據資訊資產分級結果重現檢視比較現有控制措施及附錄 A，確認未忽略必要之控制措施，並產生或評估適用性聲明書，包括附錄 A 之控制措施，且不論是否實作，提供納入或排除之理由。
5. 制訂風險處理計畫並取得核准
   制訂風險處理計畫，並取得風險擁有者對風險處理計畫之核准，以及對剩餘風險之接受。

(三) 管理目標及其達成之規劃

施行機關(構)或學校應針對異動與未達成之管理目標，設定符合管理政策與策略之可量測指標，並保存管理目標之文件化資訊。

施行機關(構)或學校應對前述管理目標規劃因應行動，包含：

1. 相關執行活動或事項。
2. 所需配置之人員、預算、設備技術與程序表單等資源。
3. 活動或事項負責人員。
4. 活動或事項預計完成時間。
5. 管理目標是否達成之評估方式。

四、 支援

(一) 資源

施行機關(構)或學校應依據管理目標達成規劃，提供建立、實行、維持及持續改善管理制度所需資源。

（二） 能力

施行機關(構)或學校應採取下列措施：

1. 指派受過適當教育訓練、具備證照或具有經驗人員，執行資通安全或個人資料管理相關任務；規劃培訓以強化人員能力時，應評估培訓之有效性。
2. 有關人員能力訓練，ISMS 應參照附錄 A .7 人力資源安全，PIMS 則依附錄 B.3 人員認知與訓練要求執行。
3. 應保存文件化資訊(如：如證書、證照、培訓紀錄等)，作為人員勝任之證據。

（三） 認知

應規劃人員認知宣導或訓練，讓所有人員知悉：

1. 管理政策及目標。
2. 管理程序與流程，要求事項與人員責任。
3. 未遵循要求可能產生對個人與單位的影響與衝擊，包含但不限於獎懲措施。

ISMS 應參照附錄 A .7 人力資源安全，PIMS 則依附錄 B.3 人員認知與訓練要求執行。

（四） 文件化資訊

管理制度文件化資訊應滿足下列要求：

1. 管理制度文件應包括本規範要求之文件化資訊，及施行機關(構)或學校要求管理制度為達成其有效性之文件化資訊與作業紀錄。

   其文件化資訊至少應包含：

   (1) 決議事項確認其關注方(利害相關團體)與要求事項
   (2) 管理政策
   (3) 管理目標
   (4) 人員勝任之證據
   (5) 管理制度執行證據
   (6) 風險處理計畫與風險處理結果
   (7) 有效性評估證據
   (8) 管理審查執行之證據
   (9) 不符合項目及矯正措施
2. 制訂及更新應遵循既有文件管理程序，進行審查及核准。
3. 管控文件化資訊派送、存取、檢索、使用、儲放與維護、變更管制、留存及屆期處置，並適切保護。
4. 施行機關(構)或學校應識別對管理制度規劃及運作必要之外部文件。

五、 運作

（一） 運作之規劃及控制

施行機關(構)或學校之管理制度運作應滿足下列要求：

1. 應依據管理制度各階文件，以及為達成管理目標所規劃之流程、程序與控制措施執行，並應保存執行證據。
2. ISMS 應依據所屬級別實作選定之附錄 A 控制措施，PIMS 則應實作附錄 B 訂定之控制措施。
3. 應確保各項委外執行作業受到控制與管理，屬 ISMS 委外管理可連結附錄 A 之 A.15 供應者關係，PIMS 則依據附錄 B 之 B.12 委外管理執行。

（二） 執行風險評鑑

1. 施行機關(構)或學校依規劃期間(至少每年一次)、管理階層指示或發生重大變更後一個月內，應執行風險評鑑，確認管理制度各項風險加以識別，並保存風險評鑑執行紀錄。
2. PIMS 施行機關(構)或學校應分析可能造成當事人損失或困擾之個人資訊處理流程，由風險擁有者進行審查。
3. 擬定風險處理計畫，並取得風險擁有者對其及剩餘風險之核准。

（三） 實作風險處理

施行機關(構)或學校應實作風險處理計畫並保存風險處理結果之文件化證據資訊。

六、 績效評估

（一） 監督、量測、分析及評估

1. 施行機關(構)或學校應針對已施行之常態性作業流程或控制措施建立監督機制，如機房管理、網路管理作業審查等。
2. 對於該年度異動之管理目標，以及風險處理措施設定有效性量測指標，並界定明確計算方式與資料來源、量測人員、週期與時間點，以及分析及評估量測結果之人員、週期與時間點。
3. 應留存文件化資訊，作為有效性評估證據。

（二） 內部稽核

1. 施行機關(構)或學校應定期(至少每年一次)或於重大變更後執行一次內部稽核，以確認機關(構)或學校與人員是否遵循本規範與機關(構)或學校管理程序要求，並有效實作及維持管理制度。ISMS 施行機關(構)或學校可連結附錄 A.18 遵循性執行。
2. 稽核程序應包括頻率、方法、職責、規劃要求事項及報告。稽核計畫應包含適用範圍內核心業務與高風險個人資料流程或系統，並將前次稽核之結果納入考量。

3. 稽核員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性。
4. 稽核結果應對相關管理階層報告，留存相關紀錄以作為稽核計畫及稽核結果之證據。

(三) 管理審查

管理小組應定期(每年至少一次)進行管理審查，以審查管理制度執行狀況，並確保其持續的適切性、合宜性及有效性。

1. 管理審查應包含下列討論事項：
   (1) 過往管理審查之議案的處理狀態
   (2) 資通訊安全或個資管理要求的變更，如上級機關要求、最高行政管理會議決議事項
   (3) 管理目標與指標量測結果
   (4) 內外部稽核結果
   (5) 資安事故與不符合項目之矯正情形
   (6) 風險評鑑結果及風險處理計畫執行進度
   (7) 持續改善之機會
2. 管理審查決議事項應包含持續改善機會與管理制度變更需求之決議。
3. 施行機關(構)或學校應保存相關紀錄，以作為管理審查執行之證據。

七、 改善

(一) 不符合項目及矯正措施

不符合項目發生時，施行機關(構)或學校應進行下列作為，並保存紀錄：

1. 先對不符合項目採取行動以控制並矯正，進而處理其後果。
2. 判定其發生原因及矯正措施，並評估是否有其類似不符合項目存在，並據此提出並執行矯正措施，並必要時得考量對管理制度進行變更。

(二) 持續改善

施行機關(構)或學校應持續改善管理制度的合宜性、適切性及有效性。