# 附錄 C

# 個人資料保護規範對照表

## 一、 教育機構個人資料保護工作事項檢核對照表

| 查核項目 | 教育體系資通安全暨個人資料管理規範 | 附錄A 資訊安全管理規範 | 附錄B 個人資料管理規範 |
|---|---|---|---|
| **一、規劃** | | | |
| **1. 配置個人資料管理之人員及相當資源** | | | |
| 1.1 是否建立個人資料保護管理政策？ | 柒、二、(二)建立政策與目標 | | B.1.1.1 個人資料管理政策 |
| 1.2 是否成立個人資料保護管理小組，並由單位副首長擔任機關召集人？ | 柒、二、(一)領導及承諾 | | B.2.1.1管理階層角色及責任 |
| 1.3 是否指定專人依法令規定辦理個人資料安全維護及保管事項？ | 柒、二、(三)組織角色、責任與授權 | | B.2.1.2日常作業管理責任<br>B.2.1.3個人資料管理專人 |
| 1.4 是否決定並提供單位規劃與施行個人資料保護工作所需的資源，包含人力、物資或外部諮詢顧問等？ | 柒、四、(一)資源 | | |
| **2. 界定個人資料之範圍** | 柒、一、組織全貌 | | |
| 2.1 是否定期執行個人資料檔案鑑別作業？ | | A.8.1.1 資產清冊 | B.4.1.1個人資料清冊 |
| 2.2 是否建立與維護個人資料檔案清冊？ | | A.8.1.1 資產清冊 | B.4.1.1個人資料清冊 |
| 2.3 公務機關是否依個人資料保護法要求在網站上公開個人資料檔案相關資訊？ | | | B.5.2.1告知事項 |
| **3. 個人資料保護之風險評估及管理機制** | 柒、三、(二)<br>建立風險管理程序 | | |
| 3.1 是否訂定個人資料檔案衝擊影響程度評估準則？ | 1.建立與維持風險準則 | | B.4.1.2高風險個人資料<br>B.4.2.1 風險管理 |
| 3.2 是否進行個資資產之衝擊影響程度分析？ | 2.識別、分析並評估風險 | | B.4.2.1 風險管理 |
| 3.3 是否定期執行個人資料檔案之風險評鑑作業？ | 柒、五、(二) 執行風險評鑑 | | B.4.2.1 風險管理 |
| 3.4 是否針對這些風險訂定處理計畫？ | 柒、五、(三) 實作風險處理 | | B.4.2.1 風險管理 |
| **4. 事故之預防、通報及應變機制** | 柒、三、(一)風險與機會處理措施<br>(二) 建立風險管理程序 | | |
| 4.1 人員是否瞭解個人資料保護法之要求，克盡職責保護及管理相關業務所接觸之個人資料？ | | | B.3.1.2認知與教育訓練 |

| 查核項目 | 教育體系資通安全暨個人資料管理規範 | 附錄A 資訊安全管理規範 | 附錄B 個人資料管理規範 |
|---|---|---|---|
| 4.2 當發生個人資料資訊安全事件時，人員是否了解通報流程？ | | A.16.1.2通報資訊安全事件A.16.1.3通報資訊安全弱點 | B.10.2.1安全事故管理程序與紀錄 |
| 4.3 當發生個人資料資訊安全事件時，是否會通報主管機關？ | | A.16.1.2通報資訊安全事件 | B.10.2.1安全事故管理程序與紀錄 |
| 4.4 當發生個人資料資訊安全事件，導致個人資料被竊取、洩漏、竄改或造成其他侵害，是否建立查明事件及通知當事人之程序？ | | A.16.1.4資訊安全事件評估及決策<br>A.16.1.5對資訊安全事故之回應 | B.10.2.1安全事故管理程序與紀錄 |
| 4.5 是否訂定個人資料資訊安全事件處理程序？ | | A.16.1.5對資訊安全事故之回應 | B.10.2.1 安全事故管理程序與紀錄 |
| 4.6 是否設置「個資保護聯絡窗口」及重大個資外洩事件之民眾聯繫單一窗口？ | | | B.10.2.1 安全事故管理程序與紀錄 |
| 4.7 是否將「個資保護聯絡窗口」之聯繫方式（如：電話、email）置於單位網站，以便利民眾提出申訴與救濟。 | | | B.10.2.1 安全事故管理程序與紀錄 |
| **二、執行** | | | |
| **5. 個人資料蒐集、處理及利用之內部管理程序** | | | |
| 5.1 蒐集、處理或利用個人資料，是否符合不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯？ | | | B.5.1.1 蒐集與處理作業審查<br>B.6.1.1 特定目的處理準則<br>B.6.1.2 新特定目的同意 |
| 5.2 蒐集個人資料時，是否明確告知當事人相關資訊：<br>(a) 機關名稱<br>(b) 蒐集目的<br>(c) 個人資料的類別<br>(d) 個人資料利用期間、地區、對象及方式<br>(e) 當事人行使之權利事項及方式等<br>(f) 當事人不提供個人資料對其權益之影響 | | | B.5.2.1 告知事項<br>B.5.2.2 告知或同意作業程序 |
| 5.3 是否於法律允許之範圍內提供資料當事人下列權利：<br>(a) 查詢或請求閱覽<br>(b) 請求製給複製本<br>(c) 請求補充或更正<br>(d) 請求停止蒐集、處理或利用<br>(e) 請求刪除 | | | B.9.1.1 當事人權利行使程序<br>B.10.1.2 抱怨與申訴流程 |

| 查核項目 | 教育體系資通安全暨個人資料管理規範 | 附錄A 資訊安全管理規範 | 附錄B 個人資料管理規範 |
|---|---|---|---|
| 5.4 蒐集非由當事人提供之個人資料時，是否於處理或利用前，向當事人告知下列資訊：<br>(a) 個人資料來源<br>(b) 機關名稱<br>(c) 蒐集目的<br>(d) 個人資料的類別<br>(e) 個人資料利用期間、地區、對象及方式<br>(f) 當事人行使之權利事項及方式 | | | B.5.2.2 告知或同意作業程序 |
| 5.5 是否維護個人資料的正確性？ | | | B. 7.2.1 正確性管理<br>B. 7.2.3 新流程的審查 |
| 5.6 是否主動依當事人的請求更正或補充個人資料？ | | | B. 7.2.2 錯誤資料的更正 |
| 5.7 是否符合個資法第16條與第20條有關特定目的以外之利用規範？ | | | B.6.1.1 特定目的處理準則<br>B.6.1.2 新特定目的同意 |
| **6. 資料安全管理及人員管理** | | 4.13安全議題 | |
| **資料安全管理** | | A.8資產管理 | |
| 6.1 機關學校所管理之網站或網頁內容，於確有必要公布個人資料時，是否經所屬單位主管核准？ | | | B.6.1.1 特定目的處理準則<br>B.6.2.2 資料揭露程序 |
| 6.2 公布在網站上的個人資料是否依相關法律及規範處理？ | | | B.6.1.1 特定目的處理準則<br>B.6.2.2 資料揭露程序 |
| 6.3 對於個人資料之調閱是否經申請並核准？ | | | B.6.2.1 資料分享規劃與協議<br>B.6.2.2 資料揭露程序 |
| 6.4 是否加以記錄調閱個人資料者之身分及行為？ | | | B.6.2.1 資料分享規劃與協議<br>B.6.2.2 資料揭露程序 |
| 6.5 調閱紀錄是否視機關實際需求存檔，以利後續人員查詢及追蹤？ | | | B.6.2.1 資料分享規劃與協議<br>B.6.2.2 資料揭露程序 |
| 6.6 處理個人資料時，是否核對個人資料之輸入、輸出、編輯或更正是否與原件相符？ | | | B. 7.2.1 正確性管理 |
| 6.7 個人資料提供利用時，對資料相符與否如有疑義，是否調閱原檔案查核？ | | | B.6.2.1 資料分享規劃與協議 |
| 6.8 個人資料檔案是否定期備份（例如每個月）？ | | A.12.3.1 資訊備份 | B.10.1.1 個人資料控管措施 |

| 查核項目 | 教育體系資通安全暨個人資料管理規範 | 附錄A 資訊安全管理規範 | 附錄B 個人資料管理規範 |
|---|---|---|---|
| 6.9 是否防止備份檔案被竊取、竄改、毀損、滅失或洩漏？ | | | B.10.1.1 個人資料控管措施 |
| 6.10 個人資料輸入、輸出、存取、更新、更正或註銷等處理行為，是否釐定使用範圍及調閱或存取權限？ | | A.9.2.2 使用者存取權限之配置 | B.10.1.2 存取權限管理程序 |
| 6.11 含有個人資料之紙本報表的申請、讀取、列印、使用、存檔、轉交及銷毀等處理及利用行為，是否建立相關之授權、監督及行為記錄機制？ | | A.8.2.3 資產之處置 | B.10.1.2 存取權限管理程序 |
| 6.12 個人資料檔案之處理行為是否設置使用者代碼及通行碼？ | | A.9.2.4 使用者之秘密鑑別資訊的管理 | B.10.1.2 存取權限管理程序 |
| 6.13 使用者代碼是否與他人共用？ | | A.9.2.4 使用者之秘密鑑別資訊的管理 | B.10.1.2 存取權限管理程序 |
| 6.14 通行碼是否定期更新？ | | A.9.2.4 使用者之秘密鑑別資訊的管理 | B.10.1.2 存取權限管理程序 |
| 6.15 是否視業務及資料重要性，考量其他輔助安全措施？ | | | B.10.1.1 個人資料控管措施<br>B.10.1.3 安全控制措施審查 |
| 6.16 個人資料檔案使用完畢後，是否立即退出應用程式？ | | A.9.4.1 資訊存取限制 | |
| 6.17 是否訂定處理個人資料檔案資訊設備或系統登入通行碼之更換與設定規則？（例如通行碼至少每六個月更換一次，通行碼長度應至少8碼，且包含文數字等。） | | A.9.3.1 秘密鑑別資訊之使用 | |
| 6.18 個人資料檔案之處理，是否視需要考量採取權限區隔、資料加密機制，或相關核准程序加以控管？ | | A.10.1.1 使用密碼式控制措施(加密控制措施)政策 | |
| 6.19 非專責處理特定個人資料者是否具有存取或查閱個人資料之權限？ | | A.9.2.2 使用者存取權限之配置 | B.10.1.2 存取權限管理程序 |
| 6.20 是否留存使用者身分、識別帳號與其行為紀錄以供事後稽查？ | | A.12.4.1事件存錄 | |
| 6.21 個人資料檔案是否禁止存放於網路芳鄰分享目錄？ | | A.9.4.1 資訊存取限制 | |
| 6.22 儲存個人資料的資訊設備是否使用螢幕保護程式？ | | A.11.2.8 無人看管之使用者設備<br>A.11.2.9 桌面淨空及螢幕淨空政策 | |
| 6.23 是否設定螢幕保護密碼？（如將螢幕保護啟動時間設定為15分鐘以內。） | | A.11.2.8 無人看管之使用者設備 | |

| 查核項目 | 教育體系資通安全暨個人資料管理規範 | 附錄A 資訊安全管理規範 | 附錄B 個人資料管理規範 |
|---|---|---|---|
| 6.24 儲存個人資料之資訊設備是否安裝防毒軟體？ | | A.12.2.1 防範惡意軟體之控制措施 | |
| 6.25 是否至少每日更新病毒碼？ | | A.12.2.1 防範惡意軟體之控制措施 | |
| 6.26 是否每週執行排程掃瞄病毒？ | | A.12.2.1 防範惡意軟體之控制措施 | |
| 6.27 儲存個人資料之資訊設備是否定期檢視、更新作業系統、應用程式漏洞（如：Windows作業系統、Windows Office、Adobe Acrobat等）？ | | A.12.6.1 技術脆弱性管理 | |
| 6.28 內部傳遞或與其他機關交換個人資料時，是否選擇可靠且具備保密機制之傳遞方式？（如於實體文件封袋加上彌封、或對資料檔案壓縮加密） | | A.13.2.1資訊傳送政策及程序 | |
| 6.29 是否對轉交或傳輸行為加以記錄流向備查？ | | A.13.2.1資訊傳送政策及程序 | |
| 6.30 自行開發或委外處理個人資料檔案之資訊系統，是否在系統開發生命週期之初始階段，將個人資料檔案的安全需求納入考量（如：邏輯測試）？ | | A.14.1.1 資訊安全要求事項分析及規格 | |
| 6.31 系統之維護、更新、上線、及版本異動等作業，是否有安全管制，避免危害個人資料安全？ | | A.14.2.2 系統變更控制程序 | |
| 6.32 是否允許維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作？ | | A.6.2.2 遠距工作 | |
| 6.33 若需使用遠端登入方式進行維護，是否透過加密通道進行（如：HTTPS、SSH等）且進行監控？ | | A.6.2.2 遠距工作 | |
| 6.34 自行開發或委外處理個人資料檔案之資訊系統，是否將個人資料（包含測試用）施予妥善保護與控管？ | | A.14.3.1 測試資料之保護 | |
| **人員管理** | | A.7人力資源安全 | |
| 6.35 處理個人資料檔案之人員，其職務如有異動，是否將所保管之儲存媒體及有關資料列冊移交？ | | A.8.1.4資產之歸還 | |
| 6.36 接辦人員是否於相關系統重置通行碼或視需要更換使用者識別帳號？ | | A.9.2.6 存取權限之移除或調整 | |
| 6.37 處理個人資料檔案之人員，是否簽訂保密切結書？ | | A.7.1.2聘用條款及條件 | |
| 6.38 處理個人資料檔案之人員離職時或合約終止時，是否有確認取消或停用其使用者識別帳號？ | | A.9.2.6 存取權限之移除或調整 | |

| 查核項目 | 教育體系資通安全暨個人資料管理規範 | 附錄A 資訊安全管理規範 | 附錄B 個人資料管理規範 |
|---|---|---|---|
| 6.39 處理個人資料檔案之人員離職時或合約終止時，是否收繳其通行證及相關證件？ | | A.8.1.4資產之歸還 | |
| 6.40 是否禁止個人資料檔案處理人員使用如 Skype 等即時通訊軟體傳輸個人資料檔案？ | | A.13.2.3 電子傳訊 | |
| 6.41 是否禁止使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案？ | | A.13.2.3 電子傳訊 | |
| 6.42 是否禁止使用點對點(P2P)軟體及Tunnel相關工具下載或提供分享檔案？ | | A.13.2.3 電子傳訊 | |
| 6.43 是否禁止在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料？ | | A.13.2.3 電子傳訊 | |
| 6.44 個人資料檔案若委外建檔，是否於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則？ | | A.13.2.4 機密性或保密協議 | B.12.1.2 委外協議要項 |
| 6.45 與委外廠商所簽訂正式書面協議或契約中，是否明確陳述契約終止時，相關個人資料的銷毀或交還程序？ | | A.15.1.1 供應者關係之資訊安全政策<br>A.15.1.2 於供應者協議中闡明安全性 | B.12.1.2 委外協議要項 |
| **7.認知宣導及教育訓練** | | | |
| 7.1 是否對處理個人資料檔案之人員施予資訊安全與個資隱私保護之教育訓練（內、外訓皆可）？ | | A.7.2.2資訊安全認知、教育及訓練 | B.3.1.2認知與教育訓練 |
| 7.2 是否定期於單位內宣導個資隱私保護之重要性？ | | | B.3.1.1政策認知訓練 |
| 7.3 全體員工及經手個人資料之第三人是否對個人資料保護法及個人資料保護法施行細則等法令有基礎認知？ | | | B.3.1.2認知與教育訓練 |
| 7.4 辦理個人資料保護認知宣導活動完畢後，是否留存相關紀錄備查？ | 柒、四、(三)認知 | | |
| **8.設備安全管理** | | A.11 實體及環境 安全 | 4.13安全議題 |
| 8.1 是否指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施？ | | | B.8.1.1 資料保存與銷毀程序<br>B.10.1.1 個人資料控管措施 |
| 8.2 儲存個人資料檔案之資訊設備是否檢視、處理其錯誤或異常事件等訊息？ | | A.12.4.1 事件存錄 | |
| 8.3 儲存個人資料之資訊設備是否置放於實體安全區域，或與外部網路隔絕？ | | A.13.1.3 網路之區隔 | |
| 8.4 儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，是否指定專人管理？ | | A.8.3.1可移除式媒體之管理 | |

| 查核項目 | 教育體系資通安全暨個人資料管理規範 | 附錄A 資訊安全管理規範 | 附錄B 個人資料管理規範 |
|---|---|---|---|
| 8.5 儲存個人資料檔案的儲存媒體是否放置在有實體保護之環境？ | | A.8.3.1可移除式媒體之管理 | |
| 8.6 是否建立備援機制，以防止資料損壞、遺失或遭竊取？ | | A.12.3.1 資訊備份 | |
| 8.7 個人資料檔案儲存媒體攜出或拷貝複製，是否需經權責單位同意並留存紀錄？ | | A.8.3.1可移除式媒體之管理<br>A.11.2.5 財產之攜出 | |
| 8.8 外部團體或個人更新或維修電腦設備時，是否指派專人在場，確保個人資料之安全及防止個人資料外洩？ | | A.11.2.4 設備維護 | |
| 8.9 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，是否確實刪除該設備所儲存之個人資料檔案？ | | A.11.2.7 設備汰除或再使用之保全 | |
| **三、檢查** | | | |
| **9. 資料安全稽核機制** | 柒、六、(二)內部稽核 | | |
| 9.1 是否定期執行稽核作業，以確保相關管理措施之有效性？ | 柒、六、(二)內部稽核 | A.18.2.2安全政策及標準之遵循<br>A.18.2.3技術遵循性審查 | |
| 9.2 是否建立稽核計畫？ | 柒、六、(二)內部稽核 | | |
| 9.3 是否產生稽核報告？ | 柒、六、(二)內部稽核 | | |
| 9.4 是否在業務變更時，立即執行稽核作業？ | 柒、六、(二)內部稽核 | | |
| **10. 使用紀錄、軌跡資料及證據保存** | | | |
| 10.1是否針對以下個人資料處理相關活動，評估及進行紀錄的保存，以為未來舉證等用途？<br>(a) 因應事故發生所採取行為之紀錄<br>(b) 確認受託人執行委託人要求事項之紀錄<br>(c) 提供當事人行使權利之紀錄<br>(d) 確認資料正確性及更正之紀錄<br>(e) 權限新增、變動及刪除之紀錄<br>(f) 備份及還原測試之紀錄<br>(g) 個人資料交付、傳輸之紀錄<br>(h) 個人資料刪除、廢棄之紀錄<br>(i) 存取個人資料系統之紀錄<br>(j) 定期檢查處理個人資料之資訊系統之紀錄<br>(k) 教育訓練之紀錄<br>(l) 計畫稽核及改善程序執行之紀錄 | 柒、四、(五)文件化資訊 | A.12.4.1 事件存錄 | |
| **11. 個人資料安全維護之整體持續改善** | 柒、七、改善 | | |
| 11.1是否針對個資安全事件及稽核缺失訂定改善行動或預防措施，以減低事件再次發生機會？ | 柒、七、(一)不符合項目及矯正措施 | | |
| 11.2是否將缺失改善情形、風險評估結果及個人資料資訊安全事件等，定期呈報個人資料保護管理小組？ | 柒、六、(三)管理審查 | | |

## 二、 個資法施行細則 11 項安全維護事項要求對照表

| 個資法<br>安全維護事項 | ISO 27001:2013 | BS10012:2009 | ISO 29100:2011 |
|---|---|---|---|
| 配置管理之人員及相當資源 | 5.3組織角色、責任與授權<br>7.1資源 | 3.5職責與歸責性<br>3.6 資源提供<br>4.1重要職責指派 | 5.10歸責性 |
| 界定個人資料之範圍 | 4.3決定資訊安全管理系統範圍 | 3.2 PIMS的範圍與目標 | 4.2行為者及角色<br>4.3互動<br>4.4辨識PII |
| 個人資料之風險評估及管理機制 | 6.1風險與機會處理措施 | 4.4風險評鑑 | 4.5隱私保全要求事項 |
| 事故之預防、通報及應變機制 | 6.1風險與機會處理措施<br>附錄A 全<br>A.16資訊安全事故管理<br>A.17 營運持續管理 資訊安全層面 | 4.7公平與合法的處理<br>4.13安全議題 | 4.6 隱私權政策<br>4.7隱私控制措施 |
| 個人資料蒐集、處理及利用之內部管理程序 | | 4.8個人資料處理的特定目的<br>4.9 適當、相關且不過度<br>4.10正確性<br>4.11保存與處置<br>4.12個人權利<br>5.2管理審查 | 5.2當事人同意與選擇<br>5.3目的合法性明確化<br>5.4蒐集限制<br>5.5個資最小化<br>5.6使用、保存及揭露限制<br>5.7正確性與品質<br>5.8公開、透明及通知<br>5.9當事人權利<br>5.12隱私遵循性 |
| 資料安全管理及人員管理 | A.7人力資源安全<br>A.8資產管理 | 4.13安全議題 | 5.11資訊安全 |
| 認知宣導及教育訓練 | 7.3認知<br>A.7人力資源安全 | 3.7將PIMS納入組織文化<br>4.3訓練與認知 | |
| 設備安全管理 | A.11 實體及環境 安全 | 4.13安全議題 | 5.11資訊安全 |
| 資料安全稽核機制 | 9.2 內部稽核<br>A.18.2.3技術遵循性審查 | 5.1內部稽核 | |
| 必要之使用紀錄、軌跡資料及證據之保存 | 7.5 文件化資訊<br>A.12.4 存錄及監視 | | |
| 個人資料安全維護之整體持續改善 | 10改善 | 6改進PIMS | |