

中華民國 105 年 8 月 5 日
教育部令 臺教資（四）字第 1050094009B 號

訂定「教育體系資通安全暨個人資料管理規範」，並自即日生效。

附「教育體系資通安全暨個人資料管理規範」

部 長 潘文忠 出國
政務次長 蔡清華 代行

教育體系 資通安全暨個人資料 管理規範



中 華 民 國 105 年 8 月 5 日

本規範歷次變更紀錄

[illegible]

目 錄

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

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，得斟酌組織規模、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，值得注意的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：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。

附錄 A

資通安全管理規範

本標準列出之控制目標與控制措施乃參考ISO/CNS 27001:2013 附錄 A 控制措施，並依據原有「教育體系資通安全規範」，以及教育體系與相關單位既有之屬性與特點，歸納各等級應有安全控制措施。

為方便各施行單位承辦人員與驗證稽核人員參照國際與國家標準的要求與實作指引。本規範控制措施條文要求援引 ISO/CNS 27001:2013 附錄 A 控制措施的條文編號與說明，而控制措施實作指引中，屬原有控制措施者依據原有「教育體系資通安全規範」進行說明，新增控制措施部分則增加 ISO/CNS 27002:2013 實作指引說明。各單位在實作時宜參考相關內容，以確保執行的完整性，實作指引說明將如有「應」一字為必要執行項目，「宜」一字則為可選擇是否執行之項目，施行單位可依據其資訊系統特性與風險狀況選用適當之實作方式。

同時，為減少各施行單位轉換上的困難，援引原有學群分類方式進行安全等級歸類。施行單位可依據「附件 1 各級教育機構適用控制項對照表」之建議導入各適用之控制措施，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，施行單位識別出具有等級為「高」者之資訊系統時，則應加入 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。各單位得考量自身之需求與特性，考慮增加其他必要之控制目標及控制措施。

附註：控制項編號下(I/P)註記代表 ISMS 與 PIMS 可共用項目，並以規範建置步驟與附錄 A 控制項編號進行對照，俾便施行單位進行 ISMS 的建置作業，同時導入 PIMS 則應考量適用該共用項目以符合 ISMS 與 PIMS 的要求。

A.5

資訊安全政策訂定與評估

所謂的資訊安全政策，代表著管理階層的決心以及其對於單位推動資訊安全的支持，除了制定資訊安全政策以貫徹至單位上下外，不斷的評估、檢視已制定資訊安全政策的合適性與否，也是重要的部份；本章節的重點，在於管理階層的態度表示，雖不至於各項細節皆事必躬親，然而大方針的規劃與制定，將能讓所有的員工體認管理者的投入，以及對於單位資訊安全重要性的了解。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.5 資訊安全政策					A.5
控制目標	A.5.1	資訊安全之管理指導方針		B.1.1	A.5.1
控制項	A.5.1.1 (I/P)	資 訊 安 全 政 策	資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。	B.1.1.1	A.5.1.1
	A.5.1.2 (I/P)	資 訊 安 全 政 策 之 審 查	資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。	B.1.1.1	A.5.1.2

實作指引

(一) 資訊安全之管理指導方針 (A.5.1)

1. 資訊安全政策 (A.5.1.1)

資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。

施行單位制定資訊安全控制政策或原則，應說明管理階層的承諾及該單位管理資訊安全的方法，宜含括下列事項：

- (1) 符合法令及契約對施行單位資訊安全的要求與規定。
- (2) 人員資訊安全角色與責任的相關規定，宜載明於人員工作說明書或相關作業手冊中。
- (3) 施行單位員工如違反資訊安全相關規定，應依紀律程序處理。
- (4) 政策遵須所需參考文件，例如針對特定資訊系統的詳盡安全政策和程序或使用者應遵守的安全規則。

2. 資訊安全政策之審查 (A.5.1.2)

資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。

面對資訊安全事件的發生、資訊安全相關法令與其他影響因素的改變時，資訊安全控制政策或原則應進行即時的評估，並定期（宜每半年）審查政策或原則的可行性與有效性。

施行單位宜評估資訊安全控制政策或原則，含括下列事項：

- (1) 資訊安全評估對象宜包含資訊設備及系統提供者、資訊及資料擁有者、使用者、管理者、系統維護者與其他相關人員。
- (2) 資訊系統管理者宜配合定期（宜每半年）資訊安全評估作業，檢討相關人員是否遵守施行單位之資訊安全控制政策、規範與其他規定。
- (3) 宜定期（宜每半年）檢討評估各項軟、硬體設備的安全性，確保其符合施行單位的安全標準。
- (4) 安全評估可視需求委由內部或外界專業人員進行，以人工或自動化軟體工具方式執行，產生技術評估報告，供日後解讀分析。
- (5) 評估宜記錄備查。
- (6) 修訂過的控制政策宜獲得管理階層的批准。

A.6

資訊安全組織

在施行單位資訊安全政策建立完成後，執行組織因應而生，以落實及推動各項既定政策；因此，施行單位應由副首長以上擔任或指定管理制度之管理人或召集人，代表學校或單位落實資訊安全的決心，負責推動資訊安全組織，召開資訊安全會報、訂定權責分屬、主導評估建置等相關活動，除了解各項需求外，籌備必要資源，確保資訊安全措施正常運作，建立起一完善、安全之環境，降低施行單位資訊安全威脅的機率。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.6 資訊安全之組織					A.6 A.10 A.11
控制目標	A.6.1	內部組織		柒二 (B.2.1)	A.6.1 A.10.1
控制項	A.6.1.1 (I/P)	資訊安全之 角色及責任	應定義及配置所有資訊安全責任。	柒二(三) B.2.1.1 B.2.1.2 B.2.1.3	A.6.1.1
	A.6.1.2	職務區隔	衝突之職務及責任範圍應予以區隔，以降低組織資產遭未經授權或非蓄意修改或誤用之機會。		A.10.1.3
	A.6.1.3	與權責機關 之聯繫	應維持與相關權責機關之適切聯繫。		A.6.1.4
	A.6.1.4	與特殊關注 方之聯繫	應維持與各特殊關注方或其他各種專家安全論壇及專業協會之適切聯繫。		A.6.1.5
	A.6.1.5 (建議)	專案管理之 資訊安全	不論專案之型式，應在專案管理中因應資訊安全。		
控制目標	A.6.2	行動裝置及遠距工作			A.11.6
控制項	A.6.2.1	行動裝置政 策	應採用政策及支援之安全措施，以管理因使用行動裝置所導致之風險。		A.11.6.1
	A.6.2.2	遠距工作	應實作政策及支援之安全措施，以保護存取、處理或儲存於遠距工作場所之資訊。		A.11.6.2

實作指引

(一) 內部組織 (A.6.1)

1. 資訊安全之角色及責任 (A.6.1.1)

應定義及配置所有資訊安全責任。

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，並應依據「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」或相關資安規定中各級單位資安專責人力要求進行指派。

由 ISMS 管理人與管理小組舉辦之定期(宜每半年)資訊安全會報，召集相關單位代表進行工作與責任的分派，確保資訊安全相關計畫的進行，並展現管理階層的支持。

定期(宜每半年)召開之資訊安全會報權責宜包含：

- (1) 訂定資訊安全角色與權責分工，賦予相關人員應有之安全權責，包含資訊安全相關政策、計畫、措施、技術規範、安全技術研究、建置、評估，乃至使用管理、保護、資訊機密維護、稽核等，並以書面或其他方式記錄留存。
- (2) 確保安全活動符合資訊安全政策。
- (3) 資訊安全教育訓練及認知之提昇。
- (4) 評估資訊安全事項審查及監視的結果，並針對資訊安全事故提出適當的行動方案。

2. 職務區隔 (A.6.1.2)

衝突之職務及責任範圍應予以區隔，以降低組織資產遭未經授權或非蓄意修改或誤用之機會。

資訊安全責任之分散，宜考量：

- (1) 對關鍵性資訊業務，分散資訊安全管理及執行作業的責任，建立相互制衡機制，分別賦予相關人員必要的安全責任，以降低人為疏忽或故意，導致資料或系統遭不法或不當之使用，或遭未經授權的人員竄改；。
- (2) 宜在資訊人力許可下，盡可能由不同人員執行下列業務及功能：
 - a. 業務系統之使用。
 - b. 資料建檔。
 - c. 系統使用與操作。
 - d. 網路管理。
 - e. 系統管理。
 - f. 系統發展及維護。
 - g. 變更管理。
 - h. 安全管理。
 - i. 安全稽核。

3. 與權責機關之聯繫 (A.6.1.3)

應維持與相關權責機關之適切聯繫。

為確保資訊安全作業的順利運行，需與執法機關、主管機構、資訊服務廠商及電信公司建立適當的溝通管道。

在跨機關的合作與協調上，宜達到：

- (1) 與資訊安全業務相關機關視需求建立與維護適當的互動管道，以即時獲得外

部的資源協助，解決相關問題。

- (2) 在與外部機關互動交流時，宜予以適當的限制，防止敏感性資訊遭未經授權之存取。

4. 與特殊關注方之聯繫 (A.6.1.4)

應維持與各特殊關注方或其他各種專家安全論壇及專業協會之適切聯繫。

在必要時，須向單位內部專業人員或外部專業諮詢人員徵詢、協調資訊安全建議。在資訊安全顧問及諮詢方面，宜考量：

- (1) 施行單位資訊安全人力、能力和經驗不足情況下，得以委請內部專業人員或外界專家學者提供顧問諮詢的服務。
- (2) 對經由委請之提供顧問諮詢服務的專家學者，相關單位及人員應予以必要的協助及支援。

5. 專案管理之資訊安全 (A.6.1.5) (建議)

不論專案之型式，應在專案管理中因應資訊安全。

對於有完成時間之資訊相關專案，如資訊系統發展、維護或升級專案、軟硬體購置或升級專案等，宜考量在專案管理之資訊安全，如：

- (1) 將資訊安全目標涵蓋於專案目標內。
- (2) 在專案的初期階段實施資訊安全風險評鑑以識別必要的控制措施。
- (3) 資訊安全要求事項納入專案各階段管理作業。
- (4) 在所有專案中宜每階段或專案變更前處理與審查資訊安全相關議題。
- (5) 在專案管理方法中宜對特定角色界定與賦予資訊安全責任。

(二) 行動裝置及遠距工作 (A.6.2)

1. 行動裝置政策 (A.6.2.1)

應採用政策及支援之安全措施，以管理因使用行動裝置所導致之風險。

使用行動裝置時，應特別小心以確保不會危及營運資訊。行動裝置政策宜考慮在無保護的環境下以行動裝置工作的風險。

在公共場所、會客室以及其他無保護區域，使用行動裝置應謹慎。宜備妥保護措施避免在這些裝置上儲存與處理的資訊遭到未經授權存取或揭露，例如使用密碼技術與強制使用機密鑑別資訊。

行動裝置政策宜考慮下列事項：

- (1) 行動裝置之註冊。
- (2) 實體保護之要求。
- (3) 軟體安裝之限制。
- (4) 行動裝置軟體版本與適用修補程式的要求。
- (5) 連接資訊服務的限制。
- (6) 存取控制。
- (7) 密碼學技術。
- (8) 惡意軟體保護。
- (9) 遙控關閉、抹除及鎖定。

(10) 備份。

(11) 網頁服務與網頁應用系統之使用。

2. 遠距工作 (A.6.2.2)

應實作政策及支援之安全措施，以保護存取、處理或儲存於遠距工作場所之資訊。

關於遠距工作活動的控管宜：

(1) 適用單位既訂之作業控制措施，降低各種可能的資訊安全風險。

(2) 受到權責單位的核可及符合相關規定，才得以進行遠距工作。

A.7

人力資源安全

再怎麼嚴密完整的政策與控制措施，缺乏觀念正確、訓練有素的人員執行，亦是惘然。因此，施行單位所屬相關人員需針對其擔負的資訊安全責任，進行管理與教育訓練，透過定期的課程訓練，確保其在職位上能執行各項相關資訊安全措施，降低可能的資訊安全風險。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.7 人力資源安全					A.8
控制目標	A.7.1	聘用前		B.10.1	
控制項	A.7.1.1 (I/P)	篩選	對所有可能被聘用者所進行之背景調查，應依照相關法律、法規及倫理，並應相稱於營運要求及其將存取之資訊保密等級及組織所察覺之風險聘用。	B.10.1.1	
	A.7.1.2 (I/P)	聘用條款及條件	施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。	B.10.1.1	
控制目標	A.7.2	聘用期間		B.3.1 B.10.1	A.8.2
控制項	A.7.2.1 (I/P)	管理階層責任	管理階層應要求所有員工及承包者，依施行單位所建立政策及程序施行資訊安全事宜。	B.10.1.1	
	A.7.2.2 (I/P)	資訊安全認知、教育及訓練	施行單位內所有員工及相關之承包者，均應接受及其工作職務相關的組織政策及程序之適切認知、教育及訓練，並定期更新。	柒四(二) 柒四(三) B.3.1.2 B.10.1.1	A.8.2.1
	A.7.2.3	懲處過程	應具備正式即已傳達之懲處過程，以對違反資訊安全之員工採取行動。		A.8.2.2
控制目標	A.7.3	聘用之終止及變更		B.10.1	A.8.3
控制項	A.7.3.1 (I/P)	聘用責任之終止或變更	應對員工及承包者定義、傳達於聘用終止或變更後資訊安全責任及義務仍保持有效，並執行之。	B.10.1.1	A.8.3.1

實作指引

(一) 聘任前 (A.7.1)

1. 篩選 (A.7.1.1)

對所有可能被聘用者所進行之背景調查，應依照相關法律、法規及倫理，並應相

稱於營運要求及其將存取之資訊保密等級及組織所察覺之風險聘用。

執行或接觸機密或敏感性業務的人員，在聘用前應考量依照相關法令法規及倫理，及營運要求與風險，進行背景查核或評估。

為特定資訊安全角色而聘用人員時，施行單位宜確保應徵者：

- (1) 有必要資格以執行資訊安全角色。
- (2) 可被信賴以承擔該角色，特別是施行單位之關鍵角色。

2. 聘用條款及條件 (A.7.1.2)

施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。施行單位應讓員工了解在資訊安全上應負的一般及特定之資訊安全責任，包括資訊安全事件的通報。(原 A.5.1.1)

施行單位與員工及承包者簽訂之聘僱契約等或保密協議書等契約化協議，應敘明雙方對資訊安全的責任。

員工的契約義務宜反映施行單位的資訊安全政策：

- (1) 資訊安全角色與責任宜在聘用前向工作應徵者進行傳達。
- (2) 施行單位宜確保員工所擁有的資訊系統和服務存取權限僅限於雙方簽訂之協議書範圍內。
- (3) 適當時，聘用條款與條件所包含的責任在結束聘用關係後宜持續一段期間。

(二) 聘用期間 (A.7.2)

1. 管理階層責任 (A.7.2.1)

管理階層應要求所有員工，依施行單位所建立政策及程序施行資訊安全事宜。

管理階層責任宜包括確保員工：

- (1) 核准存取敏感的資訊或資訊系統前，瞭解其資訊安全角色與責任。
- (2) 對個人安全角色與責任的認知程度，符合聘用條款與條件，擁有適切之技能與資格，並定期（宜每半年）接受教育訓練。
- (3) 具有通報管道以通報資訊安全政策或程序之違反情事。

2. 資訊安全認知、教育及訓練 (A.7.2.2)

所有員工及相關之承包者，均應接受及其工作職務相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

應依據「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」或相關資安規定中各級單位資安教育訓練要求進行規劃。

施行單位內所有員工、合作廠商與第三方使用者應接受適當之資訊安全訓練，以及資訊安全政策與程序之認知宣導課程。

有關資訊安全教育與訓練的部份：

- (1) 宜定期（宜每半年）以人員角色及職能為基礎，針對不同層級人員進行進行資訊安全教育及訓練，促使員工了解資訊安全的重要性以及各種可能的安全風險，提高員工資訊安全意識，並遵守資訊安全規定。
- (2) 施行單位同意及授權使用者存取系統前，宜教導使用者登入系統之程序，以及如何正確地操作及使用軟體及違規處理。

(3) 非施行單位所屬員工之相關人員，宜確保其對資訊安全政策、相關控制及程序有一定的了解，並清楚其資訊安全責任。

3. 懲處過程 (A.7.2.3)

應具備正式即已傳達之懲處過程，以對違反資訊安全之員工採取行動。

依據既定之條款或合約，違反施行單位之資訊安全政策與程序之人員，應予以適當之懲罰處理。

(三) 聘用之終止及變更 (A.7.3)

1. 結束聘用之處理 (A.7.3.1)

應對員工及承包者定義、傳達於聘用終止或變更後資訊安全責任及義務仍保持有效，並執行之。

對於離調職員工傳達資訊安全要求事項與法律責任仍應持續遵守，並儘可能包括所有保密協議或聘用條款與條件中所包含的責任，且在結束聘用關係後宜持續一段期間。

A.8

資產管理

為確保施行單位資產獲得適切的保護，明確的資產分類與保護層級，提高資產保管執行效率，降低受危害的可能性，勢必進行徹底財產清點與分類；由於財產記錄在各學校單位已有職掌單位，為避免工作重疊的浪費，可僅進行補充加強的部份，擴充既有的資訊資產清單，使其符合資訊安全政策，降低可能的威脅及危險。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.8 資產管理					A.7 A.8 A.10
控制目標	A.8.1	資產責任		B.4.1	A.7.1 A.8.3
控制項	A.8.1.1 (I/P)	資產清冊	應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。	B.4.1.1	A.7.1.1
	A.8.1.2	資產擁有權	清冊中所維持之資產應有擁有者。		A.7.1.1
	A.8.1.3	資產之可被接受的使用	對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。		A.7.1.1
	A.8.1.4	資產之歸還	所有員工及外部使用者於其聘用、契約或協議終止時，應歸還其據有之全部組織資產。		A.8.3.2
控制目標	A.8.2	資訊分級		B.4.1 B.10.1	A.7.1 A.10.7
控制項	A.8.2.1 (I/P)	資訊之分級	資訊應依法律要求、價值、重要性及其對未經授權揭露或修改之敏感性分級。	B.4.1.2 B.10.1.1	A.7.1.2
	A.8.2.2 (I/P)	資訊之標示	應依施行單位所採用之資訊級方案，發展及實作一套適切的資訊標示程序。	B.4.1.2 B.10.1.1	A.7.1.2
	A.8.2.3 (I/P)	資產之處置	應依施行單位所採用之資訊分級方案，發展及實作處置資產之程序。	B.10.1.1	A.10.7.3
控制目標	A.8.3	媒體處理		B.8.1 B.10.1	A10.7
控制項	A.8.3.1 (I/P)	可移除式媒體之管理	應依施行單位所採用之資訊分級方案，實作管理可移除式媒體之程序。	B.10.1.1	A.10.7.1

	A.8.3.2 (I/P)	媒體之汰除	當不再需要媒體時，應使用正式程序加以安全汰除。	B.8.1.1 B.10.1.1	A.10.7.2
	A.8.3.3 (I/P)	實體媒體傳送	應保護含有資訊之媒體在傳送時，不受未經授權的存取、誤用或毀損。	B.10.1.1	

實作指引

(一) 資產責任 (A.8.1)

1. 資產清冊 (A.8.1.1)

應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。

應製作所有資訊資產之清冊，並定期（宜每半年）維護、更新。

資訊資產之清冊宜達到：

- (1) 建立一份資訊資產目錄，訂定該資產之項目、擁有者及安全等級分類等，並定期（宜每半年）維護與更新其內容。
- (2) 資訊資產參考類別如下：
 - a. 一般資產：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業性及支援程序、業務永續運作計畫、預備作業計畫等。
 - b. 軟體資產：應用軟體、系統軟體、發展工具及公用程式等。
 - c. 實體資產：電腦及通訊設備、磁性媒體資料及其他技術設備。
 - d. 技術服務資產：電腦及通信服務、其他技術性服務（電源及空調）。
- (3) 所有有關資訊系統或服務之資產宜指定專責單位保管，其職掌如下：
 - a. 確定資訊及資產適當地分級。
 - b. 定期（宜每半年）審查存取限制及分類。
- (4) 有關資訊系統或服務的資產，其可接受的使用方式宜被確認，並以書面或其他方式記錄後確實執行。

2. 資產擁有權 (A.8.1.2)

清冊中所維持之資產應有擁有者。

資訊資產之清冊宜達到：

- (1) 所有有關資訊系統或服務之資產宜指定專責單位保管，其職掌如下：
 - a. 確定資訊及資產適當地分類。
 - b. 定期（宜每半年）審查存取限制及分類。

3. 資產之可被接受的使用 (A.8.1.3)

對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。

有關資訊系統或服務的資產，其可接受的使用方式應該被確認，並以書面或其他方式記錄後確實執行。並讓所有具有存取權限的員工或委外單位使用者，知悉資產可接受的使用方式，相關的資訊安全要求事項，以及其所具有的責任。

4. 資產之歸還 (A.8.1.4)

所有員工及外部使用者於其聘用、契約或協議終止時，應歸還其據有之全部組織

資產。

資產繳回應有正式的離職程序，顯示其已繳回單位資產。

資產的繳回宜：

- (1) 包括所發給的軟體、單位文件、及設備。其它單位的資產；例如行動運算設備、信用卡、智慧卡、手冊及其它必須繳回的電子媒體。
- (2) 若使用自有的設備處理資訊，宜有正常程序以確保相關資訊已轉移至單位，並安全的從設備中移除。
- (3) 對單位持續操作的重要知識或經驗，宜確實進行移轉或紀錄。

(二) 資訊分級 (A.8.2)

1. 資訊之分級 (A.8.2.1)

資訊應依法律要求、價值、重要性及其對未經授權揭露或修改之敏感或機密性進行分級作業。

資訊資產分級原則，宜包含：

- (1) 資訊安全等級分級原則如下所示：
 - a. 宜建立資訊安全等級之分級標準，考量資訊分享及限制的影響、未經授權的系統存取或是系統損害對機關業務的衝擊。
 - b. 資訊安全等級，依據國家機密保護、個人資料保護及政府資訊公開等相關法規，將區分為機密性、敏感性及一般性等三類。
 - c. 界訂資訊安全等級之責任，宜由資料的原始產生者或是由指定的系統所有者負責。
 - d. 須執行或參考其他單位訂定之資訊安全等級時，宜特別注意其與本單位的資訊安全等級，在定義及標準上是否相同。

2. 資訊之標示 (A.8.2.2)

應依施行單位所採用之安全等級方案，發展及實作一套適切的資訊標示程序。

資訊資產分級標示原則，宜包含：

- (1) 資訊標示的程序需要涵蓋實體與電子格式的資訊與其相關資產。
- (2) 標籤宜易於識別，並考量依據媒體型式於程序中述明於何處及如何附加標籤。程序可界定標籤省略之案例以降低工作負載，例如：非機密資訊之標籤。
- (3) 各系統之輸出包含經分級屬於敏感或關鍵之資訊者，宜附上適當的分級標籤。

3. 資產之處置 (A.8.2.3)

應依組織所採用之資訊分級方案，發展及實作處置資產之程序。

重要資產與資料應進行控管，並安全的保存。

保護原則宜包含：

- (1) 重要資訊資產宜依相關規定以安全方式保存，以防止遺失、毀壞、被偽造或竄改。
- (2) 超過法定保存期限的資產與資料，可依相關規定刪除或銷毀，但事前宜考量可能造成的不利影響。
- (3) 資產與資料的管理，宜遵循下列原則：

- a. 訂定資產與資料保存、儲存、處理等指導原則作為執行的依據。
- b. 資料保存期限宜依資料型態及法定保存期限之規定擬定。
- c. 宜建立及維護重要資訊資源的目錄。
- d. 宜採行適當的措施，保護機關的重要資料，防止資料遺失、毀壞及被偽造或竄改。

(三) 媒體處理 (A.8.3)

1. 可移除式媒體之管理 (A.8.3.1)

應依組織所採用之資訊分級方案，實作管理可移除式媒體之程序。

電腦儲存媒體、可攜式媒體或印出報表，應制定控管措施。

資訊資產分類原則，宜包含：

- (1) 可隨時攜帶及移動的儲存媒體，宜建立使用管理程序，規範磁帶、磁碟及電腦輸出報告等使用。
- (2) 儘量避免使用有明顯用途標示的資料儲存系統；電腦媒體儲存的資料內容，不宜在外部以明顯方式標示，以免被輕易地辨識出來。
- (3) 可重複使用的資料儲存媒體，不再繼續使用時，宜將儲存的內容消除。
- (4) 對於要帶離機關辦公場所的儲存媒體，宜建立書面的授權規定，並建立使用紀錄，以備日後稽核之用。
- (5) 儲存媒體宜依製造廠商提供的保存規格，存放在安全的環境。
- (6) 儲存資料的媒體到達製造廠商提供的使用期限時，宜在別處再作儲存，以免資料遺失。
- (7) 宜登記可攜式媒體來減少資料遺失的機會。
- (8) 可攜式媒體宜在公務理由上才可使用。

2. 媒體之汰除 (A.8.3.2)

當不再需要媒體時，應使用正式程序加以安全汰除。

宜建立媒體安全汰除之正式程序以將機密資訊洩露給未經授權人員的風險降至最低。安全的汰除含有機密資訊的媒體之程序宜考量資訊的敏感度及下列項目：

- (1) 含有機密資訊的媒體宜安全地儲存與汰除，例如：燒毀或撕碎，或清除資料後由施行單位內其他應用系統使用。
- (2) 宜備妥程序以識別可能需要安全汰除的項目。
- (3) 許多施行單位提供媒體的收集和汰除服務；宜謹慎選擇有適切控制措施和經驗的合適外部團體。
- (4) 敏感項目的汰除宜予存錄，以利事後查詢與稽核。

3. 實體媒體傳送 (A.8.3.3)

應保護含有資訊之媒體在傳送時，不受未經授權的存取、誤用或毀損。

保護傳送含有資訊之媒體，宜考慮下列項目：

- (1) 使用可靠的運輸工具或遞送公司。
- (2) 所授權的遞送人員清單宜經管理階層同意。
- (3) 發展查證遞送人員身分之程序。

- (4) 包裝宜足以保護媒體，防止因運送途中任何實體損壞而受損，並符合製造商的規格，以防範所有可損壞媒體的環境因素，例如暴露於熱源、濕氣或電磁場。
- (5) 保留日誌，識別媒體內容、保護措施以及記錄傳移給運送保管人的次數和目的地的接收者。

A.9

存取控制

施行單位應鑑別（Identify，該資料機密等級與存取動作）與文件化相關之存取行為，建立存取控制政策的內容及範圍，防範非經授權存取的可能及危險，降低相關資訊或檔案遭竊取的威脅，此部分可說是機密或敏感性資料保護的最後一道防線，何種層級人員可進行哪些部分的存取，皆須訂定嚴密的規範與機制，除可防止外部人員的竊取外，更降低內部洩露的可能。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.9 存取控制					A.8,A.11 A.12
控制目標	A.9.1	存取控制之營運要求事項		B.10.1	A.11.3
控制項	A.9.1.1 (I/P)	存取控制政策	存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。	B.10.1.2	A.11.1.1
	A.9.1.2	對網路及網路服務之存取	應僅提供予使用者存取其已被特定授權使用之網路及網路服務。		A.11.3.1
控制目標	A.9.2	使用者存取管理		B.10.1	A.8.3 A.11.1
控制項	A.9.2.1 (I/P)	使用者註冊與註銷	應實作正式之使用者註冊及註銷過程，俾能指派存取權限。	B.10.1.2	A.11.1.1
	A.9.2.2 (I/P) (建議)	使用者存取權限之配置	應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。	B.10.1.2	
	A.9.2.3 (I/P)	具特殊存取權限之管理	應限制及控制具特殊存取權限之配置及使用。	B.10.1.2	A.11.1.2
	A.9.2.4 (I/P)	使用者之秘密鑑別資訊的管理	應以正式之管理過程控制秘密鑑別資訊的配置。	B.10.1.2	A.11.1.3
	A.9.2.5 (I/P)	使用者存取權限之審查	施行單位應定期審查使用者存取權限。	B.10.1.2	A.11.1.4
	A.9.2.6 (I/P)	存取權限之移除或調整	所有員工及外部使用者對資訊及資訊處理設施之存取權限，一旦其聘用、契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。	B.10.1.2	A.8.3.3
控制目標	A.9.3	使用者責任		B.10.1	

控制項	A.9.3.1 (I/P)	秘密鑑別資訊 之使用	於使用秘密鑑別資訊時，應要求使用者遵循施行單位之實務規定。	B.10.1.2	
控制目標	A.9.4	系統及應用存取控制		B.10.1	A.11.4 A.11.5 A.12.4
控制項	A.9.4.1 (I/P)	資訊存取限制	應根據存取控制政策，限制對資訊及應用系統功能之存取。	B.10.1.2	A.11.5.1
	A.9.4.2 (I/P)	保全登入程序	當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。	B.10.1.2	A.11.4.1
	A.9.4.3 (I/P)	通行碼管理系統	通行碼管理系統應為互動式，並應確保嚴謹通行碼。	B.10.1.2	A.11.4.2
	A.9.4.4	具特殊權限公用程式之使用	應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。		A.11.4.3
	A.9.4.5	對程式源碼之存取控制	應限制對程式原始碼之存取。		A.12.4.3

實作指引

(一) 使用者存取控制 (A.9.1)

1. 存取控制政策 (A.9.1.1)

存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。

資產擁有者宜決定對其資產的存取控制規則、存取權與限制，還有反映相關資訊安全風險的控制措施之細節和嚴格性。

該政策宜考量下列內容：

- (1) 營運應用系統的安全要求。
- (2) 資訊傳播和授權政策，以及資訊的安全等級與分級。
- (3) 不同系統與網路間存取控制與資訊分級政策的一致性。
- (4) 有關保護資料或服務存取的適當法規及所有的契約責任與義務。
- (5) 存取控制角色的區隔與特權存取管理。
- (6) 存取權限申請與授權程序。
- (7) 存取控制措施定期（宜每半年）審查的要求。
- (8) 存取權限的移除。
- (9) 關於使用者身分和安全鑑別資訊之使用和管理的重要事件歸檔。

2. 對網路及網路服務之存取 (A.9.1.2)

應僅提供予使用者存取其已被特定授權使用之網路及網路服務。

施行單位須清楚限定使用者只能直接存取准許使用之服務。

宜制定一項關於網路及網路服務使用的政策，其涵蓋：

- (1) 允許存取的網路及網路服務。
- (2) 決定那些使用者可以存取那些網路及網路服務的授權程序。
- (3) 保護網路連線及網路服務的管理控制措施與程序。
- (4) 存取網路及網路服務的方式（例如使用 VPN 或無線網路）。

(5) 存取不同網路服務的使用者鑑別要求。

(6) 網路服務使用的監視。

(二) 使用者存取管理 (A.9.2)

1. 使用者註冊及註銷 (A.9.2.1)

應實作正式之使用者註冊及註銷過程，俾能指派存取權限。

關於使用者註冊管理宜：

(1) 對於多人使用的資訊系統，建立正式的使用者註冊程序。

(2) 使用者註冊管理程序，宜考量：

- a. 查核使用者是否已經取得使用該資訊系統的正式授權。
- b. 查核使用者被授權的程度是否與業務目的相稱，以及符合資訊安全政策與規定。
- c. 以書面或其他方式告知使用者系統存取權利。
- d. 要求使用者簽訂約定，使其確實了解系統存取的各項條件及要求。
- e. 在系統使用者尚未完成正式授權程序前，資訊服務提供者不得對其提供系統存取服務。
- f. 宜建立及維持系統使用者之註冊資料紀錄，以備日後查考。
- g. 使用者調整職務及離（休）職時，宜盡速註銷其系統存取權利。
- h. 宜定期（宜每半年）檢查及取消閒置不用的識別碼及帳號。
- i. 閒置不用的識別碼不宜重新配予其他的使用者。

2. 使用者存取權限之配置 (A.9.2.2) (建議)

應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。

指派或撤銷使用者身分識別之存取權限配置程序宜包括：

- (1) 使用資訊系統或服務的授權流程。
- (2) 查證存取等級授與的適當性，且符合存取政策級職務區隔等要求。
- (3) 確保授權程序完成後才開啟存取權限。
- (4) 維護資訊系統與服務之使用者存取權限記錄。
- (5) 變更角色或工作的使用者須立即調整其存取權限；已離開施行單位的使用者宜立即移除或封鎖其存取權限。
- (6) 資訊系統或服務的擁有者宜定期（宜每半年）審查存取權限。

3. 具特殊存取權限之管理 (A.9.2.3)

應限制及控制具特殊存取權限之配置及使用。

關於特許權限的限制與控管宜：

- (1) 嚴格管制系統存取特別權限。
- (2) 針對有必要特別保護的系統，賦予使用者系統存取特別權限，並依下列的授權程序管理：
 - a. 宜確認系統存取特別權限之事項，例如作業系統、資料庫管理系統、應用系統、需賦予系統存取特別權限的人員名單。

- b. 宜依執行業務的需求，視個案逐項考量賦予使用者系統存取特別權限；系統存取特別權限之配予，宜以執行業務及職務所必要者為限。
- c. 宜建立申請系統存取特別權限之授權程序，並只能在完成正式授權程序後，才能配予使用者；另外，宜將系統存取特別權限之授權資料建檔。
- d. 宜促進開發與使用系統的例行作業，以避免授予使用者特別權限的要求。
- e. 開發與使用程式，宜避免以特別權限執行。
- f. 特別權限宜授予正常營運使用之外的使用者。

4. 使用者之秘密鑑別資訊的管理 (A.9.2.4)

應以正式之管理過程控制秘密鑑別資訊的配置。

應建立用於驗證使用者身分的秘密鑑別資訊（如通行碼、加密金鑰或憑證資訊等）之管理制度。

秘密鑑別資訊之控管宜考量：

- (1) 盡量以簽訂書面約定或其他方式，要求使用者善盡保護個人通行碼之責任；如屬於群組軟體之使用者，宜確保工作群組的通行碼，僅限群組成員使用。
- (2) 如由使用者自行保管或維護秘密鑑別資訊(如通行碼)的機密性，宜以配予臨時性秘密鑑別資訊(如通行碼)並強迫使用者立即更改的方式處理。
- (3) 使用者遺失或忘記秘密鑑別資訊時，可於驗證使用者身分後，提供臨時性的通行碼，以利系統辨認使用者。
- (4) 宜以安全的方式將臨時的秘密鑑別資訊(如通行碼)交付使用者，避免經由第三者，或是以未受保護的電子郵件遞等電子方式交付給使用者，並建立確認收到之機制。
- (5) 系統如經評估須建立更高等級的安全機制，可利用電子簽章等安全等級更高的存取控制技術。

5. 使用者存取權限之審查 (A.9.2.5)

資產擁有者應定期審查使用者之存取權限。

施行單位應定期（宜每半年）審查使用者存取權限，其結果應有紀錄留存。

使用者存取權限的審查宜：

- (1) 定期（宜每半年）檢討及評估使用者的存取權限。
- (2) 當人員實施內部調動時，宜重新審查使用者存取權限。
- (3) 定期（宜每半年）檢討特別權限之核發情形。

6. 存取權限之移除或調整 (A.9.2.6)

所有員工及外部使用者對資訊及資訊處理設施之存取權限，一旦其聘用、契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。

移除或改變的存取權限宜：

- (1) 包括實體及邏輯存取、鑰匙、識別證、資訊處理設施及任何可以顯示其為單位成員的文件。
- (2) 在結束聘用或改變職務之前，評估資訊資產及資訊處理設備的存取權宜該被

降低或是移除。

- (3) 若存取權限為多人共用，例如群組帳號，則其權限宜予移除，並通知相關人員不再與離職人員分享該資訊。

(三) 使用者責任 (A.9.3)

1. 秘密鑑別資訊之使用 (A.9.3.1)

於使用秘密鑑別資訊時，應要求使用者遵循組織之實務規定。

施行單位於使用秘密鑑別資訊（如通行碼、加密金鑰或憑證資訊等）時，應要求使用者遵循單位之規定。

使用者宜：

- (1) 維持秘密鑑別資訊的機密性，確保不洩露給包括授權人員的任何一方。
- (2) 避免保留秘密鑑別資訊的紀錄（例如：在紙張、軟體檔案或手持裝置），除非其能被安全地存放，且該存放方式經過核准（例如：密碼庫）。
- (3) 只要秘密鑑別資訊有可能遭受破解的跡象，宜立即更改。
- (4) 選用嚴謹的秘密鑑別資訊，具有足夠長的最短長度（宜至少八碼，英數字混合）。
- (5) 不要與他人共用個人的秘密鑑別資訊。
- (6) 自動登入程序中內含秘密鑑別資訊做為機密鑑別資訊並儲存時，宜確保適當地保護通行碼。
- (7) 公務與非公務使用目的勿使用相同秘密鑑別資訊。

(四) 系統及應用存取控制 (A.9.4)

1. 資訊存取限制 (A.9.4.1)

應根據存取控制政策，限制對資訊及應用系統功能之存取。

依資訊存取規定，配予應用系統的使用者與業務需求相稱的資料存取及應用系統的使用權限。

關於作業與應用系統功能的存取限制措施宜：

- (1) 以選單方式控制使用者僅能使用系統的部份功能。
- (2) 適當的編輯作業手冊，限制使用者僅能獲知或取得授權範圍內的資料及系統存取知識。
- (3) 控制使用者存取系統的能力（例如唯讀、寫入、刪除或執行等功能）。
- (4) 處理敏感性資訊的應用系統，系統輸出的資料，宜僅限於與使用目的有關者，且只能輸出到指定的端末機及位址。

2. 保全登入程序 (A.9.4.2)

當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。

使用者存取電腦系統應經由安全的系統登入程序。

登入程序建議宜具備下列功能：

- (1) 不宜顯示系統及應用系統識別碼，直到成功登入系統。
- (2) 在系統登入程序中，必要時宜顯示"只有被授權的使用者才可存取系統"等警告性的資訊。

- (3) 系統不宜在登入程序中，提供未經授權的使用者登入系統的說明或協助使用者的訊息。
 - (4) 在完成所有的登入資料輸入後，系統才開始查驗登入資訊的正確性；如果登入發生錯誤，系統不宜顯示那一部分資料是正確的，那一部分資料是錯誤的。
 - (5) 宜限制系統登入不成功時可以再嘗試的次數，原則上以三次為原則，系統並宜：
 - a. 記錄系統登入不成功的事件。
 - b. 在使用者嘗試登入系統失敗後，宜強迫必須間隔一段時間之後才能再次登入。
 - c. 宜中斷資料連結作業。
 - (6) 在系統登入被拒絕後，宜立即中斷登入程序，並不得給予任何的協助。
 - (7) 宜限制系統登入程序的最長及最短時間，如果超出時間限制，系統宜自動中斷登入。
 - (8) 在成功登入系統後，宜顯示下列的資訊：
 - a. 上次成功登入系統的日期及時間。
 - b. 上次成功登入系統之後，有無被系統拒絕登入的詳細資料。
 - (9) 登入時不顯示通行碼或以符號隱藏通行碼字元。
 - (10) 網路上不要以明文方式傳遞通行碼。
- 必要時限制使用者在高風險應用系統的連線作業時間。
- 針對連線時間的控制宜：
- (1) 對處理機密及敏感性系統的端末機，限定連線作業及網址連線時間，減少未經授權存取系統的機會。
 - (2) 限定連線時間措施如：
 - a. 只允許在設定的時間內與系統連線。
 - b. 如無特別延長作業時間的需求，限制只能在正常上班時間內進行連線。
 - c. 宜限制連線的網址。
 - d. 限制經過一段時間後必需重新認證。

3. 通行碼管理系統 (A.9.4.3)

通行碼管理系統應為互動式，並應確保嚴謹通行碼。

應以安全有效的使用者通行碼管理系統鑑別使用者身份。

關於通行碼之管理宜：

- (1) 要求必須使用通行碼，明定系統的使用責任。
- (2) 允許使用者自行選擇及更改通行碼；系統宜具備資料輸入錯誤之更正功能。
- (3) 要求使用者必須使用最低長度的密碼（建議使用至少八碼，英數字混合的通行碼）。
- (4) 要求使用者定期（三個月一次）更改通行碼。
- (5) 以更頻繁的次數定期（少於三個月）更新系統存取特別權限的通行碼。
- (6) 使用者自行選擇密碼時，宜在第一次登入系統時強迫使用者更改臨時性密碼。
- (7) 建立使用者密碼的歷史紀錄，最好保存至少一年的使用記錄，避免使用者重複使用相同的密碼。

- (8) 在登入系統程序中，系統不宜顯示使用者的密碼資料。
- (9) 使用者密碼宜與應用系統資料分開存放。
- (10) 使用單向加密演算法儲存使用者密碼。
- (11) 在軟體完成安裝作業後，立即更改廠商預設的使用者密碼。
- (12) 利用工具檢查，或由使用者自行考量通行碼是否安全可靠，參考基準如下：
 - a. 是否使用與日期有關的年、月、日。
 - b. 是否使用公司名稱、識別碼或是其他參考性資訊作為通行碼。
 - c. 是否以使用者識別碼、團體識別碼或其他系統識別碼作為通行碼。
 - d. 是否使用重覆出現兩個字以上的識別字碼作為通行碼。
 - e. 是否使用全數字或全字母作為通行碼。

4. 具特殊權限公用程式之使用 (A.9.4.4)

應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。

關於具有特殊權限之系統公用程式的管理宜：

- (1) 嚴格限制及控管電腦公用程式之使用。
- (2) 制訂公用程式之安控措施，如：
 - a. 設定使用者密碼以保護系統公用程式。
 - b. 將系統公用程式與宜用系統分離。
 - c. 將有權使用系統公用程式的人數限制到最少的數目。
 - d. 建立臨時使用公用程式的授權制度。
 - e. 限制系統公用程式的可用性，例如變更公用程式的使用時間授權規定。
 - f. 記錄系統公用程式的使用情形，備日後考察。
 - g. 訂定系統公用程式的授權規定。

5. 對程式源碼之存取控制 (A.9.4.5)

應限制對程式原始碼之存取。

程式源碼的存取必須採取嚴格的控制措施，避免在存取程式源碼的程序中，造成程式源碼的損毀。

程式源碼的存取宜：

- (1) 應用程式原始碼資料庫宜儘可能不要存放在作業系統的檔案中。
- (2) 應用程式原始碼宜指定專人控管。
- (3) 不宜核發人員無限制存取應用程式原始碼之權限。
- (4) 發展中或是維護中的應用程式，宜與實務作業之程式原始碼資料庫區隔，不宜放置在一起。
- (5) 應用程式原始碼資料庫之更新，以及核發應用程式原始碼供程式設計人員使用，宜由原始碼資料庫管理人員執行。
- (6) 程式目錄清單宜放置在安全的環境中。
- (7) 宜建立所有存取程式原始碼資料庫的稽核軌跡。
- (8) 舊版的原始程式宜妥慎典藏保管，詳細記錄使用的明確時間，並宜保存所有的支援應用程式軟體、作業控制、資料定義及操作程序等資訊。
- (9) 應用程式原始碼資料庫之維護及複製，宜依嚴格的變更控制程序進行。

A.10

密碼學(加密控制)

為保護資料在處理、使用及傳輸時的機密性與完整性，應藉由加密控制措施，確保適當及有效使用軟硬體加密機制，以保護資訊之機密性、鑑別性及/或完整性。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.10 密碼學(加密控制)					A.12
控制目標	A.10.1	密碼式控制措施(加密控制措施)		B.10.1	A.12.3
控制項	A.10.1.1 (I/P)	使用密碼式 控制措施(加 密控制措施) 政策	應發展及實作政策，關於資訊保護之密碼 式控制措施的使用。	B.10.1.2	A.12.3.1
	A.10.1.2 (建議)	金鑰管理	應加以發展及實作政策，關於貫穿其整個 生命週期之密碼金鑰的使用、保護及生命 期。		A.12.3.2

實作指引

(一) 密碼式控制措施(加密控制措施) (A.10.1)

1. 使用密碼式控制措施(加密控制措施)政策 (A.10.1.1)

應發展及實作政策，關於資訊保護之密碼式控制措施(加密控制措施)的使用。

必須發展加密控制措施保護資訊之政策。

資訊保護之密碼式控制措施(加密控制措施)政策宜：

- (1) 對高機密性或敏感性的資訊，宜在傳輸或儲存過程中以加密方法保護。
- (2) 是否使用加密方法，宜進行風險評估，以決定採取何種等級的安全保護措施。
- (3) 使用加密技術時，如資訊專業人力及經驗不足，可借重外界學者專家提供技術諮詢服務。

2. 金鑰管理 (A.10.1.2) (建議)

應加以發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。

以一套公認之標準、流程及方法為金鑰管理系統之基礎，支援加密技術之運用。

- (1) 憑證機構金鑰之產生、儲存、使用、備份、銷毀、更新及復原作業等，宜建立嚴格的安全管理機制。
- (2) 憑證機構資訊系統（含應用系統、密碼模組等）之安全驗證，宜遵照權責主管單位訂定之規範作業，以確保其安全性。
- (3) 憑證機構使用之數位簽章或加密金鑰長度，宜依權責主管單位建議之參考值及視系統的安全需求設定。

A.11

實體及環境安全

為保護資訊處理設施以及所在位置的安全，除環境的管制保護措施外，軟硬體防護措施也需徹底實行，以有效降低資訊安全事件發生的機率。這部份為各項資訊資產保護的基礎，再嚴密的處理程序及規範，缺少實體及環境的安全落實，仍舊無法達到保護的目的，因此，此部分管理措施的落實與否，實為各項進一步控管制度的基石。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.11 實體及環境安全					A.9 A11
控制目標	A11.1	安全區域		B.10.1	A.9.1
控制項	A11.1.1 (I/P)	實體安全周界	應定義及使用安全周界，以保護收容敏感或重要資訊及資訊處理設施之區域。	B.10.1.1	A.9.1.1
	A.11.1.2 (I/P)	實體進入控制措施	保全區域應藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。	B.10.1.1	A.9.1.2
	A.11.1.3	保全之辦公室、房間及設施	應設計資訊處理設施所在區域之實體安全並施行之。		A9.1.3
	A.11.1.4	防範外部及環境威脅	應設計並施行實體保護，以防範天然災害、惡意攻擊或事故。		A.9.1.3
	A.11.1.5	於保全區域內工作	應設計及施行資訊處理設施所在區域內工作之程序。		A.9.1.3
	A.11.1.6 (建議)	交付及裝卸區	對諸如交付及裝卸區及其他未經授權人員可進入作業場所之進出點，應加以控制；若可能，應與資訊處理設施隔離，以避免未經授權之存取。		
控制目標	A.11.2	設備		B.8.1 B.10.1	A.9.2 A.11.2
控制項	A.11.2.1 (I/P)	設備安置及保護	應安置並保護設備，以降低來自環境之威脅及危害造成的風險，以及未經授權存取之機會。	B.10.1.1	A.9.2.1
	A.11.2.2	支援之公用服務事業	應保護設備免於電源失效，及因其他支援之公用服務事業失效，所導致之中斷。		A.9.2.2
	A.11.2.3	佈纜安全	應保護通訊纜線及資訊處理設備之電源，降低受竊聽或破壞的可能損失。		A.9.2.3

A.11.2.4 (I/P)	設備維護	應正確維護設備，以確保其持續之可用性及完整性。	B.10.1.1	A.9.2.4
A.11.2.5 (I/P)	財產之攜出	未經事前授權，不得將設備、資訊或軟體帶出場域外。	B.10.1.1	A.9.2.7
A.11.2.6 (建議)	場所外設備及資產的安全	安全應適用於場域外資產，並將於施行單位場所外工作之不同風險納入考量。		
A.11.2.7 (I/P)	設備汰除或再使用之保全	含有儲存媒體之所有設備組件，於汰除前或再使用前應加以查證，以確保任何敏感性資料及有版權之軟體已被移除或安全地覆寫。	B.8.1.1 B.10.1.1	A.9.2.5
A.11.2.8 (建議)	無人看管之使用者設備	使用者應確保無人看管之設備具備適切保護。		
A.11.2.9	桌面淨空及螢幕淨空政策	對紙本及可移除式儲存媒體應採用桌面淨空政策，且對資訊處理設施應採用螢幕淨空政策。		A.11.2.1

實作指引

(一) 區域之安全 (A.11.1)

1. 實體安全周界 (A11.1.1)

應定義及使用安全周界，以保護收容敏感或重要資訊及資訊處理設施之區域。

施行單位應採用適當防護措施保障資訊處理設施所在區域（機房設備、人員辦公區域）的安全。

資訊處理設施所在區域之安全宜：

- (1) 以事前劃定的各項週邊設施為基礎，設置必要的管制，達成安全控管的目的。
- (2) 依資訊資產及服務系統的價值及安全風險，決定實體保護的程度。

2. 實體進入控制措施 (A11.1.2)

保全區域應藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。

施行單位應實施控制措施，確保只有授權人員可以進出安全區域。

關於人員進出安全區域的管制，宜確保：

- (1) 有適當的進出管制保護措施，使無授權的人員不得進入。
- (2) 來訪人員進入管制區宜予適當管制，並紀錄進出時間；來訪人員只有在特定的目的或是被授權情形下，才能進入管制區。
- (3) 員工離職後，宜立即撤銷進入管制區的權利。

3. 保全之辦公室、房間及設施 (A.11.1.3)

應設計資訊處理設施所在區域之實體安全並施行之。

為確保區域之安全性，採取的控制措施與指引宜包含：

- (1) 資訊處理設施宜遠離大眾或是公共運輸系統可直接進出的地點。
- (2) 資訊處理設施宜儘可能不要有過於明顯的標示；在建築物內部及外部的說

明，儘可能不要有過於明顯的指引或配置說明。

(3) 顯示機密資訊處理設施的地點或人員通訊錄，不宜讓未經授權人員取得。

4. 防範外部及環境威脅 (A.11.1.4)

應設計並施行實體保護，以防範天然災害、惡意攻擊或事故。

為確保區域之安全性，採取的控制措施與指引宜包含：

- (1) 資訊處理設施所在區域宜設立良好的實體安全措施，考量各種自然及人為災害的可能性，考量鄰近空間的可能安全威脅。
- (2) 危險性及易燃性物品宜遠離資訊處理設施的安全地點；非有必要，電腦相關文具設備不宜存放在電腦機房內。
- (3) 備援作業用的設備及備援媒體，宜存放在安全距離以外的地點。
- (4) 宜安裝適當的安全偵測及防制設備，各項安全設備宜依廠商的使用說明書定期（宜每半年）檢查，並針對相關員工進行適當的安全設備使用訓練。

5. 於保全區域內工作 (A.11.1.5)

應設計及施行資訊處理設施所在區域內工作之程序。

為確保於保全區域工作安全，所採取的控制措施宜包含：

- (1) 僅讓授權員工知道該保全區域或在區域內進行的活動。
- (2) 區域內宜避免進行未受監督之工作。
- (3) 無人的保全區域，加以上鎖並定時檢查。
- (4) 非經授權不宜允許進行拍照、錄影及其他紀錄活動。

6. 交付及裝卸區 (A.11.1.6) (建議)

對諸如交付及裝卸區及其他未經授權人員可進入作業場所之進出點，應加以控制；若可能，應與資訊處理設施隔離，以避免未經授權之存取。

宜考慮下列事項：

- (1) 宜限制只有經過識別並被授權的人員才能從建物外面進出交付及裝卸區。
- (2) 交付及裝卸區宜設計讓遞送人員不需要進入建築物的其他位置即可裝卸貨物。
- (3) 宜在確定交付及裝卸區的對外大門安全時，才能開啟對內大門。
- (4) 進入物品從交付及裝卸區移動前，宜進行檢查是否有爆裂物、化學品或其他危害物質。
- (5) 宜在入口處依資產管理程序對進入貨物進行登記。
- (6) 如果可行，進貨及出貨宜在實體上隔離。
- (7) 宜檢視進入物品是否有在途中開啟之證據。若發現已被開啟，宜立即通報安全人員

(二) 設備 (A.11.2)

1. 設備安置及保護 (A.11.2.1)

應安置並保護設備，以降低來自環境之威脅及危害造成的風險，以及未經授權存取之機會。

施行單位應安置或保護設備，降低環境之威脅、災害以及未授權存取所造成的可能損失。

設備安置須遵循下列之原則：

- (1) 設備宜盡量安置在可減少人員不必要經常進出的工作地點。處理機密性及敏感性資料的工作站，宜放置在員工可以注意及照顧的地方。
- (2) 需要特別保護的設備，宜考量與一般設備區隔，安置在獨立的區域。
- (3) 宜檢查及評估火災、煙、火、灰塵、震動、化學效應、電力供應、電磁輻射等可能的風險。
- (4) 電腦作業區宜禁止抽菸及飲用食物。

2. 支援之公用服務事業 (A.11.2.2)

應保護設備免於電源失效，及因其他支援之公用服務事業失效，所導致之中斷。施行單位應保護資訊處理設備，降低電力、電信、供水或空調等公用服務失效或異常所造成中斷或影響的機會。

有關於資訊處理設備所使用的公用服務宜：

- (1) 防止公用服務不正常導致的傷害；各項公用服務供應宜依據製造商提供的規格設置。
- (2) 考量定期對各公用服務容量規劃與評估，並考量建立警報系統偵測故障。
- (3) 宜考量安置預備電源，並考量使用不斷電系統；不斷電系統宜依據製造廠商的建議，定期（宜每半年）進行測試。
- (4) 宜謹慎使用電源延長線，以免電力無法負荷導致火災等安全情事。
- (5) 將公用服務失效之後的應變措施納入資訊安全事件緊急處理應變計畫。

3. 佈纜安全 (A.11.2.3)

應保護傳送資料或支援資訊服務之電源及電信佈纜，以防範竊聽、干擾或損害。施行單位應保護通訊纜線及資訊處理設備之電源，降低受竊聽或破壞的可能損失。電力及通信用的電纜線宜予適當的保護，其保護原則如下：

- (1) 連接資訊設施的電源及通信線路，宜盡可能地下化；如不能地下化，宜視需求採取足夠的替代保護措施。
- (2) 宜考量保護網路通信線路的措施，以防止遭截取或是受到破壞。
- (3) 對於特別敏感性或是特別重要的系統，宜採取額外強化的安全措施。
- (4) 清楚的識別電纜線與設備標示，以及文件化的清單，減少錯誤發生的可能性。

4. 設備維護 (A.11.2.4)

應正確維護設備，以確保其持續之可用性及完整性。

資訊處理設備應予以適當的維護，確保其持續運作。

為確保設備的完整性及可持續使用宜：

- (1) 宜依據廠商建議的維修服務週期及說明，進行設備維護。
- (2) 設備的維護只能由授權的維護人員執行。
- (3) 宜將所有的錯誤或是懷疑的錯誤予以記載。
- (4) 當設備送場外維修時，宜採取適當的控制措施。（例如：將內部敏感性的資料

移清除)

5. 財產之攜出 (A.11.2.5)

未經事前授權，不得將設備、資訊或軟體帶出場域外。

施行單位所屬之設備、資訊或軟體未經授權禁止移動。

關於財產移轉之安全管理宜：

- (1) 在沒有管理人員授權的情況下，設備、資訊或是軟體不宜被帶離所屬區域。
- (2) 宜紀錄攜出與歸還的人員與時間，並查證是否逾時未歸還。

6. 場所外設備及資產的安全 (A.11.2.6) (建議)

安全應適用於場域外資產，並將於施行單位場所外工作之不同風險納入考量。

在施行單位場所之外使用任何資訊儲存及處理設備宜經過管理階層授權。此控制措施適用於施行單位擁有之設備及代表施行單位使用之私有設備。

針對場外設備的保護，宜考慮下列事項：

- (1) 攜出場所外之設備和媒體，留置於公共場所時不宜無人看管。
- (2) 如因在家、遠距工作及臨時置放場地等，於場外位置使用設備時，宜視需要採用適當控制措施，例如：可上鎖的檔案櫃、桌面淨空政策、電腦存取控制措施及與辦公室之遠距通信安全。
- (3) 場外設備在不同個人或外部團體間轉移時，宜準備設備保管日誌，其中至少包括設備負責人員之姓名及單位。

7. 設備汰除或再使用之保全 (A.11.2.7)

含有儲存媒體之所有設備組件，於汰除前或再使用前應加以查證，以確保任何敏感性資料及有版權之軟體已被移除或安全地覆寫。

資訊處理設備在報廢或再使用的過程中，應避免內存資料的外洩，進行必要之清除動作。

有關於設備處理之安全措施，需在儲存媒體的設備項目（例如硬碟）處理前詳加檢查，確保任何機密性、敏感性的資料及有版權的軟體已經被移除。

8. 無人看管之使用者設備 (A.11.2.8) (建議)

使用者應確保無人看管之設備具備適切保護。

所有使用者宜認知保護無人看管使用者設備的安全要求與程序，以及他們實作這類保護措施的責任，建議使用者宜：

- (1) 使用完畢後宜有適切的鎖定機制，例如以通行碼保護的螢幕保護程式。
- (2) 使用完畢後登出應用系統或網路服務。
- (3) 電腦或行動裝置不用時，使用鑰匙上鎖或同等控制措施，例如通行碼存取以防止未經授權的使用。

9. 桌面淨空及螢幕淨空政策 (A.11.2.9)

對紙本及可移除式儲存媒體應採用桌面淨空政策，且對資訊處理設施應採用螢幕淨空政策。

應考量採用辦公桌面與螢幕的淨空政策，以減少文件及儲存媒體等在正常的辦公時間之外遭未被授權的人員取用、遺失、竄改或是被破壞的機會。

考量的事項如下：

- (1) 文件及儲存媒體在不使用或是不上班時，宜存放在櫃子內。
- (2) 機關的機密性及敏感性資訊，不使用或下班時應該上鎖，最好是放在防火櫃之內。
- (3) 個人電腦及電腦終端機不再使用時，宜以上鎖、通行碼或是其他控制措施保護。
- (4) 宜該考量保護一般郵件進出的地點，以及無人看管的傳真機。
- (5) 當列印敏感性或分類機密資訊後，宜立即從印表機上取走。

A.12

運作安全

為確保正確以及安全的操作資訊處理設施，降低各種可能的風險與損害，維護資訊處理與通訊服務之完整性及可用性，必須設立通訊與作業安全之管理措施。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.12 運作安全					A.10 A.12 A.15
控制目標	A.12.1	運作程序及責任		B.10.1	A.10.1 A.10.3
控制項	A.12.1.1	文件化運作程序	運作程序應加以文件化，並使所有需要之使用者均可取得。		A.10.1.1
	A.12.1.2 (I/P)	變更管理	應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更。	B.10.1.1	A.10.1.2
	A.12.1.3	容量管理	各項資源之使用應受監視及調適，並對未來容量要求預作規劃，以確保所要求之系統效能。		A.10.3.1
	A.12.1.4	開發、測試及運作環境之區隔	應區隔開發、測試及運作之環境，以降低對運作環境未經授權存取或變更的風險。		A.10.1.4 A.11.5.2
控制目標	A.12.2	防範惡意軟體		B.10.1	A.10.4
控制項	A.12.2.1 (I/P)	防範惡意軟體之控制措施	應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。	B.10.1.1	A.10.4.1
控制目標	A.12.3	備份		B.10.1	A.10.5
控制項	A.12.3.1 (I/P)	資訊備份	應依議定之備份政策，定期取得資訊、軟體及系統的影像檔備份複本，並測試之。	B.10.1.1	A.10.5.1
控制目標	A.12.4	存錄及監視		B.10.1 B.10.2	A.10.9
控制項	A.12.4.1 (I/P)	事件存錄	應產生、保存並定期審查記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。	B.10.2.1	A.10.9.1 A.10.9.2 A.10.9.5
	A.12.4.2 (I/P)	日誌資訊之保護	應防範存錄設施及日誌資訊遭竄改及未經授權存取。	B.10.2.1	A.10.9.3

	A.12.4.3 (I/P)	管 理 者 及 操 作 者 日 誌	應存錄系統管理者及操作者之活動，且應保護及定期審查該日誌。	B.10.2.1	A.10.9.4
	A.12.4.4	鐘訊同步	組織或安全領域內所有相關資訊處理系統之鐘訊，應與單一參考時間源同步。		A.10.9.6
控制目標	A.12.5	運作中軟體之控制			A.12.4
控制項	A.12.5.1	運 作 中 系 統 之 軟 體 安 裝	應實作各項程序，以控制對運作中系統之軟體安裝。		A.12.4.1
控制目標	A.12.6	技術脆弱性管理			A.12.6
控制項	A.12.6.1	技 術 脆 弱 性 管 理	應及時取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。		A.12.6.1
	A.12.6.2 (建議)	對 軟 體 安 裝 之 限 制	應建立並實作使用者安裝軟體之管控規則。		
控制目標	A.12.7	資訊系統稽核考量			A.15.3
控制項	A.12.7.1	資 訊 系 統 稽 核 控 制 措 施	應仔細規劃並議定，涉及運作中系統之稽核要求事項及活動，以使營運過程中斷降至最低。		A.15.3.1

實作指引

(一) 運作程序及責任 (A.12.1)

1. 文件化運作程序 (A.12.1.1)

運作程序應加以文件化，並使所有需要之使用者均可取得。

安全政策所規定之作業程序，應文件化並定期（宜每半年）維護。

關於作業程序之訂定宜：

- (1) 制訂電腦系統作業程序，並以書面或其他方式載明，確保員工正確及安全地操作及使用電腦，並以此作為系統發展、維護及測試作業的依據。
- (2) 載明每項執行電腦作業程序的詳細規定：
 - a. 如何正確地處理資料檔案。
 - b. 如何備份。
 - c. 電腦作業時程的需求，包括與其他系統的相互關係、作業啟動的最早時間及作業結束的最晚時間。
 - d. 處理電腦當機及發生作業錯誤之規定，及其他電腦作業之限制事項。
 - e. 遭遇非預期電腦作業技術問題時，如何與支援人員聯繫之規定。
 - f. 資料輸出處理的特別規定，例如使用特別的文具，或是對機密資料輸出之管理、電腦當機或作業錯誤時所輸出資訊之安全處理規定等。
 - g. 電腦當機重新啟動及回復正常作業之程序。
 - h. 電腦及網路之日常管理作業，例如開關機程序、資料備援、設備維護、電腦機房之安全管理；作業程序宜視為正式文件，作業程序的更改必須

經權責單位核准。

i. 電腦稽核軌跡及系統記錄資訊之管理。

2. 變更管理 (A.12.1.2)

應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更。

資訊處理設施、系統之變更，應進行管制。

關於資訊處理設施、系統之變更宜：

(1) 建立控制及管理機制，以免造成系統安全上的漏洞。

(2) 執行作業變更之管理：

a. 界定及記錄重大變更的事項。

b. 作業變更的規劃與測試。

c. 評估作業變更之可能衝擊。

d. 建立作業變更之程序。

e. 與相關人員溝通作業變更之細節。

f. 作業變更不能順利執行時之回復計畫，或失敗變更回復之作業程序及責任。

3. 容量管理 (A.12.1.3)

各項資源之使用應受監視及調適，並對未來容量要求預作規劃，以確保所要求之系統效能。

施行單位應適時預估系統容量需求，確保有充分處理資料與儲存的空間。

系統作業容量之規劃宜包含：

(1) 宜隨時注意及觀察分析系統的作業容量，並進行需求預測，以避免容量不足而導致電腦當機。

(2) 宜預留預算及採購行政作業的前置時間，以利進行前瞻性規劃，並及時取得必要的作業容量。

(3) 系統管理人員，宜隨時注意及觀察分析系統資源使用狀況，包括處理器、主儲存裝置、檔案儲存、印表機及其他輸出設備和通信系統之使用狀況；主管人員宜隨時注意上述設備的使用趨勢，尤其注意系統在業務處理及資訊管理上的應用情形。

(4) 宜隨時掌握及利用電腦與網路系統容量使用狀況的資訊，分析與找出可能危及系統安全的瓶頸，預作補救措施之規劃。

4. 開發、測試及運作環境之區隔 (A.12.1.4)

應區隔開發、測試及運作之環境，以降低對運作環境未經授權存取或變更的風險。

開發或測試用之設備、軟體轉換至作業狀態，應制定規則分隔開來，並加以文件化。

系統發展及測試作業之分散宜：

(1) 將系統發展及系統實際作業的設施分散，降低可能的安全風險，以減少作業軟體或資料遭意外竄改，或是遭未經授權的存取。

(2) 系統發展及系統實際作業之分散，宜考量下列措施：

- a. 軟體從開發轉移至實作狀態的規則，宜予界定並文件化。
- b. 系統發展及實際作業的軟體，宜盡可能在不同的處理器上作業，或是在不同的目錄或領域（Domain）下作業。
- c. 系統發展及測試作業宜盡可能分開。
- d. 編輯器及其他公用程式不再使用時，不宜與作業系統共同存放在一起。

（二）防範惡意軟體（A.12.2）

1. 電腦病毒及惡意軟體之控制（A.12.2.1）

應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。施行單位應進行防備電腦病毒與惡意軟體之偵測及預防的控制措施，以及使用者認知程序。

關於惡意程式的控制宜：

- (1) 採取必要的事前預防及保護措施，防治及偵測各種可能的惡意程式侵入。
- (2) 促使員工正確認知惡意軟體的威脅，提升員工的資訊安全警覺，健全系統存取控制機制。
- (3) 惡意程式的防範宜考量下列原則：
 - a. 建立軟體管理政策，規定各單位及使用者宜遵守軟體授權規定，禁止使用未取得授權的軟體。
 - b. 選擇信譽良好、功能健全的防制軟體，並依下列原則使用：
 - 防制軟體宜定期（宜每周）更新。
 - 使用防制軟體事前掃描電腦系統及資料儲存媒體，偵測是否受感染。
 - 視需求安裝可偵測軟體是否遭更改的工具軟體，並偵測執行碼是否遭變更。
 - 宜充分了解防制軟體的特性及功能。
 - 定期（宜每半年）檢查軟體及重要系統資料內容，如發現有偽造的檔案或是未經授權的修正事項，宜立即調查找出原因。
 - 對來路不明及內容不確定的儲存媒體，宜在使用前詳加檢查。
 - 宜建立防制攻擊事件及回復作業的管理程序，並訂定相關人員責任。
 - 宜建立妥適的業務永續運作計畫，將必要的資料及軟體加以備份，並於事前訂定回復作業計畫。

（三）備份（A.12.3）

1. 資訊備份（A.12.3.1）

應依議定之備份政策，定期取得資訊、軟體及系統的影像檔備份複本，並測試之。重要資訊、軟體及系統應定期（至少每周）或依據須備份單位所申請備份周期進行備份。

關於資料備份宜：

- (1) 準備適當及足夠的備援設施，定期（宜每半年）執行必要的資料及軟體備份及備援作業，以便在發生災害或是儲存媒體失效時，可迅速回復正常作業。
- (2) 系統資料備份及備援作業，宜符合單位業務永續運作之需求。
- (3) 資料備份作業的原則為：

- a. 正確及完整的備份資料，除存放在主要的作業場所外，宜另存放於安全距離的場所，防止災害發生時可能帶來的傷害。
- b. 重要資料的備份，建議以維持三代以上為原則。
- c. 備份資料宜有適當的實體及環境保護。
- d. 宜定期（宜每半年）測試備份資料，確保其可用性。
- e. 資料的保存時間以及永久保存的需求，宜由資料擁有者研提。
- f. 宜定期（宜每半年）檢查測試回復程序，確保回復程序能在指定時間內完成復原作業程序。
- g. 重要機密的資料備份，宜使用加密方式來保護。

(四) 存錄及監視 (A.12.4)

1. 事件存錄 (A.12.4.1)

應產生、保存並定期審查記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。

應結合臺灣學術網路資安監控系統(北區 SOC、南區 SOC、Mini-SOC、TACERT)或教育部資安監控系統機制，進行資安預警情資、事件通報及應變處置。

建立及製作例外事件及資訊安全事項的稽核軌跡，並明定合理保存期限，以作為日後調查及監督之用。

系統稽核軌跡宜包括下列事項：

- (1) 使用者識別碼。
- (2) 登入及登出系統之日期及時間。
- (3) 儘可能記錄終端機的識別資料或其位址。
- (4) 存取系統成功與失敗情形的紀錄。
- (5) 存取資料與其他資源的成功與失敗情形的紀錄。
- (6) 更改系統設定。
- (7) 特別權限的使用。
- (8) 系統公用程式與應用程式的使用。
- (9) 檔案存取及存取類型
- (10) 網址及通信協定
- (11) 存取權限提昇警報
- (12) 保護系統的執行與撤銷（例如防毒系統及入侵偵測系統）

系統發生錯誤之事項時，宜予以忠實的記錄，並進行適當的處理程序。

其中宜包含：

- (1) 系統發生作業錯誤時，宜迅速報告權責主管人員，並採取必要的更正行動。
- (2) 使用者對電腦及通信系統作業錯誤的報告，宜正式記錄下來，以供日後查考。
- (3) 宜建立明確的系統作業錯誤報告程序及作業規定，要項如下：
 - a. 宜檢查錯誤情形的紀錄，確保系統作業錯誤已經改正。
 - b. 宜檢查更正作業是否妥適，確保更正作業依正當的授權程序辦理，且未破壞系統原有的安控措施。

2. 日誌資訊之保護 (A.12.4.2)

應防範存錄設施及日誌資訊遭竄改及未經授權存取。

應保護未授權的變更或存取，以及防止記錄設備操作發生問題。

記錄保護之內容宜包括：

- (1) 已記錄之記錄型態的改變。
- (2) 記錄檔被修改或刪除。
- (3) 超過媒體記錄容量，所產生的錯誤。

3. 管理者及操作者日誌 (A.12.4.3)

應存錄系統管理者及操作者之活動，且應保護及定期審查該日誌。

應忠實記錄系統管理者與作業人員之相關操作記錄。

操作記錄宜包含：

- (1) 宜忠實記錄系統啟動及結束作業時間、系統錯誤、更正作業及建立日誌條目的人員或程序等事項。
- (2) 作業人員的系統作業紀錄，宜定期（宜每半年）交由客觀的第三者檢查，以確認其是否符合機關訂定的作業程序。

4. 鐘訊同步 (A.12.4.4)

組織或安全領域內所有相關資訊處理系統之鐘訊，應與單一參考時間源同步。

應定義使用的標準參考時間，以及與該標準參考時間之內部同步作業設定方式。

對未能設定時間同步之設備，應以人工方式定期（宜每月）依據同一時間源之資訊進行時間校正作業。對於設定同步作業之設備亦應定期（宜每季）確認系統時間同步機制的有效性，以維持系統稽核紀錄的正確性及可信度，作為事後法律上或是紀律處理上的重要依據。

連接至國家標準時間的時間伺服器，可以做為稽核存錄系統主要校時依據，網路時間協定也用做為所有伺服器與主要鐘訊同步之機制。

(五) 運作中軟體之控制 (A.12.5)

1. 運作中系統之軟體安裝 (A.12.5.1)

應實作各項程序，以控制對運作中系統之軟體安裝。

需建立作業系統各個軟體實施的管制程序，避免軟體影響作業系統之完整。

作業軟體之控管宜：

- (1) 嚴格執行下列控制程序，減少在作業系統上執行應用軟體可能危害作業系統的風險：
 - a. 作業用的應用程式更新作業，宜限定只能由授權的管理人員才可執行。
 - b. 只將執行碼存放在作業系統內。
 - c. 執行碼尚未測試成功且未被使用者接受前，不宜在作業系統執行。
 - d. 設定檔控制系統可控管所有實作軟體和系統文件。
 - e. 在變更實作前宜建立回寫策略（rollback）。
 - f. 宜建立應用程式的更新稽核紀錄。
 - g. 舊有軟體的版本宜被儲存，包括所有需要的資訊和參數、程序、設定詳

細資料、及支援軟體，與資料保留的時間相同。

(六) 技術脆弱性管理 (A.12.6)

1. 技術脆弱性管理 (A.12.6.1)

應及時取得關於使用中之資訊系統的技術脆弱性資訊、並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。

應依據「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」或相關資安規定中各級單位安全性檢測要求進行弱點偵測及滲透測試。

應及時取得有關針對系統弱點的資訊，並評估該弱點暴露的程度及所造成的可能危機。

系統弱點控制包括：

- (1) 宜明定管理系統弱點的角色及責任，包括弱點監控、弱點風險評估、修補弱點、資產追蹤及任何需要協調的責任。
- (2) 針對潛在的系統弱點的通報時間宜明確定義。
- (3) 一旦確認潛在的系統弱點，宜採取相關措施。(例如修補漏洞)
- (4) 若使用修補檔，宜比較使用修補檔所產生的風險(例如當機)，與未安裝修補檔所產生的風險。修補檔宜在安裝前經過測試。若無修補檔，則宜考慮其它安控措施如：
 - a. 關掉服務或與此弱點有關的功能。
 - b. 調整或增加存取控制，例如增加防火牆。
 - c. 提高使用者之認知(例如針對該弱點特性，提醒使用者應注意事項)
 - d. 相關的稽核記錄宜保持，以便後續使用。
 - e. 高風險系統優先考量前述安控措施。

2. 對軟體安裝之限制 (A.12.6.2) (建議)

應建立並實作使用者安裝軟體之管控規則。

宜採用給予最少軟體安裝之特殊權限原則。

施行單位宜識別允許之軟體安裝型式(例如：現有軟體之更新及安全修補)以及禁止之軟體安裝型式(例如：僅限個人使用之軟體及已知或懷疑具有潛在惡意行為之軟體)。並在考量使用者之角色後授與上述安裝軟體權限。

(七) 系統稽核的考量 (A.12.7)

1. 資訊系統稽核控制措施 (A.12.7.1)

應仔細規劃並議定，涉及運作中系統之稽核要求事項及活動，以使營運過程中斷降至最低。

為避免作業系統稽核造成系統中斷的危險，應進行審慎、一致的規劃；必要時可向外部專家顧問尋求協助。

A.13

通訊安全

為確保對網路及其支援之資訊處理設施中資訊之保護，降低各種可能的風險與損害，維護資訊處理與通訊服務之完整性及可用性，必須設立通安全之管理措施。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.13 通訊安全					A.6 A.10 A.11
控制目標	A.13.1	網路安全管理			A.10.6 A.11.3
控制項	A.13.1.1	網路控制措施	應實施網路控制措施，維護網路安全。		A.10.6.1 A.11.3.2 A.11.3.3 A.11.3.4 A.11.3.5 A.11.3.6
	A.13.1.2	網路服務之安全	應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外所提供。		A.10.6.2
	A.13.1.3	網路之區隔	應區隔各群組之資訊服務、使用者及資訊系統使用的網路。		A.11.3.4
控制目標	A.13.2	資訊傳送		B.6.2 B.10 B.11	A.6.1 A.10.8
控制項	A.13.2.1 (I/P)	資訊傳送政策及程序	應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。	B.6.2.1 B.6.2.2 B.10.1.1 B.11.1.1	A.10.8.1
	A.13.2.2 (I/P)	資訊傳送協議	協議應闡明組織與外部各方間營運資訊之安全傳送。	B.6.2.1 B.10.1.1 B.11.1.1	A.10.8.1
	A.13.2.3 (I/P)	電子傳訊	應適切保護電子傳訊時所涉及之資訊。	B.6.2.1 B.6.2.2 B.10.1.1 B.11.1.1	A.10.8.2

	A.13.2.4 (I/P)	機密性或保 密協議	應識別、定期審查及文件化，以反映施行 單位對資訊保護之需要的機密性或保密 協議之要求事項。		A.6.1.3
--	-------------------	--------------	---	--	---------

實作指引

(一) 通訊安全 (A.13.1)

1. 網路控制措施 (A.13.1.1)

應管理及控制網路，以保護資訊系統及應用。

應實施網路控制措施，維護網路安全。

應依據「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」或相關資安規定中各級單位縱深防護要求進行規劃。

網路安全規劃與管理，宜包含：

(1) 網路安全規劃：

- 建立電腦網路系統的安全控管機制，確保網路傳輸資料的安全，保護連線作業及未經授權的系統存取。
- 加強跨單位間電腦網路系統之網路安全管理。
- 利用公眾網路或無線網路傳送敏感性資料，宜採取特別的安全保護措施，保護資料的完整性及機密性，並保護連線作業系統之可用性。

(2) 網路安全管理：

- 盡可能將電腦作業及網路作業責任分開。
- 建立管理遠端設備的責任及程序。
- 實施適當的記錄與監控。
- 密切協調電腦及網路管理作業，以便發揮網路系統最大的服務功能，確保其在跨單位的基礎架構上運作。

2. 網路服務之安全 (A.13.1.2)

應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外所提供。

使用公用或私用網路，應評估網路服務提供者之安全措施是否足夠，並提供明確的安全措施說明，另應考量使用該項網路對維持機關資料傳輸機密性、資料完整性及可用性等各種安全影響。

網路服務安全宜包括：

- (1) 提供連線服務、私有網路服務、加值網路及受管理網路的安全解決方案，例如防火牆及入侵偵測系統。
- (2) 若網路服務是委外提供，宜確認廠商提供約定服務的安全管理能力。

3. 網路分隔 (A.13.1.3)

應區隔各群組之資訊服務、使用者及資訊系統使用的網路。

網路應視需求控制措施，將資訊服務、使用者及各資訊系統區隔。

網路區隔之控管宜：

- (1) 考量將不同使用者及電腦系統分開成不同的領域，降低網路系統規模過於龐

大造成的可能安全風險。

- (2) 不同領域的網路系統，每一領域宜以特定的安全設施加以保護；例如設置防火牆及網路閘道隔開不同的網路系統。
- (3) 依據施行單位訂定的系統存取控制政策及需求，決定是否將規模龐大的網路分成數個不同領域的網路系統，並考量成本因素及使用網路路由器與閘道技術對作業效率之影響。
- (4) 考量無線網路的區隔。

(二) 資訊傳送 (A.13.2)

1. 資訊傳送政策及程序 (A.13.2.1)

應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。

使用通訊設施作資訊傳送時需遵循的程序和控制措施，宜考量下列項目：

- (1) 保護所傳送之資訊，以防範截取、複製、修改、誤選路 (mis-routing) 及破壞的程序。
- (2) 偵測與防範可能藉由電子通信傳輸的惡意軟體之程序。
- (3) 保護以附件形式傳輸之敏感性電子資訊之程序。
- (4) 通信設施之使用規則。
- (5) 員工、承包者及任何其他使用者對施行單位的責任，例如：禁止毀謗、騷擾、假冒、轉寄連鎖信及未經授權的購買等。
- (6) 密碼技術的使用，例如：用以保護資訊之機密性、完整性及鑑別性。
- (7) 所有公務來往書信 (包括訊息) 的保留和作廢規則，須符合相關法律與法規。
- (8) 與通信設施 (例如：電子郵件自動轉寄到外部的郵件地址) 相關之使用規則。
- (9) 採取適當的預防措施，避免洩露機密資訊。
- (10) 不在答錄機或傳真機上遺留含敏感資訊的訊息。

2. 資訊傳送協議 (A.13.2.2)

協議應闡明組織與外部各方間營運資訊之安全傳送。

單位間交換資訊與軟體的行為 (具機密性或敏感性內容) 應有安全保護措施以及協議規範，必要時制定正式合約。

單位間資訊與軟體交換行為規範，包含：

- (1) 單位間進行資料或軟體交換，宜訂定正式的協定，將機密性及敏感性資料的安全保護事項及責任列入協定。
- (2) 單位間資料及軟體交換的安全協定內容，宜考量：
 - a. 控制資料及軟體傳送、送達收受的管理責任及作業程序。
 - b. 資料、軟體包裝及傳送的最低技術標準。
 - c. 識別資料及確定軟體傳送者身分的標準。
 - d. 資料遺失的責任及義務。
 - e. 資料及軟體的所有權、資料保護的責任、軟體的智慧財產權規定等。
 - f. 紀錄及讀取資料及軟體的技術標準。
 - g. 保護機密或敏感性資料的安全措施。(如使用加密技術)

h. 確保可追蹤和不可否認性的作業程序。

3. 電子傳訊 (A.13.2.3)

應適切保護電子傳訊時所涉及之資訊。

應制定電子傳訊(如電子郵件、即時通訊或 FTP 資料傳檔等)使用政策，並實施控制措施降低安全風險。

電子傳訊之資訊安全宜考量：

- (1) 以符合資訊安全等級的訊息保護方式來避免避免遭受未經授權存取、變更或阻絕服務。
- (2) 確保訊息的正確定址與傳送。
- (3) 服務的可靠度與可用性。
- (4) 法律考量，例如要求電子簽章。
- (5) 使用諸如即時傳訊、社群網路或檔案共享等外部公共服務之前，先取得核准。
- (6) 更強等級的使用者鑑別方式以控制來自公眾網路的存取。

有關電子郵件安全管控，包括：

- (7) 郵件伺服器應進行防護設定，或利用電子郵件安全管理系統的防護措施。
- (8) 依施行單位安全政策及規定，明訂電子郵件使用規定。
- (9) 建立電子郵件安全管理機制，降低電子郵件可能帶來的業務或安全上的風險。
- (10) 電子郵件安全管理規定，應評估下列事項：
 - a. 訊息遭未經授權的擷取及竄改的安全弱點。(較適用於第一群)
 - b. 發生資料錯誤誤投的安全弱點。(較適用於第一群)
 - c. 電子郵件服務的可靠性及可用性。(較適用於第一群)
 - d. 電子郵件法律效力的考量，例如來源證明、送達、發送及收受等。(較適用於第一群)
 - e. 使用者從遠端存取電子郵件帳號之安全控管。
- (11) 密等以上的公文及資料，不得以電子郵件傳送；敏感性資訊如有電子傳送之必要，得經加密處理後傳送。
- (12) 必要時以電子簽章方式簽發電子郵件，達到身份辨識及不可否認的目的。
- (13) 電子郵件附加檔案，應事前檢視內容有無錯誤後方可傳送。
- (14) 察覺有人員違反電子郵件管理政策，須適時規勸並指導正確的使用方式。

4. 機密性或保密協議 (A.13.2.4)

應識別、定期審查及文件化，以反映施行單位對資訊保護之需要的機密性或保密協議之要求事項。

機密性或保密協議宜使用具有法定強制效力之用語闡明保護機密資訊的要求。

機密性或保密協議適用於外部團體或施行單位之員工。

為識別機密性或保密協議的要求，宜考量下列要件：

- (1) 將受保護之資訊（例如：機密性資訊）。
- (2) 協議預訂持續的期間，包括機密性可能需要無限期維持的情況。
- (3) 協議終止時所需的行動。
- (4) 簽署者的責任與行動，以避免未經授權的資訊揭露。

- (5) 資訊、交易秘密與智慧財產的擁有，以及其與機密資訊保護的關聯。
- (6) 機密資訊的受准許使用，與簽署者使用資訊的權利。
- (7) 對涉及機密資訊之稽核與監視活動的權利。
- (8) 通知與通報未經授權揭露或機密資訊洩漏的過程。
- (9) 協議停止時資訊歸還或銷毀的條款。
- (10) 一旦違反此協議時將會採取的行動。

A.14

系統獲取、開發及維護

系統開發與維護應納入資訊安全方面的考量，從初始的規畫、設計、乃至測試、上線、維護等程序，針對可能的危機與錯誤採取相對的措施，在不違反各資訊安全政策與措施的情形下，符合施行單位的要求。此部份需要考量的因素較為細小繁雜，有賴於合作廠商或是外部專家的專業知識，以達到完善的系統安全，降低可能的損害與毀壞。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.14 系統獲取、開發及維護					A.10 A.12
控制目標	A.14.1	資訊系統之安全要求事項			A.10.8 A.12.1
控制項	A.14.1.1 (I/P)	資訊安全要求事項分析及規格	資訊安全相關要求，應納入新資訊系統或既有資訊系統之強化的要求事項中。	B.10.1.1	A.12.1.1
	A.14.1.2	保全公共網路之應用服務	應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。		A.10.8.4
	A.14.1.3 (建議)	保護應用服務交易	應保護應用服務交易中涉及之資訊，以防止不完整的傳輸、誤選路（mis-routing），未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。		
控制目標	A.14.2	於開發及支援過程中之安全			A.12.5
控制項	A.14.2.1 (建議)	保全開發政策	應建立軟體及系統開發之規則，並應用至施行單位內之開發。		
	A.14.2.2	系統變更控制程序	應藉由使用正式之變更控制程序，以控制開發生命週期內之系統變更。		A.12.5.1
	A.14.2.3	運作平台變更後，應用之技術審查	當運作平台變更時，應審查及測試營運之關鍵應用，以確保對組織運作或安全無不利衝擊。		A.12.5.2
	A.14.2.4	軟體套件變更之限制	應不鼓勵修改軟體套件，且僅限於必要變更，並應嚴格控制所有變更。		A.12.5.3

	A.14.2.5	保全系統工程原則	保全系統之工程原則，應予建立、文件化、維持及應用於所有資訊系統實作工作。		A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.4
	A.14.2.6 (建議)	保全開發環境	對涵蓋整個系統開發生命週期之系統開發及整合工作，施行單位應建立並適切地保護安全開發環境。		
	A.14.2.7	委外開發	組織應監督及監視委外系統開發活動。		A.12.5.5
	A.14.2.8 (I/P) (建議)	系統安全測試	於開發中，應實施安全功能之測試。	B.10.1.1	
	A.14.2.9 (I/P)	系統驗收測試	應建立新資訊系統、系統升級及新版本之驗收測試計畫及準則。	B.10.1.1	
控制目標	A.14.3	測試資料			A.12.4
控制項	A.14.3.1 (I/P)	測試資料之保護	應小心選擇、保護及控制測試資料。	B.10.1.1	A.12.4

實作指引

(一) 資訊系統之安全要求事項 (A.14.1) 一較適用於行政資訊系統

1. 資訊安全要求事項分析及規格 (A.14.1.1)

資訊安全相關要求，應納入新資訊系統或既有資訊系統之強化的要求事項中。

應詳述新系統或既有系統之各項控制措施要求。

系統安全之控制措施宜：

- (1) 在資訊系統規劃之需求分析階段，即將安全需求納入；新發展的資訊系統或顯有系統功能之強化，皆宜明定資訊安全需求，並將安全需求納入系統功能。
- (2) 除系統自動執行的安控措施外，亦可考量由人工執行的安控措施；採購套裝軟體時，亦宜進行相同的安全需求。
- (3) 系統的安全需求及控制程度，宜與資訊資產價值相稱，並考量安全措施不足對機關可能帶來的傷害程度。
- (4) 資訊安全需求分析，宜特別考量：
 - a. 評估保護資訊機密性、整合性及可用性的需求。
 - b. 找出及決定各種不同的安全控管措施，以防範、偵測電腦當機或發生安全事件時，能立即執行回復作業。
 - c. 宜於相關文件規定資訊安全控制措施，以利使用者及電腦支援人員明瞭系統內建之安控系統功能。

2. 保全公共網路之應用服務 (A.14.1.2)

應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。

對外提供服務的資訊系統或網頁，應進行資訊安全考量事項，且對外公告資訊前

應有正式授權程序，並避免未授權之竄改。

關於對外服務資訊系統管理，宜考量：

- (1) 對外開放的資訊系統，宜儘可能安裝在一部專用的主機上，並以防火牆與機關內部網路區隔，提高內部網路的安全性。
- (2) 建立對外公告資訊程序，公告前須經由權責人員確認內容，並有正式授權證明，才得以進行公告動作。
- (3) 對外開放系統內之公告資訊內容須符合單位相關規定，避免含有機密性或敏感性資料。
- (4) 避免未授權之竄改，已對外公告資訊內容之修改須經由相關權責人員的認可及證明，才得以進行內容的調整。
- (5) 對外開放的資訊系統所提供之網路服務(FTP,Gopher,HTTP 等)，宜做適當的存取控管，以維護系統正常運作。

3. 保護應用服務交易 (A.14.1.3) (建議)

應保護應用服務交易中涉及之資訊，以防止不完整的傳輸、誤選路 (mis-routing)，未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。

應用服務交易(如應用系統傳輸之資訊)的資訊安全考量宜包括下列項目：

- (1) 交易的所有層面，亦即確保：
 - a. 所有各方的使用者機密鑑別資訊為有效及經查證的。
 - b. 保持交易之機密性。
 - c. 保持相關各方的隱私權。
- (2) 所有與所涉及各方間的通信管道予以加密。
- (3) 用於與所涉及各方間的通信協定是安全的。
- (4) 確保交易細節的儲存於施行單位內部網路的儲存平台，不留存於與暴露在從網際網路可直接存取的儲存媒體上。

(二) 於開發及支援過程中之安全 (A.14.2)

1. 保全開發政策 (A.14.2.1) (建議)

應建立軟體及系統開發之規則，並應用至施行單位內之開發。

保全開發是建立一安全服務、架構、軟體及系統之要求。保全開發政策內，下列層面宜納入考量：

- (1) 開發環境之安全。
- (2) 軟體開發生命週期內安全之指引：
 - a. 軟體開發方法論之安全。
 - b. 所用每一程式語言之安全編碼指導綱要。
- (3) 設計階段內之安全要求。
- (4) 計畫期程內之安全查核點。
- (5) 開發資料保存安全。
- (6) 版本控制之安全。
- (7) 必要之應用系統安全知識。
- (8) 開發者避開、找出及修補脆弱性之能力。

2. 系統變更控制程序 (A.14.2.2)

應藉由使用正式之變更控制程序，以控制開發生命週期內之系統變更。

實施變更作業應依循嚴格的變更管制措施。

變更作業的控制程序宜：

- (1) 建立正式的變更控制措施，並嚴格執行，降低可能的安全風險；變更作業之控制程序，宜確保系統安全控制程序不會被破壞，並確保程式設計人員只能存取系統作業所需的項目，且任何的系統變更作業，皆宜獲得權責主管人員的同意。
- (2) 建立變更控制程序，宜考量的事項如下：
 - a. 規定系統使用者提出變更需求之權責，及接受系統變更建議之授權程序。
 - b. 規定系統完成變更作業後，系統使用者是否認可之權責。
 - c. 規定檢視系統安全控制及檢視系統真確性的程序，以確保系統變更作業不致影響或破壞系統原有的安全控制措施。
 - d. 宜找出系統變更作業需要修正的軟體、資料檔案、資料庫及硬體項目。
 - e. 在實際執行變更作業前，變更作業的細項建議，宜取得權責主管人員之核准。
 - f. 在執行變更作業前，宜確保系統變更作業能為使用者接受。
 - g. 系統文件在每次完成變更作業後，宜立即更新，舊版的系統文件亦宜妥善保管及處理。
 - h. 宜建立軟體更新的版本控制機制。
 - i. 所有的系統變更作業請求，皆宜建立稽核紀錄。

3. 運作平台變更後，應用之技術審查 (A.14.2.3)

當運作平台變更時，應審查及測試營運之關鍵應用，以確保對組織運作或安全無不利衝擊。

應用系統所在的運作平台/作業系統進行變更後，需進行必要之技術審核及測試。作業系統變更之技術評估宜：

- (1) 評估作業系統變更時，其對應用系統是否造成負面的影響，或產生安全上的問題。
- (2) 作業系統變更之評估程序，宜考量：
 - a. 評估應用系統的安控措施及查驗系統的真確性，以確保其未受作業系統變更之影響。
 - b. 作業系統變更的評估及測試結果，如需進行必要的調整，宜納入年度計畫及預算。
 - c. 作業系統的變更宜即時通告相關人員，以便在作業系統變更前，相關人員可以進行適當及充分的評估作業。
 - d. 確保營運持續管理計畫做適當的變更。

4. 軟體套件變更之限制 (A.14.2.4)

應不鼓勵修改軟體套件，且僅限於必要變更，並應嚴格控制所有變更。

避免修改套裝軟體，有必要修改時需採取嚴格管制。

套裝軟體變更之控管宜：

- (1) 廠商提供的套裝軟體，宜儘可能不要自行變更或修改。
- (2) 若需針對套裝軟體進行修改，宜考量：
 - a. 是否會破壞系統內建的安全控制，以及危害鑑別系統真確性作業的風險。
 - b. 宜取得套裝軟體開發廠商的同意。
 - c. 宜考量標準化的系統更新方式，請廠商進行必要的變更。
 - d. 宜考量如自行變更套裝軟體，日後進行軟體維護的可能性。
 - e. 保留原始軟體，並將變更資料予以記錄，備日後軟體在更新之用。

5. 保全系統工程原則 (A.14.2.5)

保全系統之工程原則，應予建立、文件化、維持及應用於所有資訊系統實作工作。宜建立、文件化、維持及應用基於保全工程原則之程序於內部資訊系統工程活動。權衡資訊安全之需求與可及性之需求，將安全性設計納入所有架構層（營運、資料、應用系統及技術）。並分析新技術安全風險並審查設計以避免已知的攻擊形式。可考量下列等安全設計需求：

- (1) 資料輸入之驗證。
- (2) 系統內部作業處理之驗證。
- (3) 訊息真確性之鑑別。
- (4) 資料輸出控管。

宜定期審查（宜每半年）上述原則及已建立之工程程序以確保其可有效地用於工程過程中。以確保其可有效應對新的潛在威脅，並維持技術之可用性與現有解決方案之適用性。

若可行，宜對外包資訊系統於契約及外包供應者與其他組織間的協議，載明建立之安全工程原則。

6. 保全開發環境 (A.14.2.6) (建議)

對涵蓋整個系統開發生命週期之系統開發及整合工作，施行單位應建立並適切地保護安全開發環境。

安全開發環境包括人員、過程及與系統開發及整合有關之技術。施行單位宜評鑑個別系統開發工作有關之風險，並對特定系統開發工作建立安全開發環境，並考量下列項目：

- (1) 系統處理、儲存及傳輸之資料的敏感性。
- (2) 適用之外部及內部要求事項，如來自法規或政策。
- (3) 支援系統開發已實作之安全控制措施。
- (4) 開發環境內工作人員之可信賴性。
- (5) 與系統開發有關之外包程度。
- (6) 不同開發環境間區隔之需要。
- (7) 對開發環境存取之控制措施。
- (8) 對環境及存於其中程式碼變更之監控。
- (9) 備份儲存於安全之異地理位置。

(10) 資料搬遷之控制措施。

7. 委外開發 (A.14.2.7)

施行單位應監督及監視委外系統開發活動。

委外開發需採取適當之管制及檢查。

在委外開發時宜考慮：

- (1) 授權作業、程式碼所有權及智慧財產權。
- (2) 品質驗證和工作執行的準確性
- (3) 預防受委託者因故無法執行的託管協定。
- (4) 工作完成時，為稽核品質和正確性所需的存取權限。
- (5) 程式碼品質的合約要求。

8. 系統安全測試 (A.14.2.8) (建議)

於開發中，應實施安全功能之測試。

新系統或系統更新時需在開發過程中測試及查證安全功能要求與工程原則，其中宜規劃測試活動的詳細時程、測試輸入條件以及預期輸出等。

若為內部開發，開發小組宜先執行上述測試。

9. 系統驗收測試 (A.14.2.9)

應建立新資訊系統、系統升級及新版本之驗收測試計畫及準則。

新資訊系統、系統升級與新版本正式上線前應予以適當的測試，建立驗收程序。

新系統上線作業之安全評估宜包含：

- (1) 訂定新系統被認可及納入正式作業的標準，並在新系統上線作業前，執行適當的測試。
- (2) 新系統被認可及納入正式作業的標準，宜執行：
 - a. 評估系統作業效能及電腦容量是否滿足需求。
 - b. 檢查發生錯誤後之回復作業以及系統重新啟動程序的準備作業，和資訊安全事件之緊急應變作業是否已經完備。
 - c. 進行新系統正式納入例行作業程序之準備及測試。
 - d. 評估新系統的建置不致影響現有的系統作業，尤其是對系統尖峰作業時段之影響。
 - e. 辦理新系統作業及使用者教育訓練。
- (3) 在發展重要系統時，宜確定系統的功能及確保系統的作業效能能夠滿足需求；例如在系統發展的每一階段，充分諮詢相關人員的意見。

(三) 測試資料 (A.14.3)

1. 測試資料之保護 (A.14.3.1)

應小心選擇、保護及控制測試資料。

系統之測試資料須予以保護與控管。

關於系統測試資料：

- (1) 宜保護及控制測試資料，避免以含有個人資料的真實資料庫進行測試；如需

應用真實資料，宜於事前將足以辨識個人的資料去除。

(2) 使用真實資料進行測試時宜：

- a. 確保適用在實際作業系統的存取控制措施，亦適用在測試用系統。
- b. 真實資料被複製到測試系統時，宜依複製作業的性質及內容，在取得授權後始能進行。
- c. 測試完畢後，真實資料宜立即從測試系統中刪除。真實資料的複製情形宜予以記錄，以備日後稽核之用。

A.15

供應者關係

為確保對供應者可存取之施行單位資產的保護，降低各種可能的風險與損害，維護資訊處理與服務之完整性及可用性，必須設立施行單位與供應者之管理措施。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.15 供應者關係					A.6 A.10
控制目標	A.15.1	供應者關係中之資訊安全		B.12.1	A.6.2
控制項	A.15.1.1 (I/P)	供應者關係 之資訊安全 政策	應與供應者議定並文件化，降低與供應者 存取施行單位資產關聯之風險的資訊安 全要求事項。	B.12.1.1	
	A.15.1.2 (I/P)	於供應者協 議中闡明安 全性	應與每個可能存取、處理、儲存或傳達資 訊，或提供 IT 基礎建設組件資訊之供應 者，建立及議定所有相關資訊安全要求事 項。	B.12.1.2	A.6.2.1
	A.15.1.3 (I/P) (建議)	資訊及通訊 技術供應鏈	與供應者之協議，應包含因應與資訊及通 訊技術服務及產品供應鏈關聯之資訊安 全風險。	B.12.1.2	
控制目標	A.15.2	供應者服務交付管理		B.12.1	A.10.2
控制項	A.15.2.1 (I/P)	供應者服務 之監視及審 查	組織應定期監視、審查及稽核供應者服務 交付。	B.12.1.1	A.10.2.2
	A.15.2.2 (I/P)	管理供應者 服務之變更	應管理供應者所提供服務之變更，包括維 持及改善既有的資訊安全政策、程序及控 制措施，並考量所涉及之營運資訊、系統 及過程的關鍵性，以及風險之重新評鑑。	B.12.1.1	A.10.2.3

實作指引

(一) 供應者關係中之資訊安全 (A.15.1)

1. 供應者關係之資訊安全政策 (A.15.1.1)

應與供應者議定並文件化，降低與供應者存取施行單位資產關聯之風險的資訊安全要求事項。

施行單位宜在政策中識別及規定特別處理供應者存取施行單位資訊之資訊安全控制措施。上述控制措施宜列出施行單位將實作之過程及程序，以及施行單位將要求供應者實作之過程及程序，包括：

- (1) 供應者管理流程與最低資訊安全要求。
- (2) 與供應者存取有關的資安事故應變處理與責任。

- (3) 供應者人員的資安認知訓練。
- (4) 資訊安全要求及控制措施之書面協議。

2. 於供應者協議中闡明安全性 (A.15.1.2)

應與每個可能存取、處理、儲存或傳達資訊，或提供 IT 基礎建設組件資訊之供應者，建立及議定所有相關資訊安全要求事項。

面對外部人員存取施行單位資訊處理設施的可能風險，應視狀況採取適當的安全控制措施，並條列安全規定於正式合約中。

關於外部人員存取的安全控制措施，宜包含：

- (1) 評估存取風險，了解存取的資料類型、價值、安全措施與影響，並確保與外部人員建立協議，簽訂契約，才得以進行存取動作。
- (2) 外部人員存取之安全契約，宜條列資訊安全規定、標準、必要連線條件、各項法律責任及限制、撤銷使用權利規定等供其遵守。
- (3) 監督、查核外部人員存取行為，建立控制其遵守相關規定之機制，必要時做出反應並留存相關紀錄。

3. 資訊及通訊技術供應鏈 (A.15.1.3) (建議)

與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險。

供應者協議中關於分包商、技術原廠、設備零件廠商等供應鏈安全宜考量包括下列主題：

- (1) 除一般供應者關係資訊安全要求以外，界定適用於資通訊技術產品或服務之資訊安全要求。
- (2) 要求供應者對分包商、技術原廠、設備零件廠商等整個供應鏈傳達施行單位之安全要求。
- (3) 規劃實作監控流程確保交付之資通訊技術產品如預期運作。
- (4) 實作資通訊技術組件生命週期及可用性等相關安全風險的管理過程。

(二) 供應者服務交付管理 (A.15.2)

1. 供應者服務之監視及審查 (A.15.2.1)

組織應定期監視、審查及稽核供應者服務交付。

施行單位應監視和審查廠商提供的服務，確保服務標準達到協議的要求。

宜考慮下列安控措施：

- (1) 檢視服務效能標準是否符合協議要求。
- (2) 審查廠商產生的報告並按照協議需求定期（宜每半年）安排行程會議。
- (3) 施行單位提供資訊安全事件的資訊，由廠商和施行單位審查這些資訊。
- (4) 審查廠商安全事件、操作問題、錯誤的稽核存底與記錄。
- (5) 解決和管理所有界定的問題。

2. 管理供應者服務之變更 (A.15.2.2)

應管理供應者所提供服務之變更，包括維持及改善既有的資訊安全政策、程序及

控制措施，並考量所涉及之營運資訊、系統及過程的關鍵性，以及風險之重新評鑑。

面對廠商服務異動的管理程序，應注意相關的系統以及程序，確實的掌控以避免導致新資訊安全危機。

服務異動之管理程序宜包含：

- (1) 由施行單位產生的異動。
 - a. 現有服務的加強。
 - b. 任何新應用程式和系統的開發。
 - c. 單位政策與程序的修改或更新。
 - d. 需要改善安全和解決資訊安全事件的新措施。
- (2) 由廠商服務產生的異動。
 - a. 網路的改變或加強。
 - b. 新技術的使用。
 - c. 採用新產品或較新版本。
 - d. 新的開發工具和環境。
 - e. 服務設施實體位置的改變。
 - f. 賣主異動。

A.16

資訊安全事故管理

針對安全事件的發生，應即刻進行反應，並採取適當的處理措施，降低損害的擴大，並作為改進的參考；因此，當資訊安全事件發生時，除即時反應和忠實紀錄外，更需保存相關的資料紀錄，進一步列入後續的改正參考，如此才能有效的杜絕類似事件的再發生，有效降低威脅。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.16 資訊安全事故管理					A.13
控制目標	A.16.1	資訊安全事故及改善之管理		B.10.2	A.13.1 A.13.2
控制項	A.16.1.1 (I/P)	責任及程序	應建立管理責任及程序，以確保對資訊安全事故做迅速、有效及有序之回應。	B.10.2.1	A.13.2.1
	A.16.1.2 (I/P)	通報資訊安全事件	應循適切之管理管道，儘速通報資訊安全事件。	B.10.2.1	A.13.1.1
	A.16.1.3 (I/P)	通報資訊安全弱點	應要求使用資訊系統及服務之員工及承包者，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。	B.10.2.1	A.13.1.1
	A.16.1.4 (I/P)	資訊安全事件評估及決策	應評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故。	B.10.2.1	
	A.16.1.5 (I/P)	對資訊安全事故之回應	應依文件化程序，回應資訊安全事故。	B.10.2.1	
	A.16.1.6 (I/P)	由資訊安全事故中學習	應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性及衝擊。	B.10.2.1	A.13.2.2
	A.16.1.7 (I/P)	證據之收集	組織應定義及應用程序，以識別、蒐集、取得及保存可用作證據之資訊。	B.10.2.1	A.13.2.3

實作指引

(一) 資訊安全事故及改善之管理 (A.16.1)

1. 責任及程序 (A.16.1.1)

應建立管理責任及程序，以確保對資訊安全事故做迅速、有效及有序之回應。

應建立處理資訊安全事件之作業程序，並課予相關人員必要的責任，以便迅速有效處理機關資訊安全事件。

資訊安全事件的反應與處理作業的程序包括：

(1) 針對各項資訊安全事件，進行適當的處理程序；資訊安全事件可能包括：

- a. 電腦當機及中斷服務。
- b. 惡意的程式碼。
- c. 阻斷服務。

- d. 業務資料不完整，或是資料不正確導致的作業錯誤。
 - e. 機密性資料遭侵犯。
 - f. 資訊系統的不當使用。
- (2) 除正常的應變計畫外（如系統及服務回復作業），資訊安全事件之處理程序尚宜納入：
- a. 導致資訊安全事件原因之分析，與資訊安全事件之控管。
 - b. 封鎖措施。
 - c. 防止類似事件再發生之補救措施的規劃及執行。
 - d. 與使用者及其他受影響的人員，或是負責系統回復的人員進行溝通及瞭解。
 - e. 回報處理情形至權責單位。
2. 通報資訊安全事件（A.16.1.2）
- 應循適切之管理管道，儘速通報資訊安全事件。
- 施行單位宜：
- (1) 建立資訊安全事件的正式通報程序及管道，訂定接受資訊安全事件通報宜採行之行動及措施。
 - (2) 相關人員宜確實明瞭各種資訊安全事件的反應及報告程序。
3. 通報資訊安全弱點（A.16.1.3）
- 應要求使用資訊系統及服務之員工及承包者，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。
- 施行單位宜：
- (1) 如發現或懷疑有資訊安全事件時（包括系統有安全漏洞、受威脅、系統弱點及功能不正常事件等），宜依已訂定之通報管道迅速通報權掌人員立即處理。
 - (2) 所有員工及承包者宜將這些事件儘快通報連絡點，以防止資訊安全事故。通報機制宜儘可能容易、可利用及可取得。
 - (3) 系統安全上的弱點，宜由專業人員處理，不宜任由系統使用者自行修改。
4. 資訊安全事件評估及決策（A.16.1.4）
- 應評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故(incident)。
- 聯絡窗口宜使用已協議之資訊安全事件分級準則評估通報之資訊安全事件，並決定是否將其歸類為會造成營運異常或中斷，或是影響服務對象業務、權益或造成損害之資訊安全事故。
- 事件處理人員宜藉由事件之分類分級與優先順序訂定等過程來識別事故之衝擊及範圍。同時為未來參照及查證之目的，宜詳細記錄評鑑及決策之結果。
5. 對資訊安全事故之回應（A.16.1.5）
- 應依文件化程序，回應資訊安全事故。
- 宜由施行單位指定之連絡點及其他相關人員回應資訊安全事故。必要時，宜舉行後事故分析以識別事故之來源。

回應宜包括下列項目：

- (1) 發生後儘快收集證據。
- (2) 實施資訊安全鑑識分析。
- (3) 確保適當地存錄涉及之回應活動，以作日後之分析。
- (4) 處理導致或促成該事故之資訊安全弱點。
- (5) 若已成功地處理事故，正式地結案並記錄之。

6. 由資訊安全事故中學習 (A.16.1.6)

應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性及衝擊。監控並紀錄事件的過程與結果，必要時進行檢討會議，討論改善之事宜。關於資訊安全事件的發生過程與紀錄，宜針對整體資訊安全事件進行監控並紀錄，向管理階層提報，並視事件的嚴重性進行檢討會議，討論改善事宜。

7. 證據之收集 (A.16.1.7)

組織應定義及應用程序，以識別、蒐集、取得及保存可用作證據之資訊。電腦稽核軌跡及相關的證據，應以適當的方法保護，以利於下列作業：

- (1) 作為機關內部分析問題之依據。
- (2) 作為研析是否違反契約或是違反單位資訊安全規定的證據。
- (3) 作為與軟體及硬體供應商，協商補償之依據。

宜依據「政府機關（構）資安事件數位證據保全標準作業程序」或相關證據保全作業規範，進行數位證據之蒐集與保存。

A.17

營運持續管理之資訊安全層面

永續運作的目的在於碰到重大意外或造成學校或單位運作中止的突發狀況時，使必要業務得以不受影響持續運行，將其傷害減至最低；所以，為維持施行單位業務的永續運作，應進行相關的規劃及檢測，以達到業務進行不中斷之目標。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.17 營運持續管理之資訊安全層面					A.14
控制目標	A.17.1	資訊安全持續			A.14.1
控制項	A.17.1.1	規劃資訊安全持續	施行單位應決定對其資訊安全之要求事項，以及在不利情況下（例：危機或災難期間），對資訊安全之持續性要求事項。		A.14.1.1
	A.17.1.2	實作資訊安全持續	施行單位應建立、文件化、實作及維持過程、程序及控制措施，以確保在不利情況期間所要求之資訊安全持續等級。		A.14.1.1
	A.17.1.3	查證、審查及評估資訊安全持續	組織應定期查證所建立及實作之資訊安全持續控制措施，以確保其於不良情況期間係生效及有效。		A.14.1.2
控制目標	A.17.2	多重備援			
控制項	A.17.2.1	資訊設備之可用性	應對資訊處理設施實作充分之多重備援，以符合可用性要求。		

實作指引

(一) 資訊安全持續 (A.17.1)

1. 實作資訊安全持續 (A.17.1.1)

施行單位應決定對其資訊安全之要求事項，以及在不利情況下（例：危機或災難期間），對資訊安全之持續性要求事項。

施行單位宜決定資訊安全持續是否已留存於營運持續管理過程或災害復原管理過程內。宜在規劃營運持續及災害復原時決定資訊安全要求。

施行單位可執行資訊安全層面之營運衝擊分析以決定適用於不良情況下之資訊安全要求。

關於營運持續作業規劃及架構建立宜：

- (1) 建立跨部門的營運持續計劃程序，研訂及維護機關業務持續運作之計畫。
- (2) 營運持續運作的規劃作業，宜研析並降低人為或是意外因素對機關重要業務運作可能導致的威脅，使重要業務在系統發生事故、設施失敗或是受損害時，仍可持續運作。
- (3) 營運持續計畫，宜考量下列事項：
 - a. 界定重要的業務作業程序，並訂定優先順序。

- b. 評估各種災害對機關業務可能的衝擊。
 - c. 維持機關永續運作之人員責任界定，以及緊急應變措施之安排。
 - d. 建立機關永續運作之作業程序及流程，並以書面或其他方式記載。
 - e. 宜就緊急應變程序及作業流程，進行員工教育及訓練。
 - f. 宜測試緊急應變計畫。
 - g. 宜定期（宜每半年）更新緊急應變計畫。
- (4) 宜建立及維持單一的營運持續計畫架構，使各種不同層次及等級的計畫相互連貫，並宜訂定測試計畫及維護計畫之優先順序。
- (5) 營運持續計畫，宜明定行動之條件，以及員工執行計畫之責任；機關研擬新的資訊計畫，宜與機關緊急應變計畫程序相一致。
- (6) 在營運持續之整體架構內，宜訂定不同層次及等級的計畫，每一層次及等級的計畫，宜涵蓋不同的計畫重點及負責回復作業的人員安排。

2. 實作資訊安全持續（A.17.1.2）

施行單位應建立、文件化、實作及維持過程、程序及控制措施，以確保在不利情況期間所要求之資訊安全持續等級。

營運運作計畫，宜考量的作業程序為：

- a. 訂定緊急應變作業程序，規定如何在發生危害單位業務運作或危及生命的重大事件發生時，宜立即採取的行動。
- b. 訂定預備作業程序，規定如何將必要的機關業務活動或是支援性的服務，移轉至另外一個臨時的作業地點。
- c. 訂定回復作業程序，規定如何採取回復作業，使機關的業務回復到原來正常的業務運作。
- d. 訂定測試作業程序，規定如何及什麼時間行測試作業。

施行單位宜確保下列事項：

- (1) 各項計畫指定一位計畫執行督導人員。
- (2) 緊急應變作業、人員預備作業及回復計畫等，宜指定適當的單位或人員負責。
- (3) 技術服務的預備作業安排，宜由技術服務提供者負責。
- (4) 制訂並核准各項規劃、回應及復原的程序，其中包含資訊安全持續目標、中斷事件管理方式與及資訊安全等級維持方式。
- (5) 營運持續或災害復原的流程

3. 查證、審查及評估資訊安全持續（A.17.1.3）

應依據「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」或相關資安規定中各級單位業務持續運作演練要求進行規劃。

施行單位應定期查證所規畫及實作之資訊安全永續運作控制措施，以確保其於不利情況期間可有效運行。

- (1) 組織、技術或流程之變更，不論是業務運作或永續運作之內容，均可導致資訊安全要求之變更。施行單位宜針對變更之要求審查與資訊安全永續運作相關之流程及控制措施。
- (2) 施行單位宜藉由下列方式查證其資訊安全管理之永續運作：

- a. 演練與測試資訊安全永續運作流程與控制措施之功能，以確保其與資訊安全永續運作目標一致。
- b. 演練及測試運行資訊安全永續運作流程與控制措施之認知及例行作業，以確保其效能與資訊安全持續目標一致。
- c. 資訊系統、資訊安全流程與控制措施或業務永續運作管理/災害復原管理之流程變更時，宜審查資訊安全永續運作措施之有效性。

(二) 多重備援 (A.17.2)

1. 資訊設備之可用性 (A.17.2.1)

應對資訊設備實作充分之多重備援，以符合可用性要求。

- (1) 施行單位宜識別資訊系統可用性之業務運作要求。若現有系統架構無法確保可用性，宜使用多重備援系統或架構。
- (2) 施行單位宜於可行時，測試多重備援系統架構以確保資訊設備於失效時可如預期順利切換至備援之資訊設備。

A.18

遵循性

所有的 ISMS 控制措施與管理條款，除了須符合施行單位的政策外，與相關法規的符合性亦須相符，避免缺乏法源上的依據，而在於系統方面的稽核上，也需採用適當的工具進行檢測，確保運作維持不中斷。

本章節主要的內容可參照下表：

				規範 附錄 B	原規範
A.18 遵循性					A.6 A.15
控制目標	A.18.1	對法律及契約要求事項之遵循		柒一(一)	A.15.1
控制項	A.18.1.1 (I/P)	適用之法規及契約的要求事項之識別	對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。	柒一(一) B.11.1.2	A.15..1.1
	A.18.1.2	智慧財產權	應實作適切程序，以確保遵循智慧財產權及專屬軟體產品使用之相關法律、法令及契約的要求事項。	柒一(一)	A.15..1.2
	A.18.1.3 (I/P)	紀錄之保護	應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未授權存取及未經授權發布。	B.10.1.1	A.15.1.2
	A.18.1.4 (I/P)	個人可識別資訊之隱私及保護	應依適用之相關法令、法規中之要求，以確保符合個人可識別資訊之隱私及保護。	B.10.1.1	A.15.1.2
	A.18.1.5 (建議)	密碼式控制措施(加密控制措施)的監管	應使用密碼式控制措施(加密控制措施)，以遵循所有相關的協議、法律及法規。	柒一(一)	
控制目標	A.18.2	資訊安全審查		柒六(二) 柒六(三) B.10.1	A.6.1 A.15.2
控制項	A.18.2.1 (I/P)	資訊安全之獨立審查	應依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全之作法及其實作(亦即資訊安全之各項控制目標、控制措施、政策、過程及程序)。	柒六(三) B.10.1.3	A.6.1.6

	A.18.2.2 (I/P)	安全政策及標準之遵循性	管理人員應以適切之資訊安全政策、標準及其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。	柒六(二) B.10.1.3	A.15.2.1
	A.18.2.3 (I/P)	技術遵循性審查	應定期審查資訊系統對組織之資訊安全政策及標準的遵循性。	柒六(二) B.10.1.3	A.15.2.2

實作指引

(一) 對法律及契約要求事項之遵循 (A.18.1)

1. 適用之法規及契約的要求事項之識別 (A.18.1.1)

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

蒐集相關法律條文（智慧財產權、資料隱私保護及其他相關法規）、管理規定及合約要求，了解與資訊處理設施、軟體系統的關係，並予以書面或其他方式留存。

2. 智慧財產權 (A.18.1.2)

應實作適切程序，以確保遵循智慧財產權及專屬軟體產品使用之相關法律、法令及契約的要求事項。程序宜包括：

- (1) 公布智慧財產權遵循政策，此政策定義軟體與資訊產品的合法使用。
- (2) 只經由知名且信譽良好的來源採購軟體，確保不違反著作權。
- (3) 維持對保護智慧財產權政策的認知，並通知違反政策人員將遭懲處。
- (4) 維持適切的資產登記簿，並識別所有資產符合保護智慧財產權之要求。
- (5) 維護使用版權、原版碟片、手冊等所有權的證明和證據。
- (6) 執行控制措施，以確保不超過任何版權內允許的最多使用人數。
- (7) 定期（宜每半年）檢核是否只安裝經授權軟體與有使用版權的產品。

3. 紀錄之保護 (A.18.1.3)

應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未授權存取及未經授權發布。

施行單位保護之紀錄宜考量對應施行單位分類及分級法。紀錄宜按紀錄型式（例如：會計紀錄、資料庫紀錄、交易日誌、稽核日誌和運作程序）分類，每樣都有詳細的保存期間和儲存媒體型式（例如：紙張、微縮膠片、磁性或光學儲存媒體）。

4. 個人可識別資訊之隱私及保護 (A.18.1.4)

應依適用之相關法令、法規中之要求，以確保符合個人可識別資訊之隱私及保護。宜配合附錄 B 個人資料管理規範，發展和實作施行單位的個人可識別資訊之隱私及保護資料政策。

處理個人可識別資訊和確保隱私原則認知的責任宜依據相關法律及法規處理。宜實作適當的技術措施以保護個人可識別資訊。

5. 密碼式控制措施(加密控制措施)的監管 (A.18.1.5)

應使用密碼式控制措施(加密控制措施)，以遵循所有相關的協議、法律及法規。

為了遵循相關的協議、法律及法規，宜考量對加密的使用設限制，如通行碼長度、通行碼複雜度、通行碼變更週期。

對外採購加密技術時，宜請廠商提供輸出國核發之輸出許可文件，並避免採購國外金鑰代管或金鑰回復之產品。(原 A.12.3.2)

(二) 資訊安全審查 (A.18.2)

1. 資訊安全之獨立審查 (A.18.2.1)

應依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全之作法及其實作（亦即資訊安全之各項控制目標、控制措施、政策、過程及程序）。

機關制訂之資訊安全政策，應進行獨立及客觀的評估。

在資訊安全政策評估上，宜考量反映政府資訊安全管理政策、法令、技術及機關業務之最新狀況，確保資訊安全之實務作業，確實遵守施行單位的資訊安全政策，並確保資訊安全實務作業的可行性及有效性。

2. 安全政策及標準之遵循性 (A.18.2.2)

管理人員應以適切之資訊安全政策、標準及其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。

應依據「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」或相關資安規定中各級單位稽核方式要求進行規劃。

確保單位內所有區域或作業流程皆定期審查及確保遵守安全政策及規範。

3. 技術遵循性審查 (A.18.2.3)

應定期審查資訊系統對組織之資訊安全政策及標準的遵循性。

為確保資訊系統之運行符合既定之安全實施標準，應進行配合前述標準稽核周期規劃定期審查，並予以書面或其他方式留存。

附件 1 各級教育機構適用控制項對照表

A 級單位建議納入所有控制措施(計 114 項)；原適用第一學群之控制措施(計 101 項)則建議 B 級單位採用；原適用第二學群之控制措施(計 51 項)，則建議由 C 級單位使用。另外，經資訊系統分級鑑別後為「高」等級之資訊系統，則應加入 A.14 系統獲取、開發及維護與 A.15 供應者關係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。

				原規範	ISO 27001: 2005	適用單位		
A.5 資訊安全政策				A.5	A.5	C	B	A
控制目標	A.5.1	資訊安全之管理指導方針		A.5.1	A.5.1			
控制項	A.5.1.1 (I/P)	資訊安全政策	資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。	A.5.1.1	A.5.1.1	V	V	V
	A.5.1.2 (I/P)	資訊安全政策之審查	資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。	A.5.1.2	A.5.1.2	V	V	V
A.6 資訊安全之組織				A.6/A10 A.11	A.6			
控制目標	A.6.1	內部組織		A.6.1 A.10.1	A.6.1 A.8.1 A.10.1			
控制項	A.6.1.1 (I/P)	資訊安全之角色及責任	應定義及配置所有資訊安全責任。	A.6.1.1	A.6.1.3 A.8.1.1	V	V	V
	A.6.1.2	職務區隔	衝突之職務及責任範圍應予以區隔，以降低組織資產遭未經授權或非蓄意修改或誤用之機會。	A.10.1.3	A.10.1.3		V	V
	A.6.1.3	與權責機關之聯繫	應維持與相關權責機關之適切聯繫。	A.6.1.4	A.6.1.6	V	V	V
	A.6.1.4	與特殊關注方之聯繫	應維持與各特殊關注方或其他各種專家安全論壇及專業協會之適切聯繫。	A.6.1.5	A.6.1.7	V	V	V
	A.6.1.5	專案管理之資訊安全	不論專案之型式，應在專案管理中因應資訊安全。					V
控制目標	A.6.2	行動裝置及遠距工作		A.11.6	A.11.7			
控制項	A.6.2.1	行動裝置政策	應採用政策及支援之安全措施，以管理因使用行動裝置所導致之風險。	A.11.6.1	A.11.7.1		V	V
	A.6.2.2	遠距工作	應實作政策及支援之安全措施，以保護存取、處理或儲存於遠距工作場所之資訊。	A.11.6.2	A.11.7.2		V	V

A.7 人力資源安全				A.8	A.8			
控制目標	A.7.1	聘用前			A.8.1			
控制項	A.7.1.1 (I/P)	篩選	對所有可能被聘用者所進行之背景調查，應依照相關法律、法規及倫理，並應相稱於營運要求及其將存取之資訊保密等級及組織所察覺之風險聘用。		A.8.1.2		V	V
	A.7.1.2 (I/P)	聘用條款及條件	施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。		A.8.1.3	V	V	V
控制目標	A.7.2	聘用期間		A.8.2	A.8.2			
控制項	A.7.2.1 (I/P)	管理階層責任	管理階層應要求所有員工及承包者，依施行單位所建立政策及程序施行資訊安全事宜。		A.8.2.1		V	V
	A.7.2.2 (I/P)	資訊安全認知、教育及訓練	施行單位內所有員工及相關之承包者，均應接受及其工作職務相關的組織政策及程序之適切認知、教育及訓練，並定期更新。	A.8.2.1	A.8.2.2	V	V	V
	A.7.2.3	懲處過程	應具備正式即已傳達之懲處過程，以對違反資訊安全之員工採取行動。	A.8.2.2	A.8.2.3	V	V	V
控制目標	A.7.3	聘用之終止及變更		A.8.3	A.8.3			
控制項	A.7.3.1 (I/P)	聘用責任之終止或變更	應對員工及承包者定義、傳達於聘用終止或變更後資訊安全責任及義務仍保持有效，並執行之。	A.8.3.1	A.8.3.1	V	V	V
A.8 資產管理				A.7 A.8 A.10	A.7			
控制目標	A.8.1	資產責任		A.7.1 A.8.3	A.7.1 A.8.3			
控制項	A.8.1.1 (I/P)	資產清冊	應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。	A.7.1.1	A.7.1.1	V	V	V
	A.8.1.2	資產擁有權	清冊中所維持之資產應有擁有者。	A.7.1.1	A.7.1.2	V	V	V
	A.8.1.3	資產之可被接受的使用	對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。	A.7.1.1	A.7.1.3	V	V	V
	A.8.1.4	資產之歸還	所有員工及外部使用者於其聘用、契約或協議終止時，應歸還其據有之全部組織資產。	A.8.3.2	A.8.3.2	V	V	V
控制目標	A.8.2	資訊分級		A.7.1 A.10.7	A.7.2 A.10.7			
控制項	A.8.2.1 (I/P)	資訊之分級	資訊應依法律要求、價值、重要性及其對未經授權揭露或修改之敏感性分級。	A.7.1.2	A.7.2.1	V	V	V

	A.8.2.2 (I/P)	資訊之標示	應依施行單位所採用之資訊級方案，發展及實作一套適切的資訊標示程序。	A.7.1.2	A.7.2.2	V	V	V
	A.8.2.3 (I/P)	資產之處置	應依施行單位所採用之資訊分級方案，發展及實作處置資產之程序。	A.10.7.3	A.10.7.3	V	V	V
控制目標	A.8.3	媒體處理		A10.7	A10.7			
控制項	A.8.3.1	可移除式媒體之管理	應依施行單位所採用之資訊分級方案，實作管理可移除式媒體之程序。	A.10.7.1	A.10.7.1		V	V
	A.8.3.2 (I/P)	媒體之汰除	當不再需要媒體時，應使用正式程序加以安全汰除。	A.10.7.2	A.10.7.2	V	V	V
	A.8.3.3	實體媒體傳送	應保護含有資訊之媒體在傳送時，不受未經授權的存取、誤用或毀損。		A.10.8.3		V	V
A.9 存取控制				A.8 A.11 A.12	A11			
控制目標	A.9.1	存取控制之營運要求事項		A.11.3	A.11.1 A.11.4			
控制項	A.9.1.1 (I/P)	存取控制政策	存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。		A.11.1.1		V	V
	A.9.1.2	對網路及網路服務之存取	應僅提供予使用者存取其已被特定授權使用之網路及網路服務。	A.11.3.1	A.11.4.1		V	V
控制目標	A.9.2	使用者存取管理		A.8.3 A.11.1	A.8.3 A.11.2 A.11.5			
控制項	A.9.2.1 (I/P)	使用者註冊與註銷	應實作正式之使用者註冊及註銷過程，俾能指派存取權限。	A.11.1.1	A.11.2.1 A.11.5.2	V	V	V
	A.9.2.2 (I/P)	使用者存取權限之配置	應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。					V
	A.9.2.3 (I/P)	具特殊存取權限之管理	應限制及控制具特殊存取權限之配置及使用。	A.11.1.2	A.11.2.2		V	V
	A.9.2.4 (I/P)	使用者之秘密鑑別資訊的管理	應以正式之管理過程控制秘密鑑別資訊的配置。	A.11.1.3	A.11.2.3	V	V	V
	A.9.2.5 (I/P)	使用者存取權限之審查	施行單位應定期審查使用者存取權限。	A.11.1.4	A.11.2.4		V	V
	A.9.2.6 (I/P)	存取權限之移除或調整	所有員工及外部使用者對資訊及資訊處理設施之存取權限，一旦其聘用、契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。	A.8.3.3	A.8.3.3	V	V	V

控制目標	A.9.3	使用者責任			A.11.3			
控制項	A.9.3.1 (I/P)	秘密鑑別資訊之使用	於使用秘密鑑別資訊時，應要求使用者遵循施行單位之實務規定。		A.11.3.1	V	V	V
控制目標	A.9.4	系統及應用存取控制		A.11.4 A.11.5 A.12.4	A.11.5 A.11.6 A.12.4			
控制項	A.9.4.1 (I/P)	資訊存取限制	應根據存取控制政策，限制對資訊及應用系統功能之存取。	A.11.5.1	A.11.6.1	V	V	V
	A.9.4.2 (I/P)	保全登入程序	當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。	A.11.4.1	A.11.5.1 A.11.5.5 A.11.5.6	V	V	V
	A.9.4.3 (I/P)	通行碼管理系統	通行碼管理系統應為互動式，並應確保嚴謹通行碼。	A.11.4.2	A.11.5.3	V	V	V
	A.9.4.4	具特殊權限公用程式之使用	應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。	A.11.4.3	A.11.5.4		V	V
	A.9.4.5	對程式源碼之存取控制	應限制對程式原始碼之存取。	A.12.4.3	A.12.4.3		V	V
A.10 密碼學(加密控制)				A.12	A.12			
控制目標	A.10.1	密碼式控制措施(加密控制措施)		A.12.3	A.12.3.1			
控制項	A.10.1.1	使用密碼式控制措施(加密控制措施)政策	應發展及實作政策，關於資訊保護之密碼式控制措施的使用。	A.12.3.1	A.12.3.1		V	V
	A.10.1.2	金鑰管理	應加以發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。	A.12.3.2	A.12.3.2			V
A.11 實體及環境安全				A.9 A.11	A.9			
控制目標	A.11.1	安全區域		A.9.1	A.9.1			
控制項	A.11.1.1 (I/P)	實體安全周界	應定義及使用安全周界，以保護收容敏感或重要資訊及資訊處理設施之區域。	A.9.1.1	A.9.1.1	V	V	V
	A.11.1.2 (I/P)	實體進入控制措施	保全區域應藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。	A.9.1.2	A.9.1.2		V	V
	A.11.1.3	保全之辦公室、房間及設施	應設計資訊處理設施所在區域之實體安全並施行之。	A.9.1.3	A.9.1.3		V	V
	A.11.1.4	防範外部及環境威脅	應設計並施行實體保護，以防範天然災害、惡意攻擊或事故。	A.9.1.3	A.9.1.4		V	V

	A.11.1.5	於保全區域內工作	應設計及施行資訊處理設施所在區域內工作之程序。	A.9.1.3	A.9.1.5		V	V
	A.11.1.6	交付及裝卸區	對諸如交付及裝卸區及其他未經授權人員可進入作業場所之進出點，應加以控制；若可能，應與資訊處理設施隔離，以避免未經授權之存取。		A.9.1.6			V
控制目標	A.11.2	設備		A.9.2 A.11.2	A.9.2 A.11.3			
控制項	A.11.2.1	設備安置及保護	應安置並保護設備，以降低來自環境之威脅及危害造成的風險，以及未經授權存取之機會。	A.9.2.1	A.9.2.1		V	V
	A.11.2.2	支援之公用服務事業	應保護設備免於電源失效，及因其他支援之公用服務事業失效，所導致之中斷。	A.9.2.2	A.9.2.2		V	V
	A.11.2.3	佈纜安全	應保護通訊纜線及資訊處理設備之電源，降低受竊聽或破壞的可能損失。	A.9.2.3	A.9.2.3		V	V
	A.11.2.4	設備維護	應正確維護設備，以確保其持續之可用性及完整性。	A.9.2.4	A.9.2.4	V	V	V
	A.11.2.5 (I/P)	財產之攜出	未經事前授權，不得將設備、資訊或軟體帶出場域外。	A.9.2.7	A.9.2.5	V	V	V
	A.11.2.6	場所外設備及資產的安全	安全應適用於場域外資產，並將於施行單位場所外工作之不同風險納入考量。		A.9.2.6			V
	A.11.2.7 (I/P)	設備汰除或再使用之保全	含有儲存媒體之所有設備組件，於汰除前或再使用前應加以查證，以確保任何敏感性資料及有版權之軟體已被移除或安全地覆寫。	A.9.2.5	A.9.2.7	V	V	V
	A.11.2.8	無人看管之使用者設備	使用者應確保無人看管之設備具備適切保護。		A.11.3.2			V
	A.11.2.9	桌面淨空及螢幕淨空政策	對紙本及可移除式儲存媒體應採用桌面淨空政策，且對資訊處理設施應採用螢幕淨空政策。	A.11.2.1	A.11.3.3		V	V
A.12 運作安全				A.10 A.12 A.15	A.12			
控制目標	A.12.1	運作程序及責任		A.10.1 A.10.3	A.10.1			
控制項	A.12.1.1	文件化運作程序	運作程序應加以文件化，並使所有需要之使用者均可取得。	A.10.1.1	A.10.1.1	V	V	V
	A.12.1.2	變更管理	應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更。	A.10.1.2	A.10.1.2		V	V

	A.12.1.3	容量管理	各項資源之使用應受監視及調適，並對未來容量要求預作規劃，以確保所要求之系統效能。	A.10.3.1	A.10.3.1		V	V
	A.12.1.4	開發、測試及運作環境之區隔	應區隔開發、測試及運作之環境，以降低對運作環境未經授權存取或變更的風險。	A.10.1.4 A.11.5.2	A.10.1.4		V	V
控制目標	A.12.2	防範惡意軟體		A.10.4	A.10.4			
控制項	A.12.2.1	防範惡意軟體之控制措施	應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。	A.10.4.1	A.10.4.1	V	V	V
控制目標	A.12.3	備份		A.10.5	A.10.5			
控制項	A.12.3.1	資訊備份	應依議定之備份政策，定期取得資訊、軟體及系統的影像檔備份複本，並測試之。	A.10.5.1	A.10.5.1		V	V
控制目標	A.12.4	存錄及監視		A.10.9	A.10.10			
控制項	A.12.4.1	事件存錄	應產生、保存並定期審查記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。	A.10.9.1 A.10.9.2 A.10.9.5	A.10.10.1 A.10.10.2 A.10.10.5		V	V
	A.12.4.2	日誌資訊之保護	應防範存錄設施及日誌資訊遭竄改及未經授權存取。	A.10.9.3	A.10.10.3		V	V
	A.12.4.3	管理者及操作者日誌	應存錄系統管理者及操作者之活動，且應保護及定期審查該日誌。	A.10.9.4	A.10.10.4		V	V
	A.12.4.4	鐘訊同步	組織或安全領域內所有相關資訊處理系統之鐘訊，應與單一參考時間源同步。	A.10.9.6	A.10.10.6		V	V
控制目標	A.12.5	運作中軟體之控制		A.12.4	A.12.4			
控制項	A.12.5.1	運作中系統之軟體安裝	應實作各項程序，以控制對運作中系統之軟體安裝。	A.12.4.1	A.12.4.1	V	V	V
控制目標	A.12.6	技術脆弱性管理		A.12.6	A.12.6			
控制項	A.12.6.1	技術脆弱性管理	應及時取得關於使用中之資訊系統的技術脆弱性資訊、並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。	A.12.6.1	A.12.6.1		V	V
	A.12.6.2	對軟體安裝之限制	應建立並實作使用者安裝軟體之管控規則。					V
控制目標	A.12.7	資訊系統稽核考量		A.15.3	A.15.3			
控制項	A.12.7.1	資訊系統稽核控制措施	應仔細規劃並議定，涉及運作中系統之稽核要求事項及活動，以使營運過程中斷降至最低。	A.15.3.1	A.15.3.1	V	V	V
A.13 通訊安全				A.6 A.10	A.6 A.10			

				A.11	A.11			
控制目標	A.13.1	網路安全管理		A.10.6 A.11.3	A.10.6 A.11.4			
控制項	A.13.1.1	網路控制措施	應實施網路控制措施，維護網路安全。	A.10.6.1 A.11.3.2 A.11.3.3 A.11.3.4 A.11.3.5 A.11.3.6	A.10.6.1		V	V
	A.13.1.2	網路服務之安全	應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外所提供。	A.10.6.2	A.10.6.2		V	V
	A.13.1.3	網路之區隔	應區隔各群組之資訊服務、使用者及資訊系統使用的網路。	A.11.3.4	A.11.4.5		V	V
控制目標	A.13.2	資訊傳送		A.6.1 A.10.8	A.6.1 A.10.8			
控制項	A.13.2.1 (I/P)	資訊傳送政策及程序	應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。	A.10.8.1	A.10.8.1	V	V	V
	A.13.2.2 (I/P)	資訊傳送協議	協議應闡明組織與外部各方間營運資訊之安全傳送。	A.10.8.1	A.10.8.2	V	V	V
	A.13.2.3 (I/P)	電子傳訊	應適切保護電子傳訊時所涉及之資訊。	A.10.8.2	A.10.8.4		V	V
	A.13.2.4 (I/P)	機密性或保密協議	應識別、定期審查及文件化，以反映施行單位對資訊保護之需要的機密性或保密協議之要求事項。	A.6.1.3	A.6.1.5	V	V	V
A.14 系統獲取、開發及維護				A.10 A.12	A.10 A.12			
控制目標	A.14.1	資訊系統之安全要求事項		A.10.8 A.12.1	A.12.1			
控制項	A.14.1.1	資訊安全要求事項分析及規格	資訊安全相關要求，應納入新資訊系統或既有資訊系統之強化的要求事項中。	A.12.1.1	A.12.1.1		V	V
	A.14.1.2	保全公共網路之應用服務	應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。	A.10.8.4	A.10.9.1 A.10.9.3		V	V
	A.14.1.3	保護應用服務交易	應保護應用服務交易中涉及之資訊，以防止不完整的傳輸、誤選路（mis-routing），未經授權之訊息修改、		A.10.9..2			V

			未經授權之揭露、未經授權之訊息複製或重演。					
控制目標	A.14.2	於開發及支援過程中之安全		A.12.5	A.12.5			
控制項	A.14.2.1	保全開發政策	應建立軟體及系統開發之規則，並應用至施行單位內之開發。					V
	A.14.2.2	系統變更控制程序	應藉由使用正式之變更控制程序，以控制開發生命週期內之系統變更。	A.12.5.1	A.12.5.1		V	V
	A.14.2.3	運作平台變更後，應用之技術審查	當運作平台變更時，應審查及測試營運之關鍵應用，以確保對組織運作或安全無不利衝擊。	A.12.5.2	A.12.5.2		V	V
	A.14.2.4	軟體套件變更之限制	應不鼓勵修改軟體套件，且僅限於必要變更，並應嚴格控制所有變更。	A.12.5.3	A.12.5.3		V	V
	A.14.2.5	保全系統工程原則	保全系統之工程原則，應予建立、文件化、維持及應用於所有資訊系統實作工作。	A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.4	A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.4		V	V
	A.14.2.6	保全開發環境	對涵蓋整個系統開發生命週期之系統開發及整合工作，施行單位應建立並適切地保護安全開發環境。					V
	A.14.2.7	委外開發	組織應監督及監視委外系統開發活動。	A.12.5.5	A.12.5.5		V	V
	A.14.2.8	系統安全測試	於開發中，應實施安全功能之測試。					V
	A.14.2.9	系統驗收測試	應建立新資訊系統、系統升級及新版本之驗收測試計畫及準則。	A.10.3.2	A.10.3.2		V	V
控制目標	A.14.3	測試資料		A.12.4	A.12.4			
控制項	A.14.3.1	測試資料之保護	應小心選擇、保護及控制測試資料。	A.12.4.2	A.12.4.2		V	V
A.15 供應者關係				A.6 A.10	A.6 A.10			
控制目標	A.15.1	供應者關係中之資訊安全		A.6.2	A.6.2			
控制項	A.15.1.1 (I/P)	供應者關係之資訊安全政策	應與供應者議定並文件化，降低與供應者存取施行單位資產關聯之風險的資訊安全要求事項。				V	V
	A.15.1.2 (I/P)	於供應者協議中闡明安全性	應與每個可能存取、處理、儲存或傳達資訊，或提供 IT 基礎建設組件資訊之供應者，建立及議定所有相關資訊安全要求事項。	A.6.2.1	A.6.2.3	V	V	V

	A.15.1.3 (I/P)	資訊及通訊 技術供應鏈	與供應者之協議，應包含因應與資訊及 通訊技術服務及產品供應鏈關聯之資訊 安全風險。					V
控制目標	A.15.2	供應者服務交付管理		A.10.2	A.10.2			
控制項	A.15.2.1 (I/P)	供應者服務 之監視及審 查	組織應定期監視、審查及稽核供應者服 務交付。	A.10.2.2	A.10.2.2	V	V	V
	A.15.2.2 (I/P)	管理供應者 服務之變更	應管理供應者所提供服務之變更，包括 維持及改善既有的資訊安全政策、程序 及控制措施，並考量所涉及之營運資 訊、系統及過程的關鍵性，以及風險之 重新評鑑。	A.10.2.3	A.10.2.3	V	V	V
A.16 資訊安全事故管理				A.13	A.13			
控制目標	A.16.1	資訊安全事故及改善之管理		A.13.1 A.13.2	A.13.1 A.13.2			
控制項	A.16.1.1 (I/P)	責任及程序	應建立管理責任及程序，以確保對資訊 安全事故做迅速、有效及有序之回應。	A.13.2.1	A.13.2.1	V	V	V
	A.16.1.2 (I/P)	通報資訊安 全事件	應循適切之管理管道，儘速通報資訊安 全事件。	A.13.1.1	A.13.1.1	V	V	V
	A.16.1.3 (I/P)	通報資訊安 全弱點	應要求使用資訊系統及服務之員工及承 包者，注意並通報任何系統或服務中所 觀察到或可疑之資訊安全弱點。	A.13.1.1	A.13.1.2	V	V	V
	A.16.1.4 (I/P)	資訊安全事 件評估及決 策	應評鑑資訊安全事件，並決定是否將其 歸類為資訊安全事故。			V	V	V
	A.16.1.5 (I/P)	對資訊安全 事故之回應	應依文件化程序，回應資訊安全事故。			V	V	V
	A.16.1.6 (I/P)	由資訊安全 事故中學習	應使用獲自分析及解決資訊安全事故之 知識，以降低未來事故之可能性及衝擊。	A.13.2.2	A.13.2.2	V	V	V
	A.16.1.7 (I/P)	證據之收集	組織應定義及應用程序，以識別、蒐集、 取得及保存可用作證據之資訊。	A.13.2.3	A.13.2.3	V	V	V
A.17 營運持續管理之資訊安全層面				A.14	A.14			
控制目標	A.17.1	資訊安全持續		A.14.1	A.14.1			
控制項	A.17.1.1	規劃資訊安 全持續	施行單位應決定對其資訊安全之要求事 項，以及在不利情況下（例：危機或災 難期間），對資訊安全之持續性要求事 項。	A.14.1.1	A.14.1.1		V	V
	A.17.1.2	實作資訊安 全持續	施行單位應建立、文件化、實作及維持 過程、程序及控制措施，以確保在不利 情況期間所要求之資訊安全持續等級。	A.14.1.1	A.14.1.1 A.14.1.3		V	V

	A.17.1.3	查證、審查及評估資訊安全持續	組織應定期查證所建立及實作之資訊安全持續控制措施，以確保其於不良情況期間係生效及有效。	A.14.1.2	A.14.1.5		V	V
控制目標	A.17.2	多重備援						
控制項	A.17.2.1	資訊設備之可用性	應對資訊處理設施實作充分之多重備援，以符合可用性要求。				V	V
A.18 遵循性				A.6 A.15	A.15			
控制目標	A.18.1	對法律及契約要求事項之遵循		A.15.1	A.15.1			
控制項	A.18.1.1 (I/P)	適用之法規及契約的要求事項之識別	對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。	A.15.1.1	A.15.1.1	V	V	V
	A.18.1.2	智慧財產權	應實作適切程序，以確保遵循智慧財產權及專屬軟體產品使用之相關法律、法令及契約的要求事項。	A.15.1.2	A.15.1.2	V	V	V
	A.18.1.3	紀錄之保護	應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未授權存取及未經授權發布。	A.15.1.2	A.15.1.3	V	V	V
	A.18.1.4 (I/P)	個人可識別資訊之隱私及保護	應依適用之相關法令、法規中之要求，以確保符合個人可識別資訊之隱私及保護。	A.15.1.2	A.15.1.4	V	V	V
	A.18.1.5	密碼式控制措施(加密控制措施)的監管	應使用密碼式控制措施(加密控制措施)，以遵循所有相關的協議、法律及法規。		A.15.1.6			V
控制目標	A.18.2	資訊安全審查		A.6.1 A.15.2	A.6.1 A.15.2			
控制項	A.18.2.1 (I/P)	資訊安全之獨立審查	應依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全之作法及其實作（亦即資訊安全之各項控制目標、控制措施、政策、過程及程序）。	A.6.1.6	A.6.1.8	V	V	V
	A.18.2.2 (I/P)	安全政策及標準之遵循性	管理人員應以適切之資訊安全政策、標準及其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。	A.15.2.1	A.15.2.1	V	V	V
	A.18.2.3 (I/P)	技術遵循性審查	應定期審查資訊系統對組織之資訊安全政策及標準的遵循性。	A.15.2.2	A.15.2.2		V	V

附件 2 補充說明

一、 新增適用控制措施

1. 原規範為刪除之控制措施

控制項			原規 範	ISO 27001: 2005	適用單位		
					C	B	A
A.7.1.1	篩選	對所有可能被聘用者所進行之背景調查，應依照相關法律、法規及倫理，並應相稱於營運要求及其將存取之資訊保密等級及組織所察覺之風險聘用。		A.7.1.2		V	V
A.7.1.2	聘用條款及條件	施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。		A.7.1.3	V	V	V
A.8.3.3	實體媒體傳送	應保護含有資訊之媒體在傳送時，不受未經授權的存取、誤用或毀損。		A.10.8.3		V	V
A.9.1.1 (I/P)	存取控制政策	存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。		A.11.1.1		V	V
A.9.3.1 (I/P)	秘密鑑別資訊之使用	於使用秘密鑑別資訊時，應要求使用者遵循施行單位之實務規定。		A.11.3.1	V	V	V

適用說明

A.7.1.1 篩選

原規範因鑒於施行單位在人員篩選上的實行度相當低，故將此項刪除，以簽訂完善之保密條款代替。然因個人資料保護法與法令法規施行與資訊安全要求應評估其能力與背景適用程度，施行單位仍須因應對其人員與委外廠商人員進行適當評估，故建議納入本控制項。

A.7.1.2 聘用條款及條件

原規範以保密協議或條款涵蓋資訊安全責任，將 A.6.1.5 保密協議與 A.8.1.3 聘用條件與限制合併，ISO 27001:2013 版，原 A.6.1.5 保密協議改為 A.13.2.4 機密性或保密協議，應識別、定期審查及文件化，以反映施行單位對資訊保護之需要的機密性或保密協議之要求事項。以資訊傳輸之保密要求事項為主，未完全包含 A.7.1.2 聘用條款及條件中要求施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。故建議納入所有等級之控制措施。

A.8.3.3 實體媒體傳送

原規範以「一般施行單位鮮少有運送重要儲存媒體之情事，加上存取控制，應無未授權侵入之可能；若為移動式儲存媒體，亦有限制未授權存取的規定，無須特地規範運送安全之條款。」刪除本控制項，然現今異地備份需求與利用儲存媒體進行資訊傳輸作業日益頻繁，其媒體管制與保護的要求已逐漸成為施行單位必要措施，故建議將此控制項納

入。

A.9.1.1 存取控制政策

原規範說明因「有關存取控制的各個管理措施，在存取控制安全的其他項目皆有規範，因此將此兩項屬原則性質之內容，修改為存取控制安全的釋句，不作為獨立的規範」而刪除本控制項，然以各施行單位於各項存取控制措施規劃時，均須依據單位資訊資產存取控制原則規劃，為免各承辦人員對於存取管理產生標準不一致狀況，建議重新納入本控制項。

A.9.3.1 秘密鑑別資訊之使用

原規範說明「此部份與系統管理者於管理使用者通行碼的內容相同，由於多數限制設定可由系統功能上完成，因此將此項刪除。」然有關使用者對於秘密鑑別資訊之使用，仍由其保管與維護之要求，且上級機關對於如通行碼等秘密鑑別資訊均有使用者設定或保管的要求，故建議仍列入控制項。

2. ISO 27001:2013 新增或修訂後納入之控制措施

控制項			原規範	ISO 27001: 2005	適用單位		
					C	B	A
A.14.2.5	保全系統工程原則	保全系統之工程原則，應予建立、文件化、維持及應用於所有資訊系統實作工作。	A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.4	A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.4		V	V
A.15.1.1 (I/P)	供應者關係之資訊安全政策	應與供應者議定並文件化，降低與供應者存取施行單位資產關聯之風險的資訊安全要求事項。				V	V
A.16.1.4 (I/P)	資訊安全事件評估及決策	應評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故。			V	V	V
A.16.1.5 (I/P)	對資訊安全事故之回應	應依文件化程序，回應資訊安全事故。			V	V	V
A.17.2.1	資訊設備之可用性	應對資訊處理設施實作充分之多重備援，以符合可用性要求。				V	V

適用說明

A.14.2.5 保全系統工程原則

ISO 27001:2013 標準條文將系統發展條文中較為技術性的要求如 A.12.2.1 資料輸入之驗

證、A.12.2.2 系統內部作業處理之驗證、A.12.2.3 訊息真確性之鑑別、A.12.2.4 資料輸出控管與 A.12.5.4 資訊洩漏控制等控制措施加以合併，並調整為由施行單位依據資訊應用系統特性規劃適用的系統設計工程原則，本項控制措施因相關控制措施原已適用於第一學群，建議加已納入。

A.15.1.1 供應者關係之資訊安全政策

由於近年來委由供應商進行資訊服務提供的情況越來越普及，且個人資料保護法等相關法規要求將委外管理納入監督，因此除對供應商說明資訊安全要求外，更應考量列入契約規範以強化資訊安全要求的強制性與監督的正當性，本控制項要求：「應與供應者議定並文件化，降低與供應者存取施行單位資產關聯之風險的資訊安全要求事項。」符合現有需求，故建議納入新增控制項。

A.16.1.4 資訊安全事件評估及決策

資訊安全事件之因應因先針對資訊安全事件狀態與等級進行評估後，才能給予適當的回應，且教育部資通安全處理小組作業說明柒.資安事件影響等級及資安通報應變處理流程，已針對資訊安全事件劃分等級與處理順序，因此建議配合實際作業，納入本控制項。

A.16.1.5 對資訊安全事故之回應

教育部資通安全處理小組作業說明柒.資安事件影響等級及資安通報應變處理流程，已說明各單位對資訊安全事故之回應，且已經施行，故建議納入本控制項，以符實際狀況。

A.17.2.1 資訊設備之可用性

各單位對於資訊處理設備的營運持續計畫，大多以配合可用性的要求進行備援或備份措施的規劃，符合以本控制項應對資訊處理設施實作充分之多重備援，以符合可用性要求。故建議納入本控制項。

3. B 級單位「高」等級資訊系統應納入之控制措施

控制項			原規範	ISO 27001: 2005	適用單位		
					C	B	A
A.14.1.3	保護應用服務交易	應保護應用服務交易中涉及之資訊，以防止不完整的傳輸、誤選路(mis-routing)，未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。		A.10.9.2			V
A.14.2.1	保全開發政策	應建立軟體及系統開發之規則，並應用至施行單位內之開發。					V
A.14.2.6	保全開發環境	對涵蓋整個系統開發生命周期之系統開發及整合工作，施行單位應建立並適切地保護安全開發環境。					V

A.14.2.8	系統安全測試	於開發中，應實施安全功能之測試。					V
A.15.1.3 (I/P)	資訊及通訊技術供應鏈	與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險。					V

適用說明

A.14.1.3 保護應用服務交易

原規範認為 ISO 27001:2005 版標準有關線上交易之控制項，屬於電子商務的一環，且由應用系統的角度來看，電子商務可歸屬於此範圍中，另外連線單位尤其學校鮮少有類似的業務發生，予以刪除。然 ISO 27001:2013 版標準將本控制項改為保護應用服務交易，所指為對外應用服務交易的資訊安全，「高」安全等級資訊應用系統資料多為敏感或機密性資料，對外進行資訊交易或傳輸必須確保不會發生不完整的傳輸、誤選路（mis-routing），未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演等資安事故，故建議納入本控制項，已進行應用服務交易保護的安全規格分析。

A.14.2.1 保全開發政策/A.14.2.6 保全開發環境/A.14.2.8 系統安全測試

此三項為 ISO 27001:2013 版新增控制措施，用以確保資訊應用系統於發展階段起即獲得安全保障，雖以現有教育體系承辦人員與開發環境勢必需要加以規劃與安排才能完成此三項控制措施，但就資訊安全風險而言，「高」安全等級資訊應用系統多處理敏感或機密性資料，需要確認該應用系統各發展階段的安全性，因此建議將此三項控制措施配合「高」安全等級資訊應用系統，以資訊應用系統適用方式納入適用控制措施。

A.15.1.3 資訊及通訊技術供應鏈

此項為 ISO 27001:2013 版新增控制措施，用以確認與供應者協議中，納入資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險的因應責任與控制措施。由於近來資訊及通訊產品與技術以供應鏈方式的產品與服務提供已是常態，且個人資料保護法等相關法規中有關委外管理已將分包商、技術原廠、產品零組件供應商等複委託廠商納入監督要求，因此本項控制措施有其執行必要性，然考量教育體系各機構與學校的特性，本項控制措施尚待發展，因此由 A 級單位與「高」安全等級資訊系統之 B 級單位優先施行，B 級單位可以限定適用於「高」安全等級資訊系統。

二、刪除之適用控制措施

原規範	控制項		ISO27001: 2005	ISO27001: 2013
A.6.1.2	資訊設施使用之授權	資訊處理設備的移轉(包含新設備)，應由權責主管人員進行授權、移交的程序，確保該設備後續的順利運作以及責任所屬。	A.6.1.4	刪除
A.10.7.3	資料檔案之保護	重要資料檔案應進行控管，並安全的保存。	A.10.7.3	刪除
A.10.7.4	系統文件之安全	重要系統文件應受到保護，避免未授權之存取。	A.10.7.4	刪除
A.11.3.2	遠端使用者身份鑑別	遠端連線使用者之存取需進行身份鑑別。 —較適用於第一群	A.11.4.2	併入 A13.1.1
A.11.3.3	診斷埠 (Diagnostic Ports)存取控制	診斷埠的存取行為必須嚴密控管。 —較適用於第一群	A.11.4.4	併入 A13.1.1
A.11.3.4	網路分隔控制	網路應視需求控制措施，將資訊服務、使用者及各資訊系統區隔。 —較適用於第一群	A.11.4.5	併入 A13.1.1
A.11.3.5	網路連線控制	使用者連線能力應視需求予以限制。 —較適用於第一群	A.11.4.6	併入 A13.1.1
A.11.3.6	網路路由控制	共享網路應有路由控制措施，確保電腦連線及資訊流依循應用系統之存取控管政策。 —較適用於第一群	A.11.4.7	併入 A13.1.1
A.11.4.4	連線作業時間之控制	必要時限制使用者在高風險應用系統的連線作業時間。 —較適用於第一群	A.11.5.6	併入 A13.1.1
A.11.5.2	機密及敏感性系統之獨立作業	必要時對機密性及敏感性系統，考量建置獨立的或是專屬的電腦作業環境。 —較適用於第一群	A.11.6.2	併入 A.12.1.4
A.12.2.1	資料輸入之驗證	輸入應用系統之資料須確認其正確性與適當性。	A.12.2.1	併入 A.14.2.5
A.12.2.2	系統內部作業處理之驗證	系統需建立確認檢查機制，以偵知所處理資料的塗改。	A.12.2.2	併入 A.14.2.5
A.12.2.3	訊息真確性之鑑別	必要時應採用訊息鑑別機制，保護訊息內容的完整性。 —較適用於第一群	A.12.2.3	併入 A.14.2.5
A.12.2.4	資料輸出控管	應用系統的資料輸出需經過確認，確保處理程序的正確性與適當性。	A.12.2.4	併入 A.14.2.5

A.12.5.4	資訊洩漏控制	預防施行單位資訊遭洩漏的危機，制定適當的控管措施。 —較適用於第一群	A.12.5.4	併入 A.14.2.5
A.15.3.2	系統稽核工具之保護	系統稽核之相關工具需建立適當的保護措施，並視需求設立備援及緊急應變方案。	A.15.3.2	刪除

三、 新舊版本對照表

A.5.1	資訊安全管理指導方針		A.5.1	資訊安全政策訂定與評估	
A.5.1.1 (I/P)	資訊安全政策	資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。	A.5.1.1	資訊安全政策制定	資訊安全政策應參考資安相關法令及施行單位業務上的需求，並經由管理階層核准，以適當方式向所有員工公佈與宣導，在必要時告知相關單位及合作廠商，以利共同遵守。
A.5.1.2 (I/P)	資訊安全政策之審查	資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。	A.5.1.2	資訊安全政策評估	面對資安事件的發生、資安相關法令與其他影響因素的改變時，資訊安全政策應進行即時的評估，並定期審查政策的可行性與有效性。
A.6.1	內部組織		A.6.1	資訊安全組織推動與權責	
A.6.1.1 (I/P)	資訊安全之角色及責任	應定義及配置所有資訊安全責任。	A.6.1.1	資訊安全組織推動以及權責之分配	由管理階層舉辦定期之資訊安全會報，召集相關單位代表進行工作與責任的分屬，確保資安相關計畫的進行，並展現管理階層的支持。
			A.8.1.1	所屬角色與責任	施行單位之員工、廠商及第三方使用者的資訊安全角色及責任應適需求以書面或其他方式清楚定義，並與資訊安全政策一致。
A.6.1.2	職務區隔	衝突之職務及責任範圍應予以區隔，以降低組織資產遭未經授權或非蓄意修改或誤用之機會。	A.10.1.3	資訊安全責任之分散	職務與責任範圍需予區分，降低資訊或服務遭未經授權修改或誤用之機會。
A.6.1.3	與權責機關之聯繫	應維持與相關權責機關之適切聯繫。	A.6.1.4	跨單位合作及協調	為確保資訊安全作業的順利運行，需與執法機關、主管機構、資訊服務廠商及電信公司建立適當的溝通管道。

A.6.1.4	與特殊關注方之聯繫	應維持與各特殊關注方或其他各種專家安全論壇及專業協會之適切聯繫。	A.6.1.5	資訊安全諮詢與顧問	在必要時，須向單位內部專業人員或外部專業諮詢人員徵詢、協調資訊安全建議。	
A.6.1.5	專案管理之資訊安全	不論專案之型式，應在專案管理中因應資訊安全。				
A.6.2	行動裝置及遠距工作		A.11.6	行動式電腦作業與遠距工作管理		
A.6.2.1	行動裝置政策	應採用政策及支援之安全措施，以管理因使用行動裝置所導致之風險。	A.11.6.1	行動式電腦作業控制	必要時應針對行動式電腦設施制定適當的控制措施及政策。	V
A.6.2.2	遠距工作	應實作政策及支援之安全措施，以保護存取、處理或儲存於遠距工作場所之資訊。	A.11.6.2	遠距工作管理	施行單位應制定遠距工作活動的政策、流程及標準，控管相關活動的進行。	V
A.7.1	聘用前		A.8.1	聘任前之處理		
A.7.1.1	篩選	對所有可能被聘用者所進行之背景調查，應依照相關法律、法規及倫理，並應相稱於營運要求及其將存取之資訊保密等級及組織所察覺之風險聘用。				
A.7.1.2	聘用條款及條件	施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。				
A.7.2	聘用期間		A.8.2	聘用中之處理		
A.7.2.1	管理階層責任	管理階層應要求所有員工及承包者，依施行單位所建立政策及程序施行資訊安全事宜。				
A.7.2.2	資訊安全認知、教育及訓練	施行單位內所有員工及相關之承包者，均應接受及其工作職務相關的組織政策及程序之適切認知、教育及訓練，並定期更新。	A.8.2.1	資訊安全教育訓練	施行單位內所有員工、合作廠商與第三方使用者應接受適當之資安訓練與有關資安政策、程序之宣導課程。	
A.7.2.3	懲處過程	應具備正式即已傳達之懲處過程，以對違反資訊安全之員工採取行動。	A.8.2.2	違反規定之處理	依據既定之條款或合約，違反施行單位之資訊安全政策與程序之人員，應予以適當之懲罰處理。	
A.7.3	聘用之終止及變更		A.8.3	結束聘任或改變職務		
A.7.3.1	聘用責任之終止或變更	應對員工及承包者定義、傳達於聘用終止或變更後資訊安全責任及義務仍保持有效，並執行之。	A.8.3.1	結束聘用之處理	負責執行結束聘用或改變職務之權責，其職掌應清楚定義並指派。	
A.8.1	資產責任		A.7.1	資訊資產分類與責任分屬		

A.8.1.1 (I/P)	資產清冊	應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。	A.7.1.1	資訊資產目錄建立	應製作所有資訊資產之清冊，並定期維護、更新。	
A.8.1.2	資產擁有權	清冊中所維持之資產應有擁有者。				
A.8.1.3	資產之可被接受的使用	對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。				
A.8.1.4	資產之歸還	所有員工及外部使用者於其聘用、契約或協議終止時，應歸還其據有之全部組織資產。	A.8.3.2	資產繳回	資產繳回應有正式的離職程序，顯示其已繳回單位資產。	
A.8.2	資訊分級					
A.8.2.1 (I/P)	資訊之分級	資訊應依法律要求、價值、重要性及其對未經授權揭露或修改之敏感性分級。	A.7.1.2	資訊安全等級分類	資訊資產應進行分級與標示，並考量重要資產的需求，於必要時制定保護措施及處理流程。	
A.8.2.2 (I/P)	資訊之標示	應依施行單位所採用之資訊級方案，發展及實作一套適切的資訊標示程序。				
A.8.2.3 (I/P)	資產之處置	應依施行單位所採用之資訊分級方案，發展及實作處置資產之程序。				
A.8.3	媒體處理		A.10.7	儲存媒體的處理與安全		
A.8.3.1 (I/P)	可移除式媒體之管理	應依施行單位所採用之資訊分級方案，實作管理可移除式媒體之程序。	A.10.7.1	電腦媒體之安全管理	電腦儲存媒體、可攜式媒體或印出報表，應制定控管措施。	V
A.8.3.2 (I/P)	媒體之汰除	當不再需要媒體時，應使用正式程序加以安全汰除。	A.10.7.2	電腦媒體處理之安全	應訂定電腦媒體的處理作業程序，以降低可能的安全風險。	
A.8.3.3 (I/P)	實體媒體傳送	應保護含有資訊之媒體在傳送時，不受未經授權的存取、誤用或毀損。				V
A.9.1	存取控制之營運要求事項					
A.9.1.1 (I/P)	存取控制政策	存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。				
A.9.1.2	對網路及網路服務之存取	應僅提供予使用者存取其已被特定授權使用之網路及網路服務。	A.11.3.1	網路服務之限制	施行單位須清楚限定使用者只能直接存取准許使用之服務。	V
A.9.2	使用者存取管理		A.11.1	使用者存取控制		

A.9.2.1 (I/P)	使用者註冊與註銷	應實作正式之使用者註冊及註銷過程，俾能指派存取權限。	A.11.1.1	使用者註冊管理	應制定正式使用者註冊、註銷流程和條款，以供存取資訊系統及服務。	
A.9.2.2 (I/P) (建議)	使用者存取權限之配置	應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。				V
A.9.2.3 (I/P)	具特殊存取權限之管理	應限制及控制具特殊存取權限之配置及使用。	A.11.1.2	系統存取特別權限管理	限制與控管特許權限的分配及使用方式。	
A.9.2.4 (I/P)	使用者之秘密鑑別資訊的管理	應以正式之管理過程控制秘密鑑別資訊的配置。	A.11.1.3	一般通行碼之控管	應建立使用者通行碼之管理制度。	
A.9.2.5 (I/P)	使用者存取權限之審查	施行單位應定期審查使用者存取權限。	A.11.1.4	系統存取權限之評估	施行單位應定期審查使用者存取權限。	V
A.9.2.6 (I/P)	存取權限之移除或調整	所有員工及外部使用者對資訊及資訊處理設施之存取權限，一旦其聘用、契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。	A.8.3.3	存取權移除	所有員工、合約商及第三方使用者的存取權限應根據既有的規範或協定進行移除或改變。	
A.9.3	使用者責任		A.11.3	使用者責任		
A.9.3.1 (I/P)	秘密鑑別資訊之使用	於使用秘密鑑別資訊時，應要求使用者遵循施行單位之實務規定。				
A.9.4	系統及應用存取控制		A.11.4	作業系統存取控制		
			A.11.5	應用系統的存取控制		
A.9.4.1 (I/P)	資訊存取限制	應根據存取控制政策，限制對資訊及應用系統功能之存取。	A.11.5.1	資訊存取限制	依資訊存取規定，配予應用系統的使用者與業務需求相稱的資料存取及應用系統的使用權限。	
A.9.4.2 (I/P)	保全登入程序	當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。	A.11.4.1	系統登入程序	使用者存取電腦系統應經由安全的系統登入程序。	
A.9.4.3 (I/P)	通行碼管理系統	通行碼管理系統應為互動式，並應確保嚴謹通行碼。	A.11.4.2	使用者通行碼管理	應以安全有效的使用者通行碼管理系統鑑別使用者身份。	
A.9.4.4	具特殊權限公用程式之使用	應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。	A.11.4.3	系統公用程式管理	系統上公用程式的使用，應予限制並控管。	V

A.9.4.5	對程式源碼之存取控制	應限制對程式原始碼之存取。	A.12.4.3	原始程式庫資源之存取控制	原始程式庫(Source Library)的存取必須採取嚴格的控制措施，避免在存取原始程式庫的程序中，造成原始程式庫的損毀。	
A.10.1	密碼式控制措施(加密控制措施)		A.12.3	加密控制措施		
A.10.1.1	使用密碼式控制措施(加密控制措施)政策	應發展及實作政策，關於資訊保護之密碼式控制措施的使用。	A.12.3.1	資料加密	必須發展加密控制措施保護資訊之政策。	V
A.10.1.2	金鑰管理(建議)	應加以發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。	A.12.3.2	憑證機構之技術安全	以一套公認之標準、流程及方法為金鑰管理系統之基礎，支援加密技術之運用。	V
A.11.1	安全區域		A.9.1	區域之安全		
A.11.1.1	實體安全周界	應定義及使用安全周界，以保護收容敏感或重要資訊及資訊處理設施之區域。	A.9.1.1	實體環境安全	施行單位應採用適當防護措施保障資訊處理設施所在區域(機房設備、人員辦公區域)的安全。	
A.11.1.2	實體進入控制措施	保全區域應藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。	A.9.1.2	人員進出控制	施行單位應實施控制措施，確保只有授權人員可以進出安全區域。	V
A.11.1.3	保全之辦公室、房間及設施	應設計資訊處理設施所在區域之實體安全並施行之。	A.9.1.3	資訊處理設施安全	在資訊處理設施所在區域工作，應採取適當的控制措施與指引，確保該區域的安全性。	V
A.11.1.4	防範外部及環境威脅	應設計並施行實體保護，以防範天然災害、惡意攻擊或事故。				V
A.11.1.5	於保全區域內工作	應設計及施行資訊處理設施所在區域內工作之程序。				V
A.11.1.6	交付及裝卸區(建議)	對諸如交付及裝卸區及其他未經授權人員可進入作業場所之進出點，應加以控制；若可能，應與資訊處理設施隔離，以避免未經授權之存取。				
A.11.2	設備		A.9.2	設備之安全		
A.11.2.1	設備安置及保護	應安置並保護設備，以降低來自環境之威脅及危害造成的風險，以及未經授權存取之機會。	A.9.2.1	設備安置地點之保護措施	施行單位應安置或保護設備，降低環境之威脅、災害以及未經授權存取所造成的可能損失。	V
A.11.2.2	支援之公用服務事業	應保護設備免於電源失效，及因其他支援之公用服務事業失效，所導致之中斷。	A.9.2.2	電源供應	施行單位應保護資訊處理設備，降低電力故障或異常的影響。	

A.11.2.3	佈纜安全	應保護通訊纜線及資訊處理設備之電源，降低受竊聽或破壞的可能損失。	A.9.2.3	電纜線安全防護	施行單位應保護通訊纜線及資訊處理設備之電源，降低受竊聽或破壞的可能損失。	V
A.11.2.4 (I/P)	設備維護	應正確維護設備，以確保其持續之可用性及完整性。	A.9.2.4	設備之維護	資訊處理設備應予以適當的維護，確保其持續運作。	
A.11.2.5 (I/P)	財產之攜出	未經事前授權，不得將設備、資訊或軟體帶出場域外。	A.9.2.6	預防未經授權之移動	施行單位所屬之設備、資訊或軟體未經授權禁止移動。	
A.11.2.6 (建議)	場所外設備及資產的安全	安全應適用於場域外資產，並將於施行單位場所外工作之不同風險納入考量。				
A.11.2.7 (I/P)	設備汰除或再使用之保全	含有儲存媒體之所有設備組件，於汰除前或再使用前應加以查證，以確保任何敏感性資料及有版權之軟體已被移除或安全地覆寫。	A.9.2.5	設備報廢與再使用	資訊處理設備在報廢或再使用的過程中，應避免內存資料的外洩，進行必要之清除動作。	
A.11.2.8 (建議)	無人看管之使用者設備	使用者應確保無人看管之設備具備適切保護。				
A.11.2.9	桌面淨空及螢幕淨空政策	對紙本及可移除式儲存媒體應採用桌面淨空政策，且對資訊處理設施應採用螢幕淨空政策。	A.11.2.1	桌面淨空安全管理	應考量採用辦公桌面的淨空政策，以減少文件及儲存媒體等在正常的辦公時間之外遭未被授權的人員取用、遺失、竄改或是被破壞的機會。	V
A.12.1	運作程序及責任		A.10.1	作業程序與責任		
A.12.1.1	文件化運作程序	運作程序應加以文件化，並使所有需要之使用者均可取得。	A.10.1.1	作業程序文件化	安全政策所規定之作業程序，應文件化並定期維護。	
A.12.1.2 (I/P)	變更管理	應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更。	A.10.1.2	作業變更之管理	資訊處理設施、系統之變更，應進行管制。	V
A.12.1.3	容量管理	各項資源之使用應受監視及調適，並對未來容量要求預作規劃，以確保所要求之系統效能。	A.10.3.1	系統作業容量之規劃	施行單位應適時預估系統容量需求，確保有充分處理資料與儲存的空間。	V
A.12.1.4	開發、測試及運作環境之區隔	應區隔開發、測試及運作之環境，以降低對運作環境未經授權存取或變更的風險。	A.10.1.4	系統發展、測試及實務作業之分散	開發或測試用之設備、軟體轉換至作業狀態，應制定規則分隔開來，並加以文件化。	V
			A.11.5.2	機密及敏感性系統之獨立作業	必要時對機密性及敏感性系統，考量建置獨立的或是專屬的電腦作業環境。 ——較適用於第一群	
A.12.2	防範惡意軟體		A.10.4	電腦病毒、惡意軟體		

A.12.2.1 (I/P)	防範惡意軟體之控制措施	應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。	A.10.4.1	電腦病毒及惡意軟體之控制	施行單位應進行防備電腦病毒與惡意軟體之偵測及預防的控制措施，以及使用者認知程序。	
A.12.3	備份		A.10.5	備份作業之管控		
A.12.3.1 (I/P)	資訊備份	應依議定之備份政策，定期取得資訊、軟體及系統的影像檔備份複本，並測試之。	A.10.5.1	資料備份	重要資訊與軟體應進行定期的備份。	V
A.12.4	存錄及監視		A.10.9	系統存取及應用之監督		
A.12.4.1 (I/P)	事件存錄	應產生、保存並定期審查記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。	A.10.9.1	事件記錄	建立及製作例外事件及資訊安全事項的稽核軌跡，並保存一段的時間，以作為日後調查及監督之用。	V
			A.10.9.2	系統使用之監控	為確保使用者只能執行授權範圍內的事項，應建立系統使用監督程序。	
			A.10.9.5	系統錯誤事項之紀錄	系統發生錯誤之事項時，應予以忠實的記錄，並進行適當的處理程序。	
A.12.4.2 (I/P)	日誌資訊之保護	應防範存錄設施及日誌資訊遭竄改及未經授權存取。	A.10.9.3	記錄的保護	單位應保護未授權的變更及防止記錄設備操作發生問題。	
A.12.4.3 (I/P)	管理者及操作者日誌	應存錄系統管理者及操作者之活動，且應保護及定期審查該日誌。	A.10.9.4	系統管理者與作業人員之記錄	應忠實紀錄系統管理者與作業人員之相關操作記錄。	V
A.12.4.4	鐘訊同步	組織或安全領域內所有相關資訊處理系統之鐘訊，應與單一參考時間源同步。	A.10.9.6	系統時鐘應予同步	應定期校正系統作業時間，維持系統稽核紀錄的正確性及可信度，最為事後法律上或是紀律處理上的重要依據。	
A.12.5	運作中軟體之控制					
A.12.5.1	運作中系統之軟體安裝	應實作各項程序，以控制對運作中系統之軟體安裝。	A.12.4.1	作業軟體控制	需建立作業系統各個軟體實施的管制程序，避免軟體影響作業系統之完整。	
A.12.6	技術脆弱性管理		A.12.6	系統弱點管理		
A.12.6.1	技術脆弱性管理	應及時取得關於使用中之資訊系統的技術脆弱性資訊、並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。	A.12.6.1	系統弱點控制	應及時取得有關針對系統弱點的資訊，並評估該弱點暴露的程度及所造成的可能危機。	V
A.12.6.2	對軟體安裝	應建立並實作使用者安裝軟體				

(建議)	之限制	之管控規則。				
A.12.7	資訊系統稽核考量		A.15.	系統稽核的考量		
A.12.7.1	資訊系統稽核控制措施	應仔細規劃並議定，涉及運作中系統之稽核要求事項及活動，以使營運過程中斷降至最低。	A.15.3.1	系統稽核控制	為避免作業系統稽核造成系統中斷的危險，應進行審慎、一致的規劃；必要時可向外部專家顧問尋求協助。	
A.13.1	網路安全管理		A.10.6	網路安全管理		
A.13.1.1	網路控制措施	應實施網路控制措施，維護網路安全。	A.10.6.1	網路安全規劃與管理	應實施網路控制措施，維護網路安全。	V
			A.11.3.2	遠端使用者身份鑑別	遠端連線使用者之存取需進行身分鑑別。 —較適用於第一群	
			A.11.3.3	診斷埠 (Diagnostic Ports) 存取控制	診斷埠的存取行為必須嚴密控管。 —較適用於第一群	
			A.11.3.4	網路分隔控制	網路應視需求控制措施，將資訊服務、使用者及各資訊系統區隔。 —較適用於第一群	
			A.11.3.5	網路連線控制	使用者連線能力應視需求予以限制。 —較適用於第一群	
			A.11.3.6	網路路由控制	共享網路應有路由控制措施，確保電腦連線及資訊流依循應用系統之存取控管政策。 —較適用於第一群	
A.13.1.2	網路服務之安全	應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外所提供。	A.10.6.2	網路服務之安全控制	使用公用或私用網路，應評估網路服務提供者之安全措施是否足夠，並提供明確的安全措施說明，另應考量使用該項網路對維持機關資料傳輸機密性、資料完整性及可用性等各種安全影響。	V
A.13.1.3	網路之區隔	應區隔各群組之資訊服務、使用者及資訊系統使用的網路。				V
A.13.2	資訊傳送		A.10.8	資訊與軟體交換		
A.13.2.1 (I/P)	資訊傳送政策及程序	應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。	A.10.8.1	資訊與軟體交換安全政策與協定	單位間交換資訊與軟體的行為(具機密性或敏感性內容)應有安全保護措施以及協議規範，	

					必要時制定正式合約。	
A.13.2.2 (I/P)	資訊傳送協議	協議應闡明組織與外部各方間營運資訊之安全傳送。	A.10.8.1	資訊與軟體交換安全政策與協定	單位間交換資訊與軟體的行為(具機密性或敏感性內容)應有安全保護措施以及協議規範，必要時制定正式合約。	
A.13.2.3 (I/P)	電子傳訊	應適切保護電子傳訊時所涉及之資訊。	A.10.8.2	電子郵件安全管理	應制定電子郵件使用政策，並實施控制措施降低安全風險。	V
			A.10.8.3	電子辦公系統安全	視需求應制定並實施控制措施，以管制和電子辦公系統有關之單位及安全風險。	
A.13.2.4 (I/P)	機密性或保密協議	應識別、定期審查及文件化，以反映施行單位對資訊保護之需要的機密性或保密協議之要求事項。	A.6.1.3	保密條款之簽訂	施行單位之員工(包含正職員工、臨時雇員)應簽署獨立或包含保密條款之合約，確保其了解應有之資安責任與相關限制。	
A.14.1	資訊系統之安全要求事項		A.12.1	系統安全要求		
A.14.1.1 (I/P)	資訊安全要求事項分析及規格	資訊安全相關要求，應納入新資訊系統或既有資訊系統之強化的要求事項中。	A.12.1.1	安全需求分析及規格訂定	應詳述新系統或既有系統之各項控制措施要求。	V
A.14.1.2	保全公共網路之應用服務	應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。	A.10.8.4	對外公告資訊之管理	對外公告資訊前應有正式授權程序，並避免未授權之竄改。	V
A.14.1.3 (建議)	保護應用服務交易	應保護應用服務交易中涉及之資訊，以防止不完整的傳輸、誤選路(mis-routing)，未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。				V
A.14.2	於開發及支援過程中之安全		A.12.5	開發與支援作業的控制		
A.14.2.1 (建議)	保全開發政策	應建立軟體及系統開發之規則，並應用至施行單位內之開發。				
A.14.2.2	系統變更控制程序	應藉由使用正式之變更控制程序，以控制開發生命週期內之系統變更。	A.12.5.1	變更作業之控制程序	實施變更作業應依循嚴格的變更管制措施。	V
A.14.2.3	運作平台變更後，應用之技術審查	當運作平台變更時，應審查及測試營運之關鍵應用，以確保對組織運作或安全無不利衝擊。	A.12.5.2	作業系統變更之技術評估	應用系統必須有所變更時，需進行必要之技術審核及測試。	V

A.14.2.4	軟體套件變更之限制	應不鼓勵修改軟體套件，且僅限於必要變更，並應嚴格控制所有變更。	A.12.5.3	套裝軟體變更限制	避免修改套裝軟體，有必要修改時需採取嚴格管制。	V
A.14.2.5	保全系統工程原則	保全系統之工程原則，應予建立、文件化、維持及應用於所有資訊系統實作工作。	A.12.2.1	資料輸入之驗證	輸入應用系統之資料須確認其正確性與適當性。	V
			A.12.2.2	系統內部作業處理之驗證	系統需建立確認檢查機制，以偵知所處理資料的塗改。	
			A.12.2.3	訊息真確性之鑑別	必要時應採用訊息鑑別機制，保護訊息內容的完整性。 —較適用於第一群	
			A.12.2.4	資料輸出控管	應用系統的資料輸出需經過確認，確保處理程序的正確性與適當性。	
			A.12.5.4	資訊洩漏控制	預防施行單位資訊遭洩漏的危機，制定適當的控管措施。 —較適用於第一群	
A.14.2.6 (建議)	保全開發環境	對涵蓋整個系統開發生命周期之系統開發及整合工作，施行單位應建立並適切地保護安全開發環境。				
A.14.2.7	委外開發	組織應監督及監視委外系統開發活動。	A.12.5.5	軟體委外開發	軟體之委外、使用需採取適當之管制及檢查。	V
A.14.2.8 (I/P) (建議)	系統安全測試	於開發中，應實施安全功能之測試。				
A.14.2.9 (I/P)	系統驗收測試	應建立新資訊系統、系統升級及新版本之驗收測試計畫及準則。	A.10.3.2	新系統上線作業之安全評估	新資訊系統、系統升級與新版本正式上線前應予以適當的測試，建立固定的驗收程序。	V
A.14.3	測試資料					
A.14.3.1	測試資料之保護	應小心選擇、保護及控制測試資料。	A.12.4.2	系統測試資料之保護	系統之測試資料須予以保護與控管。	
A.15.1	供應者關係中之資訊安全		A.10.2	資訊作業委外服務之安全管理		
A.15.1.1 (I/P)	供應者關係之資訊安全政策	應與供應者議定並文件化，降低與供應者存取施行單位資產關聯之風險的資訊安全要求事項。				
A.15.1.2 (I/P)	於供應者協議中闡明安全性	應與每個可能存取、處理、儲存或傳達資訊，或提供 IT 基礎建設組件資訊之供應者，建立及議	A.10.2.1	資訊作業服務之管控	施行單位執行資訊業務委外時，應與廠商簽訂適當的資訊安全協定及課予相關的安全管	

		定所有相關資訊安全要求事項。			理責任，納入契約條款。	
A.15.1.3 (I/P) (建議)	資訊及通訊 技術供應鏈	與供應者之協議，應包含因應與 資訊及通訊技術服務及產品供 應鏈關聯之資訊安全風險。				
A.15.2	供應者服務交付管理					
A.15.2.1 (I/P)	供應者服務 之監視及審 查	組織應定期監視、審查及稽核供 應者服務交付。	A.10.2.2	服務之監控 與審查	施行單位應監視和審查廠商提 供的服務，確保服務標準達到 協議的要求。	V
A.15.2.2 (I/P)	管理供應者 服務之變更	應管理供應者所提供服務之變 更，包括維持及改善既有的資訊 安全政策、程序及控制措施，並 考量所涉及之營運資訊、系統及 過程的關鍵性，以及風險之重新 評鑑。	A.10.2.3	廠商服務異 動	面對廠商服務異動的管理程 序，應注意相關的系統以及程 序，確實的掌控以避免導致新 資安危機。	V
A.16.1	資訊安全事故及改善之管理		A.13.1	資訊安全事件與弱點之通報		
A.16.1.1 (I/P)	責任及程序	應建立管理責任及程序，以確 保對資訊安全事故做迅速、有效 及有序之回應。	A.13.2.1	資安事件處 理責任與程 序建立	應建立處理資訊安全事件之作 業程序，並課予相關人員必要 的責任，以便迅速有效處理機 關資訊安全事件。	
A.16.1.2 (I/P)	通報資訊安 全事件	應循適切之管理管道，儘速通報 資訊安全事件。	A.13.1.1	資訊安全事 件與弱點通 報	資安事件需即刻進行通報。	
A.16.1.3 (I/P)	通報資訊安 全弱點	應要求使用資訊系統及服務之 員工及承包者，注意並通報任何 系統或服務中所觀察到或可疑 之資訊安全弱點。				
A.16.1.4 (I/P)	資訊安全事 件評估及決 策	應評鑑資訊安全事件，並決定是 否將其歸類為資訊安全事故。				
A.16.1.5 (I/P)	對資訊安全 事故之回應	應依文件化程序，回應資訊安全 事故。				
A.16.1.6 (I/P)	由資訊安全 事故中學習	應使用獲自分析及解決資訊安 全事故之知識，以降低未來事故 之可能性及衝擊。	A.13.2.2	從資安事件 中學習	監控並紀錄事件的過程與結 果，必要時進行檢討會議，討 論改善之事宜。	
A.16.1.7 (I/P)	證據之收集	組織應定義及應用程序，以識 別、蒐集、取得及保存可用作證 據之資訊。	A.13.2.3	資安事件證 據之收集	電腦稽核軌跡及相關的證據， 應以適當的方法保護。	
A.17.1	資訊安全持續		A.14.1	永續運作管理之規劃		

A.17.1.1	規劃資訊安全持續	施行單位應決定對其資訊安全之要求事項，以及在不利情況下（例：危機或災難期間），對資訊安全之持續性要求事項。	A.14.1.1	業務永續運作之規劃程序	施行單位應建立業務永續運作之程序及架構，鑑定測試以及維護之優先順序，訂定與維護永續運作之計畫。	V
A.17.1.2	實作資訊安全持續	施行單位應建立、文件化、實作及維持過程、程序及控制措施，以確保在不利情況期間所要求之資訊安全持續等級。	A.14.1.1	業務永續運作之規劃程序	施行單位應建立業務永續運作之程序及架構，鑑定測試以及維護之優先順序，訂定與維護永續運作之計畫。	V
A.17.1.3	查證、審查及評估資訊安全持續	組織應定期查證所建立及實作之資訊安全持續控制措施，以確保其於不良情況期間係生效及有效。	A.14.1.2	永續運作計畫之測試及更新	永續運作計畫應進行測試與維護，確保該計畫的有效性。	V
A.17.2	多重備援					
A.17.2.1	資訊設備之可用性	應對資訊處理設施實作充分之多重備援，以符合可用性要求。				
A.18.1	對法律及契約要求事項之遵循					
A.18.1.1 (I/P)	適用之法規及契約的要求事項之識別	對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。	A.15.1	法規之遵守		
A.18.1.2	智慧財產權	應實作適切程序，以確保遵循智慧財產權及專屬軟體產品使用之相關法律、法令及契約的要求事項。	A.15.1.1	適用法規之鑑別	蒐集相關法律條文(智慧財產權、資料隱私保護及其他相關法規)、管理規定及合約要求，了解與資訊處理設施、軟體系統的關係，並予以書面或其他方式留存。	
A.18.1.3 (I/P)	紀錄之保護	應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未授權存取及未經授權發布。	A.15.1.2	適用法規之遵循	需制定適當的流程與管制，保護重要紀錄，並確保遵守智慧財產權、個人資料保護及隱私等條文規範，防止資訊處理設施遭不當之使用。	
A.18.1.4 (I/P)	個人可識別資訊之隱私及保護	應依適用之相關法令、法規中之要求，以確保符合個人可識別資訊之隱私及保護。				
A.18.1.5 (建議)	密碼式控制措施(加密控制措施)的監管	應使用密碼式控制措施(加密控制措施)，以遵循所有相關的協議、法律及法規。				
A.18.2	資訊安全審查		A.15.2	安全政策與技術符合性之檢驗		

A.18.2.1 (I/P)	資訊安全之 獨立審查	應依規劃之期間或當發生重大 變更時，獨立審查組織對管理 資訊安全之作法及其實作（亦即 資訊安全之各項控制目標、控制 措施、政策、過程及程序）。	A.6.1.6	資訊安全政 策的獨立檢 視	機關制訂之資訊安全政策，應 進行獨立及客觀的評估。	
A.18.2.2 (I/P)	安全政策及 標準之遵循 性	管理人員應以適切之資訊安全 政策、標準及其他安全要求事 項，定期審查其責任範圍內之安 全處理及程序的遵循性。	A.15.2.1	確保遵守安 全政策與規 範	確保單位內所有區域或作業流 程皆定期審查及確保遵守安全 政策及規範。	
A.18.2.3 (I/P)	技術遵循性 審查	應定期審查資訊系統對組織之 資訊安全政策及標準的遵循性。	A.15.2.2	資訊系統符 合性審查	為確保資訊系統之運行符合既 定之安全實施標準，應進行定 期的審查，並予以書面或其他 方式留存。	

附錄 B

個人資料管理規範

本附錄列出之控制目標及控制措施乃參考 BS 10012:2009 第 3 節 3.3 至 3.5、3.6，第 4 節 4.1 至 4.3 及 4.7 至 4.17 列出之管理原則，並考量「教育機構個人資料保護工作事項」、「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」，與「教育體系個人資料安全保護基本措施及作法等要求」，並配合教育體系與相關單位之屬性與特點，保留符合各層級單位之項目。除第 4 節 4.6 與我國個人資料保護法律規範不符而略去外，標準其它要求均已整合至本規範本文中，以建構完整的 PDCA 管理循環。

施行單位應完全遵循本附錄所列要求，並得考量自身的需求與特性，考慮增加其他必要之控制目標及控制措施。各控制項將標示遵循之個人資料保護法與施行細則條文，同時並將國際標準條文標號標註於，附件 1 附錄 B 個人資料控制措施與各項標準對照表，以供參考。唯本附錄目標在對教育體系相關機構之個人資料管理產生引導作用，本規範之驗證作業目的為確認資通安全或個人資料管理系統有效執行，並無法律上免責的保證，教育體系機構如遇法律議題，其法規遵循性仍應由各機構提供符合性之法律證據與軌跡資料。

附註：控制項編號下(I/P)註記代表 ISMS 與 PIMS 可共用項目，並以規範建置步驟與附錄 A 控制項編號進行對照，俾便施行單位進行 PIMS 的建置作業，同時導入 ISMS 則應考量適用該共用項目以符合 ISMS 與 PIMS 的要求。

B.1

個人資料管理政策

管理階層透過的個人資料管理政策，表述對個人資料管理成效的期待、展現對個人資料管理制度的決心與支持。文件化的管理政策，易於持續發展並傳達予施行單位內外部人員知悉。透過管理方針的規劃與制定，讓全體人員體認管理階層對個人資料管理的重視程度。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.1 個人資料管理政策					
控制目標	B.1.1	個人資料管理方針		柒二(二) A5.1	
控制項	B.1.1.1 (I/P)	個人資料管理政策	核准並定期審查個人資料管理政策，展現管理階層對遵循個人資料保護法律及良好實務的承諾	柒二(二) A5.1.1 A.5.1.2	

實作指引

(一)個人資料管理方針(B.1.1)

1. 個人資料管理政策(B.1.1.1)

施行單位應訂定文件化的個人資料管理政策，經最高管理階層核定，並傳達至所有員工，以展現對遵循個人資料保護法律與良好實務的支持與承諾。個人資料管理政策應每年、依管理階層指示或重大變更發生時，重新審查。

個人資料管理政策之內容，宜包含以下資訊與承諾：

- (1) 僅基於施行單位合法目的下，進行必要的個人資料處理；
- (2) 僅針對特定目的蒐集最小化的個人資料，且不處理過多的個人資料；
- (3) 明確提供當事人其個人資料使用方式與對象的資訊；
- (4) 僅處理相關且適當的個人資料；
- (5) 公平與合法的處理個人資料；
- (6) 維護個人資料分類清冊；
- (7) 保持個人資料的正確性，並依需要保持最新；
- (8) 僅依法律或施行單位合法目的的要求下，保存個人資料；
- (9) 尊重當事人行使其當事人權利；
- (10) 維護所有個人資料的安全；
- (11) 僅在受到適當保護下，將個人資料傳輸至我國境外；
- (12) 個人資料保護法律所允許之例外情形的應用；
- (13) 發展與實施 PIMS，使政策得以實施；
- (14) 適當時，鑑別內外部關注方，及其參與 PIMS 的程度；
- (15) 明確界定員工在 PIMS 中之責任與歸責性。

B.2

個人資料管理組織

為於落實個人資料管理政策，施行單位應建立個人資料管理組織及管理窗口網絡，以促進各項管理程序與規範的正確執行。指定適當權責之高層主管人員肩負個人資料管理責任，除展示學校或單位落實個人資料管理的決心外，更能自管理階層的高度及管理邏輯，確保個人資料管理權責委派予適當同仁，並提供必要資源強化現行作業成效，以建立完善且安全之作業環境，降低個人資料管理風險。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.2 個人資料管理組織					
控制目標	B.2.1	內部組織		柒二 A.6.1	§18 細§12
控制項	B.2.1.1 (I/P)	管理階層角色及責任	應由管理階層負責個人資料管理，確保個人資料保護法令及良好實務的遵循	柒二(一) A.6.1.1	細§12
	B.2.1.2 (I/P)	日常作業管理責任	指派合格或具經驗的人員，確保日常作業符合個人資料管理相關政策的要求	柒二(三) A.6.1.1	§18 細§12
	B.2.1.3 (I/P)	個人資料管理專人	建立各單位的個人資料管理窗口，協助個人資料相關日常作業的執行	柒二(三) A.6.1.1	§18 細§12

實作指引

(一)內部組織(B.2.1)

1. 管理階層角色及責任(B.2.1.1)

個人資料管理人：學校、機構應由副首長擔任或指定，負責督導安全維護計畫訂定及執行之人員，以展示單位在遵循資料保護法律及最佳實務之決心。其職責應包含：

- (1) 核准個人資料管理相關政策；
- (2) 依個人資料管理相關政策發展與實施 PIMS；
- (3) 遵循個人資料管理相關政策執行安全與風險管理。

宜藉由包含處罰、員工教育訓練，或訂定與實施控管程序，要求所有人員遵循個人資料管理相關政策。

2. 日常作業管理責任(B.2.1.2)

個人資料管理人應指派並授權一位或多位受過個人資料管理訓練或具經驗之員工，擔任「個人資料管理小組」，負責：

- (1) 訂定及執行安全維護計畫，包括業務終止後個人資料處理方法。
- (2) 定期就個人資料檔案安全維護管理情形，向管理人提出書面報告。
- (3) 依據稽核人員就計畫執行之評核，於進行檢討改進後，向管理人及稽核人員

提出書面報告。

「個人資料管理小組」並應承擔下列日常作業政策的遵循責任：

- (4) 發展與審核個人資料管理相關政策；
 - (5) 確保政策的實施；
 - (6) 政策的管理審查；
 - (7) 依政策要求，進行訓練與持續性認知宣導；
 - (8) 個人資料處理程序之核准，例如：
 - a. 告知事項的管理與溝通；
 - b. 當事人權利行使的處理；
 - c. 個人資料的蒐集與處理；
 - d. 抱怨的處理；
 - e. 安全事故的管理；
 - f. 委外與國際傳輸管理。
 - (9) 協調組織內部風險管理與安全議題負責單位；
 - (10) 提供資料保護法令領域專家的意見與指引；
 - (11) 個人資料處理例外狀況的說明與應用；
 - (12) 提供資料分享方案相關建議(包含資料異地處理的安全議題)；
 - (13) 蒐集與資料保護法令相關之法律修訂及合適的指導綱要；
 - (14) 持續確認法律、實務與科技的變化對 PIMS 帶來的改變；
 - (15) 考量任何具強制或諮詢性單位針對個人資料處理所制定之法規，經評估其適用性後於施行單位內實行；
 - (16) 持續評估施行單位遵循資料保護法令與最佳實務之狀況，並適時加以調整。
- 個人資料稽核人員：同時學校、機構應由校長、機構負責人指定，負責評核安全維護計畫執行情形及成效之人員。

3. 個人資料管理專人(B.2.1.3)

若適用範圍涵蓋多個執行個人資料處理作業的單位，各單位應指定專人辦理單位內，以：

- (1) 擔任所屬單位的個人資料管理窗口；
- (2) 協助員工遵循個人資料管理相關政策執行日常作業。

B.3

人員認知與訓練

完善規劃的個人資料管理政策與作業程序，唯有透過建立人員對個人資料管理理念的認同、依職掌提供教育訓練，才能確保相關規範於每日例行工作的遵循與實踐。維持與外部團體的聯繫，以取得個人資料保護法律、良好實務及科技應用的最新資訊，則可用以評估並強化現行 PIMS 運行，進一步提高個人資料管理成效。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.3 人員認知與訓練					
控制目標	B.3.1	個人資料管理認知與教育訓練		柒四(二) A.7.2.2	細§12
控制項	B.3.1.1 (I/P)	政策認知訓練	透過政策認知訓練使個人資料管理成為核心價值與績效管理的一部分	柒四(二) A.7.2.2	細§12
	B.3.1.2 (I/P)	認知與教育訓練	透過訓練與宣導，使所有員工了解處理個人資料時應有的責任	柒四(二) 柒四(三) A.7.2.2	細§12

(一)人員認知與訓練(B.3.1)

1. 政策認知訓練(B.3.1.1)

為使個人資料管理成為施行單位核心價值與績效管理的一部分，施行單位宜：

- (1) 對全體教職員工進行每年至少三小時的教育訓練或宣導，來提高、強化與維持對個人資料管理政策的認知；得考量與資訊安全管理制度或其他既有的教育訓練規劃協同辦理；
- (2) 建立並實行教職員工個人資料管理政策認知評估方法，並留存評估紀錄；
- (3) 透過各種可能管道，對所有教職員工傳達下列項目的重要性：
 - a. 達成個人資料管理相關政策的目標；
 - b. 政策與作業流程的遵循；
 - c. 個人資料管理作業的持續改善。
- (4) 課程或宣導內容，宜包含教職員工對個人資料管理相關政策目標的達成的責任，以及造成不符合事項結果的影響。

宜藉由包含處罰、員工發展或控管程序的訂定與實施，要求所有人員遵循個人資料管理相關政策。

2. 個人資料管理責任認知與教育訓練(B.3.1.2)

所有個人資料管理相關人員應獲得適切的教育訓練，以確保：

- (1) 對個人資料管理與保護相關法律與良好實務充分瞭解，並具有執行個人資料管理責任的能力；

- (2) 知悉個人資料管理相關議題，並在適當時，透過與外部團體接觸，讓員工持續獲得個人資料相關議題的訊息；
- (3) 瞭解其應有的責任，使個人資料處理能依據核定程序，並考量相關的安全要求，加以保護及處理；
- (4) 能依適當程序處理個人資料；其訓練內容宜與職掌及角色責任有適當連結。

B.4

個人資料之識別與風險管理

為確保所持有之個人資料，其蒐集、處理、利用、儲存、委外處理等符合法令規範及本標準之管理原則，並受到適切的管理，定期盤點並維護個人資料清冊，依已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險，訂定適當之管控措施，從而得以訂定並持續強化個人資料管理作為。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.4 個人資料之識別與風險管理					
控制目標	B.4.1	個人資料之識別與維護		A.8.1 A.8.2	細§12
控制項	B.4.1.1 (I/P)	個人資料清冊	清查並維護個人資料清冊	A.8.1.1	細§12
	B.4.1.2 (I/P)	高風險個人資料	應鑑別高風險個人資料	A.8.2.1 A.8.2.2	細§12
控制目標	B.4.2	個人資料之風險管理		柒三(二) 柒五(二) 柒五(三)	細§12
控制項	B.4.2.1 (I/P)	風險管理	確保組織瞭解，特定類型個人資料處理時任何相關風險。	柒三(二) 柒五(二) 柒五(三)	細§12

(一)個人資料識別與維護(B.4.1)

1. 個人資料清冊(B.4.1.1)

施行單位應維護一份個人資料清冊，每年至少重新清查並更新一次，且內容應符合以下要求：

- (1) 確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。
- (2) 個人資料包含施行單位蒐集、處理、利用、保存之所有個人資料，不論其取得來源，及留存於施行單位的期間；
- (3) 清冊欄位至少包含個人資料名稱、個人資料類別、特定目的、適用的法律規定與保存期限，並明確標示個人資料流向。

施行單位可配合「附錄 A 資訊安全管理規範」A.8 資訊資產管理，進行資訊資產盤點，將個人資料列入資訊資產項目進行機密分級、標示與管理。

2. 高風險個人資料(B.4.1.2)

高風險或敏感個人資料應加以定義與識別，個人資料保護法第六條所限定蒐集之

個人資料應列於高風險個人資料；同時並應依據業務特性界定高風險或敏感個人資料類別。

所蒐集、處理、運用與保存之高風險或敏感個人資料，宜於個人資料清冊予以明確的鑑別與描述。

施行單位應依據「附錄 A 資訊安全管理規範」A.8 資訊資產管理，將高風險個人資料列入機密或敏感資料，並依據對應之機密等級進行標示與處置。

(二)個人資料之風險管理(B.4.2)

1. 風險管理(B.4.2.1)

個人資料風險評鑑應依據本規範柒、三規劃內所建議之風險評鑑與處理流程，與附件建議之風險評鑑方法來評估當事人因個人資料處理而可能面臨的風險等級，委外執行的個人資料管理作業也應納入風險評鑑項目。

風險評鑑流程中所識別的各項風險，應進行風險處理作業，以降低違反政策要求的可能性。

任何可能造成當事人損失或(及)困擾之個人資料處理流程，應於依據程序於管理審查活動中向個資管理人與個人資料風險擁有者進行陳報與審查。

B.5

公正與合法的處理

為確保施行單位公正且合法的處理個人資料，並於清楚識別法令上之各項要求，是落實「遵循個人資料保護法律及良好實務」承諾的基礎。此部分針對個人資料無論直接及間接的蒐集行為，及後續的個人資料處理過程，提供明確的作業流程設計與執行指引。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.5 公正與合法的處理					
控制目標	B.5.1	蒐集與處理			§8, §9
控制項	B.5.1.1	蒐集與處理 作業審查	定期審查作業流程，以確保公正且合法的蒐集與處理個人資料		§8, §9
控制目標	B.5.2	告知與同意			§8, §9 §17, §7, §15, §19
控制項	B.5.2.1	告知事項	告知事項應符合個人資料保護法令要求		§8, §9 §17
	B.5.2.2	告知或同意 作業程序	訂定管理程序，以確保告知作業之執行及執行證據保存		§8, §9 §17, §7, §15, §19

實作指引

(一) 蒐集與處理(B.5.1)

1. 蒐集與處理作業審查(B.5.1.1)

與個人資料相關之蒐集與處理作業流程，應於重大變更發生時，應進行審查確認：

- (1) 所蒐集、處理及利用之個人資料如包含特種個人資料，是否符合相關法令之要件。
- (2) 蒐集、處理個人資料之特定目的符合免告知之事由。
- (3) 蒐集、處理個人資料符合本法第十五或十九條規定，具有特定目的及法定要件，符合特定目的內利用
- (4) 利用個人資料符合本法第十六條或二十條第一項規定，於特定目的外利用個人資料時具備法定特定目的外利用要件。
- (5) 僅在特定目的內，公正且合法的蒐集與處理個人資料；列為公務機關之施行單位以依適當方式公開者為限；非公務機關者以告之或合於免告知特定目的為限。有變更者，亦同。
- (6) 僅在符合施行單位需求及個人資料保護法律規範下，處理特種個人資料；
- (7) 須告知事項或取得當事人同意時，其執行時機，應遵循個人資料保護法與相關

- 法律規範，並留存必要記錄；
- (8) 利用個人資料為宣傳、推廣或行銷時，應明確告知當事人其所屬學校、機構立案名稱及個人資料來源。
- (9) 首次利用個人資料為宣傳、推廣或行銷時，
- 應提供當事人表示拒絕接受宣傳、推廣或行銷之方式，並支付所需費用；
 - 當事人表示拒絕宣傳、推廣或行銷後，應立即停止利用其個人資料宣傳、推廣或行銷，並周知所屬人員；
 - 取得行銷同意時，同意書蒐集與保存要求。
- (10) 新建立的個人資料蒐集流程於啟用前，宜由個人資料管理小組(B.2.1.2)審查並留下紀錄，確保符合資料保護法律規範；
- (11) 宜依據個人資料風險等級，訂定處理與利用之作業過程得考量採取的保護要求，並於日常作業中遵循之；
- (12) 自第三方間接蒐集的個人資料，應確認其僅透過公平與合法方式取得。

(二) 告知與同意(B.5.2)

1. 告知事項(B.5.2.1)

施行單位如屬公務機關則應依個人資料保護法要求在全球資訊網等官方網站上公開個人資料檔案相關資訊。

施行單位如非公務機關或非為免告知事項，而應對當事人進行個人資料蒐集的告知或取得當事人書面同意時，其內容及執行時機，應遵循個人資料保護法律規範。

告知事項應依個人資料保護法第 8 條明確告知當事人相關資訊：

- － 機關名稱。
- － 蒐集目的。
- － 個人資料的類別。
- － 個人資料利用期間、地區、對象及方式。
- － 當事人行使之權利事項及方式等。
- － 當事人不提供個人資料對其權益之影響。

告知事項或書面同意內容宜納入下列考量：

- (1) 告知事項或書面同意內容宜配合法令、組織架構與作業程序的變動，重新審查並適度修訂告知事項內容；
- (2) 告知事項或書面同意內容宜設計版本識別方式，降低版本誤用的風險；
- (3) 宜以完整版本的告知事項或書面同意內容進行；如僅提供文件索引，索引資訊應足以引導使用者取得完整版本的告知事項；
- (4) 告知事項或書面同意內容應考量當事人特性，使當事人易於瞭解與取得；
- (5) 透過全球資訊網蒐集個人資料時，應說明於網頁上蒐集當事人資料之技術細節，及其他有關促使處理流程公平之資訊。

2. 告知或書面同意作業程序(B.5.2.2)

施行單位宜訂定告知作業執行程序，以確保：

- (1) 於蒐集、處理前執行告知事項或取得當事人書面同意

- (2) 執行告知事項與取得當事人書面同意作業，並依程序留存必要的作業紀錄；
- (3) 維持告知事項與取得當事人書面同意之各版本完整內容，於個人資料保存期限內予以留存；
- (4) 告知事項與當事人書面同之紀錄，應等同或超過個人資料留存之時間。

施行單位如由其他外部單位蒐集或取得個人資料亦應確保公平與合法地蒐集個人資料。如使應告知事項則確保於處理或利用前，向當事人告知 B.5.2.1 告知事項所列之項目。

B.6

個人資料特定目的處理

基於良善管理責任，施行單位為確保個人資料在處理、利用、資料分享等各種日常運作，均符合告知事項所陳述的特定目的，宜透過定期審查個人資料使用情形，於新增特定目的前取得當事人的同意。管理範圍不限於施行單位內部，還應包含資料分享第三方對個人資料的使用，亦不得超出特定目的之外。

透過不同類型的個人資料比對產出的資料，可解析出更多與當事人有關之訊息，並提高對當事人的識別程度，故應確保該比對符合特定目的及法令規範，且產出資料受到良好保護。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.6 個人資料特定目的處理					
控制目標	B.6.1	蒐集與處理特定目的			§15, §19 §16, §20
控制項	B.6.1.1	特定目的處理準則	個人資料僅於特定目的下處理與使用		§15, §19 §16, §20
	B.6.1.2	新特定目的同意	個人資料用於新增特定目的應取得當事人書面同意		§16, §20
控制目標	B.6.2	資料分享與揭露		A.13.2	§15, §19 §16, §20
控制項	B.6.2.1 (I/P)	資料分享規劃與協議	資料分享應符合法令規範，簽訂資料分享協議取得合法使用承諾，並留存可供稽核紀錄	A.13.2.1 A.13.2.2 A.13.2.3	§15, §19 §16, §20
	B.6.2.2 (I/P)	資料揭露程序	訂定管理程序，以確保僅於合法且必要情況下揭露個人資料	A.13.2.1 A.13.2.3	§15, §19 §16, §20
控制目標	B.6.3	資料比對			§15, §19
控制項	B.6.3.1	資料比對	透過資料比對而產出的個人資料，應確保其比對作業及使用，符合特定目的或法律要求		§15, §19

實作指引

(一) 蒐集與處理特定目的(B.6.1)

1. 特定目的處理準則(B.6.1.1)

施行單位宜訂定特定目的審查流程，以達成以下要求：

- (1) 審查個人資料處理與利用情形，確保於處理個人資料的過程中，不會產生違反或潛在違反任何法定義務情況，包含法令條文、一般法律或契約條款等；
- (2) 確保為特定目的所蒐集之個人資料不會用於其他目的，除非符合個人資料保護法第十六條或第二十條第一項特定目的外利用要件。

2. 新特定目的同意(B.6.1.2)

擬將個人資料用於新特定目的並須取得當事人書面同意時，應確保：

- (1) 新特定目的的同意，是出於自由意識的執行與告知；
- (2) 取得並保存當事人獨立意思表示之書面同意記錄。

(二)資料分享與揭露(B.6.2)

1. 資料分享規劃與協議(B.6.2.1)

將個人資料分享予第三方前，應規劃並執行以下作業：

- (1) 資料分享前應與其分享個人資料之單位簽訂正式協議書或契約等正式文件，以：
 - － 記載雙方於個人資料管理的責任；
 - － 於書面協議或契約中說明個人資料使用的目的，並限制或禁止為其他目的的進一步使用該個人資料；
- (2) 審查任何涉及將資料分享予第三方之新處理程序，於涉及新增的分享對象時，考量調整個人資料蒐集告知內容的必要性；
- (3) 確認資料分享不違反法律規範及契約義務，必要時於分享前取得當事人的書面同意；
- (4) 當資料分享符合個人資料保護法要求而不需取得當事人同意時，應考量留存可稽核的文件化紀錄。

2. 資料揭露程序(B.6.2.2)

施行單位應拒絕揭露所蒐集、處理與保存的個人資料之無關第三人請求。而基於法令規定，施行單位應於合法且必要的情境下(如：接獲法院命令)，向經驗證符合身分的有合法權限的機關或對象，揭露最小化的個人資料。

施行單位應訂定資料揭露處理相關程序，以達成：

- (1) 針對要求資料揭露的第三方，驗證其所宣稱的身分、存取個人資料權利及法源依據的真實性；
- (2) 於可行時，僅揭露最少數量的個人資料予第三方；
- (3) 留存資料揭露的作業紀錄，以追蹤個人資料揭露之軌跡，且應包含其合法證明。

(三)資料比對(B.6.3)

1. 資料比對(B.6.3.1)

將不同來源或特定目的取得的個人資料，進行比對而產出的個人資料，如透過多筆間接識別個人資料比對以產生的直接識別個人資料，其使用應符合特定目的或遵循相關法律要求。

B.7

適當相關與正確性

基於業務、作業流程與系統異動、部門分工調整，及教育機構法令與相關標準的變化等，依既有作業程序所蒐集與處理的個人資料，存在過度蒐集或處理的可能。透過定期審查現有作業程序，以確保僅在符合組織目的及於個人資料蒐集處理特定目的下，蒐集及處理必要的最少量的個人資料。

此外，個人資料因文字辨識或傳輸的錯誤、資料鍵入失誤、未獲通知的異動，或其他可能的原因，造成個人資料的錯誤或不完整。施行單位設計各項作業流程時，應將資料正確性納入考量，透過各種主動偵測、被動通知等不同手法，驗證個人資料的正確性，並於必要時保持更新。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.7 適當相關與正確性					
控制目標	B.7.1	適當性相關且不過度			
控制項	B.7.1.1	適當性管理	個人資料的蒐集與使用的適當性審查		
	B.7.1.2	相關且不過度管理	個人資料的蒐集與使用相關且不過度審查		
控制目標	B.7.2	個人資料正確性			§11
控制項	B.7.2.1	正確性管理	整合個人資料的正確性管理至作業流程中		§11
	B.7.2.2	錯誤資料的更正	應通知或更正提供予其他施行單位的個人資料的錯漏		§11
	B.7.2.3	新流程的審查	審查新流程或系統，確保其可達成個人資料正確性的維持		§11

實作指引

(一) 適當性(B.7.1)

1. 適當性管理(B.7.1.1)

施行單位應依議定的方式，每年審查個人資料蒐集與使用的適當性。審查時宜考量：

- (1) 檢視所蒐集的個人資料，對特定目的而言是適當的；
- (2) 個人資料的處理技術與流程，確保其持續適當性。

2. 相關且不過度管理(B.7.1.2)

施行單位應依議定的方式，每年重新審查一次所蒐集與使用的個人資料及相關作業流程，包含：

- (1) 僅在符合法令要求及特定目的要求下，處理最少量的個人資料；
- (2) 不處理超出告知事項的額外個人資料，除非已取得當事人書面同意；
- (3) 涉及個人資料處理之新系統、流程或作業表單，應審查處理之個人資料是相關且不過度的；
- (4) 宜考量於組織重大變更時，針對調整後的個人資料相關作業流程及表單進行審查，以確保其相關且不過度。

(二) 資料正確性(B. 7.2)

1. 正確性管理(B. 7.2.1)

施行單位於設計或調整個人資料相關作業流程時，應考量個人資料正確性的維護與保護，得採取的管理措施如下：

- (1) 設計所處理之個人資料的完整性與正確性保護方式，並藉以檢視管理個人資料於蒐集、處理或利用過程的正確性；
- (2) 宜整合各項個人資料管理作業流程，與當事人確認其個人資料正確性，並告知其當事人權利行使方式。
- (3) 當發現個人資料不正確時，應適時更正或補充；若該不正確可歸責於施行單位者，且可能影響個資當事人權益時，應通知曾提供利用之對象。
- (4) 允許當事人對其個人資料之正確性提出質疑，並在檢驗當事人身分及更正資訊之真實性後加以修正；
- (5) 個人資料正確性有爭議者，依個人資料保護法第十一條第二項規定處理之方式。
- (6) 向員工宣導正確記錄個人資料，並僅使用最新個人資料來做出有關當事人重要決策的重要性；

2. 錯誤資料的更正(B. 7.2.2)

施行單位主動或被動得知個人資料錯誤或非最新時，應：

- (1) 通知資料分享的第三方，不可使用於影響當事人權益的決策；
- (2) 依個人資料保護法律要求或情況允許時，傳遞正確之個人資料予第三方。

3. 新流程的審查(B. 7.2.3)

新增涉及處理個人資料的流程或系統，均應經過審查，以確認：

- (1) 其已盡可能避免記錄任何錯誤或過時的個人資料；
- (2) 允許修正錯誤或過時的個人資料。

B.8

保存與處置

留存超過保存期限的個人資料，除壓縮檔案儲存空間、降低資源使用效率外，亦可能導致個人資料管理風險的提高。而進入生命週期末段的個人資料，亦應監督其銷毀作業的執行，避免因不確實導致個人資料外洩，對當事人及施行機構聲譽帶來損失或困擾。本部分要求施行單位，應預先清查個人資料檔案的保存期限需求，規劃安全的個人資料銷毀管理程序與，以確保個人資料不會保存超過必要的時間。

本章節主要的內容可參照下表：				規範 附錄 A	個資法
B.8 保存與處置					
控制目標	B.8.1	保存與銷毀		柒四(四) A.8.3 A.11.2	§11
控制項	B.8.1.1 (I/P)	資料保存與 銷毀程序	施行單位應訂定個人資料保存與銷毀管理 相關程序	柒四(四) A.8.3 A.11.2	§11

實作指引

(一) 保存與銷毀 (B.8.1)

1. 資料保存與銷毀程序(B.8.1.1)

施行單位應訂定個人資料保存與銷毀管理相關程序，包括：

- (1) 根據單位及檔案屬性，相關法令及施行單位要求，訂定檔案保存要求與保存期限並經個人資料管理小組核可；
- (2) 定期(至少每年一次)檢視其所保有個人資料之特定目的是否消失，或期限是否屆滿；確認特定目的消失或期限屆滿時而無保存必要者，應依個人資料保護法第十一條第三項規定進行刪除、銷毀或其他停止蒐集等適當之處置。。
- (3) 個人資料銷毀作業之執行，應遵循文件銷毀程序，並採用適合個人資料風險等級的安全措施，且留存文件化作業紀錄。
- (4) 超過保存期限之個人資料，當基於正當理由暫不銷毀時，應造冊列管，清冊至少應包含超過保存期限之個人資料明細、保存之正當理由，與預定銷毀期限或條件。
- (5) 待銷毀資料應依其風險程度受適宜保護，且宜採標示或分區保管等避免與其他資料混淆之方式暫存。

B.9

當事人權利

依據個人資料保護法第三條規定，個人資料當事人具有查詢、提供閱覽、製給複製本、停止處理或利用、刪除個人資料等權利。施行單位應設計作業流程，使當事人得據以主張其權利，並於法定期限內獲得完滿回應與解決，是為尊重當事人權利的具體展現。

施行單位宜透過各種方式，偵知其於個人資料相關作業有無偏差。透過建立抱怨與申訴管道，完整蒐集當事人的抱怨與建議，除體現對當事人權利尊重外，更可有效發掘持續強化與改善的契機。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.9 當事人權利					
控制目標	B.9.1	當事人權利行使			§3, §10 §11, §13 , §14
控制項	B.9.1.1	當事人權利 行使程序	訂定管理程序，以確保當事人行使其法定權利		§3, §10 §11, §13 , §14
	B.9.1.2	抱怨與申訴 流程	受理並正確處理個人資料相關抱怨與申訴案件		

實作指引

(一) 當事人權利行使 (B.9.1)

1. 當事人權利行使程序(B.9.1.1)

施行單位應訂定當事人權利行使相關程序，包含：

- (1) 建立當事人權利行使聯絡窗口、聯絡方式，以及處理流程；。
- (2) 當事人權利行使流程應涵蓋處理個人資料的所有單位，以個人資料管理小組為管理單位，並由各單位個人資料管理專人擔任單位連絡窗口；
- (3) 依據個人資料保護法，明定個人資料當事人可行使的權利，及回覆時效；並同時建立當事人個人權利行使申請及執行進度，定期清查的流程。
- (4) 當事人權利行使受理，應確認是否為資料當事人之本人，或經其委託。
- (5) 應告知是否酌收必要成本費用及其收費基準，並遵守本法第十三條處理期限規定。
- (6) 如具有個人資料保護法第十條但書、第十一條第二項但書或第三項但書得拒絕當事人行使權利之事由，回覆時應說明法律依據及理由。
- (7) 當事人個人權利行使應留存可供稽核之執行紀錄；

2. 抱怨與申訴流程 (B.9.1.2)

施行單位應設計抱怨與申訴的受理處理流程，以確保有關個人資料處理之抱怨，得到正確的處理。

- (1) 定義接受當事人抱怨，與對抱怨處理方式提出申訴之窗口與流程；
- (2) 當事人抱怨與申訴之處理進度與結果，應每年至少清查一次，清查結果宜納入持續改善的考量。

B.10

資料安全議題

施行單位應考量個人資料型態及風險等級，透過實施適當技術面與施行單位面的安全控管措施，確保個人資料於處理、儲存與傳輸，均受到保護，免於發生遺失或毀損，及未經授權或非法的處理。

安全控制措施的設定，應綜合考量其施行單位特性、規模、人員特質及可運用資源，並應與施行單位流程結合以增加可行性。相關控制措施亦可參考本標準附錄 A，選用適當的安全控制措施。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.10 資料安全議題					
控制目標	B.10.1	安全控管措施		A.8~A.14 A.18	細§12
控制項	B.10.1.1 (I/P)	個人資料控 管措施	設定並審查個人資料蒐集、處理、儲存、傳輸與存取監控的安全控制措施或科技	A.8,A.11 A.12,A.13 A.14,A.18	細§12
	B.10.1.2 (I/P)	存取權限管 理程序	以正式程序最小化授予並審查個人資料存取權限	A.8,A.9 A.10	細§12
	B.10.1.3 (I/P)	安全控制措 施審查	定期審查安全控制措施的有效性	柒五(二) 柒六(二) A.18	細§12
控制目標	B.10.2	安全事故管理		A.16 A.12	細§12
控制項	B.10.2.1 (I/P)	安全事故管 理程序與紀 錄	訂定管理程序，以妥善處理安全事故並留存可供後續追查的紀錄	A.16 A.12.4	細§12

實作指引

(一) 安全控管措施(B.10.1)

1. 個人資料安全控管措施(B.10.1.1)

個人資料的蒐集、處理、儲存、傳輸與存取監控，應明確設定安全控制措施或科技，並考量：

- (1) 個人資料數量、類別、型態及外洩時對當事人造成的損失或困擾之風險；
- (2) 安全控制措施應與個人資料風險等級相當，如基於正當理由降低，應採取補償性控制措施；
- (3) 持續維護安全控制技術之正確性及功能適切性；

- (4) 個人資料對內及對外傳輸，應選用預先核准且符合個人資料風險等級的保全方式或科技，以防護傳送中的資料。

個人資料安全管控措施應包括下列事項：

A. 安全設備或防護措施

應依據「附錄 A 資訊安全管理規範」中下列控制領域或目標之控制項要求進行，其適用之控制項請參閱各控制項中個資適用條款編號：

- A.8 資產管理：個人資料處理、儲存與傳輸與其載體(如紙本、儲存媒體)之安全管理。
- A.11 實體及環境安全：個人資料處理、儲存與傳輸設備置放環境與維護管理。
- A.12 運作安全：個人資料處理設備日常管理、惡意軟體防治、備份、軌跡紀錄等管理。
- A.13 通訊安全：個人資料傳送政策與書面協議，以及傳送安全管理。
- A.14 系統獲取、開發及維護：涉及個人資料處理之資訊系統安全規格建立，測試要求，以及測試資料處理管理。

B. 人員安全措施：

應依據「附錄 A 資訊安全管理規範」中下列控制領域或目標之控制項要求進行，其適用之控制項請參閱各控制項中個資適用條款編號：

- A.6 資訊安全之組織：配合現有資訊安全管理組織，建立個人資料相關人員之角色與責任。
- A.7 人力資源安全：個人資料流程相關人員之管理，確保個人資料處理人員的責任、認知訓練，以及責任終止後的義務。

C. 業務終止後個人資料處理措施：

應配合「附錄 A 資訊安全管理規範」中 A.8 資產管理與 A.11 實體及環境安全中對於個人資料媒體與設備之汰除與處理要求執行，並確保建立：

- 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。
- 移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。
- 刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

D. 安全維護各項程序及措施執行紀錄，應包含：

- 個人資料之交付及傳輸。
- 個人資料之維護、修正、刪除、銷毀及轉移。
- 提供當事人行使之權利。
- 存取個人資料系統之紀錄。
- 備份及還原之測試。
- 所屬人員權限之異動。
- 所屬人員違反權限之行為。
- 因應事故發生所採取之措施。

- 定期檢查處理個人資料之資訊系統。
- 教育訓練。
- 安全維護計畫稽核及改善措施之執行。
- 業務終止後處理紀錄。

2. 存取權限管理程序(B.10.1.2)

施行單位應依據個人資料盤點與風險評鑑結果，訂定個人資料處理權限，個人資料之存取權限控制措施，應符合其風險等級，尤其是特種個人資料；所有個人資料的存取作業皆受到監控。

應依「附錄 A 資訊安全管理規範」中下列控制領域或目標之控制項要求進行，其適用之控制項請參閱各控制項中個資適用條款編號：

- (1) A.8 資產管理：個人資料處理、儲存與傳輸與其載體(如紙本、儲存媒體)存取權限管理。
- (2) A.9 存取控制：個人資料處理系統與設備之存取權限管理。
- (3) A.10 密碼學(加密控制)：個人資料處理、儲存與傳輸的加密措施。

3. 安全控制措施審查(B.10.1.3)

應訂定個人資料檔案安全稽核機制，或配合資訊安全管理系統稽核機制，每年或於重大變更後檢查個人資料安全控管措施是否落實執行。

並配合風險評鑑進行評估現行安全控制措施，確保：

- (1) 使用合適的流程、方法、科技與設備，並於必要時提供改善建議；
- (2) 已考量當安全事故發生時，對當事人造成損失及困擾的風險。

(二) 安全事故管理(B.10.2)

1. 安全事故管理程序與紀錄(B.10.2.1)

施行單位應設置個資保護聯絡人員及重大個資事件單一通報與聯繫管道，將個資保護聯絡方式（如：電話、email）置於單位網站，以便利個資當事人提出申訴與救濟。

應依據「附錄 A 資訊安全管理規範」中 A.16 資訊安全事故管理各控制項要求建立個人資料安全事故管理與應變機制，在發生個人資料被竊取、洩露、竄改或其他侵害事故時，迅速處理以保護當事人之權益，並同時包含於查明事故發生原因及損害狀況後，以適當方式通知當事人。

發生安全事故時，宜依據「政府機關（構）資安事件數位證據保全標準作業程序」或相關證據保全作業規範，進行數位證據之蒐集與保存。

B.11

國際傳輸

基於各國基礎設施完善程度不一，法令規範偏重各有差異，傳輸至其他國家的個人資料可能無法受到與在我國境內同等的保護。復以國際政治現實及國家產業發展策略，當中央目的事業主管機關對資料的國際傳輸有所疑慮，施行單位應確實遵循其規範或作業準則。本段落強調在進行國際傳輸之前，應釐清並遵循主管機關的觀點與要求、驗證資料接收單位具足夠的安全防護能力，以確保傳輸至國外的個人資料安全。

本章節主要的內容可參照下表：				規範 附錄 A	個資法
B.11 國際傳輸					§21
控制目標	B.11.1	國際傳輸管理		A.13.2	§21
控制項	B.11.1.1	境外管理協議與保護	傳輸至我國境外的個人資料應受到良好的管理	A.13.2	
	B.11.1.2	傳輸法令遵循	個人資料的傳輸應符合我國相關法律要求		§21

實作指引

(一) 國際傳輸管理(B.11.1)

1. 境外管理協議與保護(B.11.1.1)

個人資料傳輸至我國境外時，應確保：

- (1) 進行個人資料國際傳輸前，檢視有無中央目的事業主管機關依個人資料保護法第二十一條規定為限制國際傳輸之命令或處分，並應遵循之。
- (2) 簽訂書面協議或契約，以明訂管理責任，包含但不限於：個人資料傳輸與保存方式、使用與處理限制、資料銷毀要求等；
- (3) 資料傳輸方式及資料接收單位，已採用與資料風險等級相符的資料保全流程、設施與科技，並經個人資料管理小組(B.2.1.2)審查核可；
- (4) 可行時時，得考量於首次傳輸前，派員執行實地稽核；
- (5) 得考量建立協議範本，提供各執行單位參考或運用。

2. 傳輸法令遵循(B.11.1.2)

個人資料傳輸至我國境外時，施行單位應確保傳輸行為、協議或契約，符合我國相關法律及教育部之規範。

B.12

委外管理

為達成個人資料管理責任的可歸責性，當受委託機構處理或利用的個人資料發生外洩時，法律責任仍由委託機構承擔。本控制領域的目的，在於協助委託機構，透過受委託機構的篩選、明訂管理責任分配的合約及保留作業稽核權利等制度設計，有效管理受委託機構及作業委託衍生的風險，遵循個人資料保護法律及良好實務。相關控制措施亦可參考本標準附錄 A，選用適當的安全控制措施。

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.12 委外管理				A.15	細§8
控制目標	B.12.1	個人資料作業委外管理		A.15	細§8
控制項	B.12.1.1 (I/P)	委外管理程序	篩選及管理委外機構	A.15.1 A.15.2	細§8
	B.12.1.2 (I/P)	委外協議要項	於協議載明委外要求，以管理委外機構	A.15.1	細§8

實作指引

(一) 個人資料作業委外管理(B.12.1)

1. 委外管理程序(B.12.1.1)

個人資料委外管理應依據「附錄 A 資訊安全管理規範」中控制領域 A.15 供應者關係之所有控制項要求進行，其內容應包含個人資料安全管理要求，並符合個人資料保護法施行細則第十二條安全維護事項之要求。

當個人資料委託其他單位進行處理前，應：

- (1) 執行受委託機構評選，僅選擇可達成科技面、實體面及組織面安全要求的機構進行合作；
- (2) 與受委託機構簽訂委託管理協議，其內容應包含 B.12.1.2 委託協議要項與「附錄 A 資訊安全管理規範」A.15 供應者關係中資訊安全要求事項；
- (3) 需要時，如委託處理大量或特種個人資料，得考量於正式交付個人資料前，進行執行實地稽核。

2. 委託協議要項(B.12.1.2)

應依個人資料保護法施行細則第八條規定對受託者為適當之監督，並明確約定相關監督事項及方式。

委託協議內容應至少包含以下要求：

- (1) 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
- (2) 受委託機關的保密及安全管理責任，及安全事故責任歸屬；

- (3) 委託機構得對其作業流程及安全控制措施進行稽核；
- (4) 是否被允許分包個人資料處理作業；如允許分包，分包機構應至少執行與委託協議同等的安全控制措施；
- (5) 受託機構或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機構通知之事項及採行之補救措施。
- (6) 委託機構如對受託者有保留指示者，其保留指示之事項。
- (7) 委託關係終止或解除時，個人資料載體之返還，及受委託機構履行委託契約以儲存方式而持有之個人資料之刪除。
- (8) 其他我國個人資料保護法律要求的要項。

附件 1 附錄 B 個人資料控制措施與各項標準對照表

個人資料控制措施				規範 附錄 A	個資法	BS10012 :2009	ISO29100 :2011
B.1 個人資料管理政策							
控制目標	B.1.1	個人資料管理方針		柒二(二) A5.1		3.3 3.4	4.6
控制項	B.1.1.1 (I/P)	個人資料 管理政策	核准並定期審查個人資料管理政策，展現管理階層對遵循個人資料保護法律及良好實務的承諾	柒二(二) A5.1.1 A.5.1.2		3.3 3.4	4.6
B.2 個人資料管理組織							
控制目標	B.2.1	內部組織		柒二 A.6.1	§18 細§12		
控制項	B.2.1.1 (I/P)	管理階層 角色及責任	應由管理階層負責個人資料管理，確保個人資料保護法令及良好實務的遵循	柒二(一) A.6.1.1	細§12	3.5 4.1.1	
	B.2.1.2 (I/P)	日常作業 管理責任	指派合格或具經驗的人員，確保日常作業符合個人資料管理相關政策的要求	柒二(三) A.6.1.1	§18 細§12	4.1.2 4.5	
	B.2.1.3 (I/P)	個人資料 管理專人	建立各單位的個人資料管理窗口，協助個人資料相關日常作業的執行	柒二(三) A.6.1.1	§18 細§12	4.1.3	
B.3 人員認知與訓練							
控制目標	B.3.1	個人資料管理認知與教育訓練		柒四(二) A.7.2.2	細§12		
控制項	B.3.1.1 (I/P)	政策認知 訓練	透過政策認知訓練使個人資料管理成為核心價值與績效管理的一部分	柒四(二) A.7.2.2	細§12	3.7	
	B.3.1.2 (I/P)	認知與教育 訓練	透過訓練與宣導，使所有員工了解處理個人資料時應有的責任	柒四(二) 柒四(三) A.7.2.2	細§12	4.3	
B.4 個人資料之識別與風險管理							
控制目標	B.4.1	個人資料之識別與維護		A.8.1 A.8.2	細§12	4.2	4.2 4.3 4.4
控制項	B.4.1.1 (I/P)	個人資料 清冊	清查並維護個人資料清冊	A.8.1.1	細§12	4.2.1	4.2 4.3 4.4
	B.4.1.2 (I/P)	高風險個 人資料	應鑑別高風險個人資料	A.8.2.1 A.8.2.2	細§12	4.2.2	4.4

控制目標	B.4.2	個人資料之風險評鑑及管理		柒三(二) 柒五(二) 柒五(三)	細§12	4.4	4.5
控制項	B.4.2.1 (I/P)	風險評鑑	確保組織瞭解，特定類型個人資料處理時任何相關風險。	柒三(二) 柒五(二) 柒五(三)	細§12	4.4	4.5
B.5 公正與合法的處理							
控制目標	B.5.1	蒐集與處理			§8, §9	4.7	5.2 5.3
控制項	B.5.1.1	蒐集與處理作業審查	定期審查作業流程，以確保公正且合法的蒐集與處理個人資料		§8, §9	4.7.1 4.7.5	5.3
控制目標	B.5.2	告知與同意			§8, §9 §17, §7, §15, §19	4.7	5.2 5.3
控制項	B.5.2.1	告知事項	告知事項應符合個人資料保護法令要求		§8, §9 §17	4.7.1 4.7.4	5.3
	B.5.2.2	告知或同意作業程序	訂定管理程序，以確保告知作業之執行及執行證據保存		§8, §9 §17, §7, §15, §19	4.7.2 4.7.3	5.2 5.3
B.6 個人資料特定目的處理							
控制目標	B.6.1	蒐集與處理特定目的			§15, §19 §16, §20	4.8	5.2~4 5.6
控制項	B.6.1.1	特定目的處理準則	個人資料僅於特定目的下處理與使用		§15, §19 §16, §20	4.8.1	5.4
	B.6.1.2	新特定目的同意	個人資料用於新增特定目的應取得當事人書面同意		§16, §20	4.8.2	5.2 5.3
控制目標	B.6.2	資料分享與揭露		A.13.2	§15, §19 §16, §20	4.8.3 4.15	5.6
控制項	B.6.2.1 (I/P)	資料分享規劃與協議	資料分享應符合法令規範，簽訂資料分享協議取得合法使用承諾，並留存可供稽核紀錄	A.13.2.1 A.13.2.2 A.13.2.3	§15, §19 §16, §20	4.8.3	5.6
	B.6.2.2 (I/P)	資料揭露程序	訂定管理程序，以確保僅於合法且必要情況下揭露個人資料	A.13.2.1 A.13.2.3	§15, §19 §16, §20	4.15	5.6
控制目標	B.6.3	資料比對			§15, §19	4.8.4	5.6
控制項	B.6.3.1	資料比對	透過資料比對而產出的個人資料，應確保其比對作業及使用，符合特定目的或法律要求		§15, §19	4.8.4	5.6
B.7 適當相關與正確性							

控制目標	B.7.1	適當性相關且不過度				4.9	5.5 5.7
控制項	B.7.1.1	適當性管理	個人資料的蒐集與使用的適當性審查			4.9.1	5.5
	B.7.1.2	相關且不過度管理	個人資料的蒐集與使用相關且不過度審查			4.9.2	5.7
控制目標	B.7.2	個人資料正確性			§11	4.10	5.7
控制項	B.7.2.1	正確性管理	整合個人資料的正確性管理至作業流程中		§11	4.10	5.7
	B.7.2.2	錯誤資料的更正	應通知或更正提供予其他施行單位的個人資料的錯漏		§11	4.10	5.7
	B.7.2.3	新流程的審查	審查新流程或系統，確保其可達成個人資料正確性的維持		§11	4.10	5.7
B.8 保存與處置							
控制目標	B.8.1	保存與銷毀		柒四(四) A.8.3 A.11.2	§11	4.11	5.6
控制項	B.8.1.1 (I/P)	資料保存與銷毀程序	訂定管理程序，以確保個人資料保存與銷毀要求的落實	柒四(四) A.8.3 A.11.2	§11	4.11	5.6
B.9 當事人權利							
控制目標	B.9.1	當事人權利行使			§3, §10 §11, §13 , §14	4.12	5.9
控制項	B.9.1.1	當事人權利行使程序	訂定管理程序，以確保當事人行使其法定權利		§3, §10 §11, §13 , §14	4.12.1	5.9
	B.9.1.2	抱怨與申訴流程	受理並正確處理個人資料相關抱怨與申訴案件			4.12.2	5.9
B.10 資料安全議題							
控制目標	B.10.1	安全控管措施		A.8~A.14 A.18	細§12	4.13	4.7
控制項	B.10.1.1 (I/P)	個人資料控管措施	設定並審查個人資料蒐集、處理、儲存、傳輸與存取監控的安全控制措施或科技	A.8 A.11 A.12 A.13 A.14 A.18	細§12	4.13.1 4.13.2 4.13.3	4.7

	B.10.1.2 (I/P)	存取權限 管理程序	以正式程序最小化授予並審查個人資 料存取權限	A.8 A.9 A.10	細§12	4.13.4	4.7
	B.10.1.3 (I/P)	安全控制 措施審查	定期審查安全控制措施的有效性	柒五(二) 柒六(二) A.18	細§12	4.13.5	4.7
控制目標	B.10.2	安全事故管理		A.16 A.12	細§12		
控制項	B.10.2.1 (I/P)	安全事故 管理程序 與紀錄	訂定管理程序，以妥善處理安全事故 並留存可供後續追查的紀錄	A.16 A.12.4	細§12	4.13.6	4.7
B.11 國際傳輸							
控制目標	B.11.1	國際傳輸管理		A.13.2	§21	4.14	4.7
控制項	B.11.1.1	境外管理 協議與保 護	傳輸至我國境外的個人資料應受到良 好的管理	A.13.2		4.14	4.7
	B.11.1.2	傳輸法令 遵循	個人資料的傳輸應符合我國相關法律 要求		§21	4.14	5.12
B.12 委外管理							
控制目標	B.12.1	個人資料作業委外管理		A.15	細§8	4.16	4.7
控制項	B.12.1.1 (I/P)	委外管理 程序	篩選及管理委外機構	A.15.1 A.15.2	細§8	4.16	4.7
	B.12.1.2 (I/P)	委外協議 要項	於協議載明委外要求，以管理委外機 構	A.15.1	細§8	4.16	4.7

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 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) 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 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 (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 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 B.6.1.1 特定目的處理準則 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： (a) 機關名稱 (b) 蒐集目的 (c) 個人資料的類別 (d) 個人資料利用期間、地區、對象及方式 (e) 當事人行使之權利事項及方式等 (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 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： (a) 查詢或請求閱覽 (b) 請求製給複製本 (c) 請求補充或更正 (d) 請求停止蒐集、處理或利用 (e) 請求刪除			B.9.1.1 當事人權利行使程序 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： (a) 個人資料來源 (b) 機關名稱 (c) 蒐集目的 (d) 個人資料的類別 (e) 個人資料利用期間、地區、對象及方式 (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 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 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 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 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 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 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 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 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 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描病毒？		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 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 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 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 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？ (a) 因應事故發生所採取行為之紀錄 (b) 確認受託人執行委託人要求事項之紀錄 (c) 提供當事人行使權利之紀錄 (d) 確認資料正確性及更正之紀錄 (e) 權限新增、變動及刪除之紀錄 (f) 備份及還原測試之紀錄 (g) 個人資料交付、傳輸之紀錄 (h) 個人資料刪除、廢棄之紀錄 (i) 存取個人資料系統之紀錄 (j) 定期檢查處理個人資料之資訊系統之紀錄 (k) 教育訓練之紀錄 (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 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 7.1資源	3.5職責與歸責性 3.6 資源提供 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 4.3互動 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 附錄A 全 A.16資訊安全事故管理 A.17 營運持續管理 資訊 安全層面	4.7公平與合法的處理 4.13安全議題	4.6 隱私權政策 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 4.9 適當、相關且不過度 4.10正確性 4.11保存與處置 4.12個人權利 5.2管理審查	5.2當事人同意與選擇 5.3目的合法性明確化 5.4蒐集限制 5.5個資最小化 5.6使用、保存及揭露限制 5.7正確性與品質 5.8公開、透明及通知 5.9當事人權利 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 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 A.7人力資源安全	3.7將PIMS納入組織文化 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 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 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	

附錄 D

規範詞彙與定義

存取控制 ACCESS CONTROL

用以確保資產存取是基於營運與安全要求經授權且限制的方法。

ISO/IEC 27000:2014

可歸責性 ACCOUNTABILITY

個體對其行動與決策的職責

ISO/IEC 27000:2014

資產 ASSET

對於組織有價值的事物

備註：資產有很多類型，包含

- a) 資訊；
- b) 軟體，例如電腦程式；
- c) 實體，例如電腦；
- d) 服務；
- e) 人員，與他們的資格、技術與經驗；及
- f) 無形資產，如聲譽與形象。

ISO/IEC 27000:2014

可用性 AVAILABILITY

在獲授權個體要求時，可存取與使用的性質。

ISO/IEC 27000:2014

營運持續性 BUSINESS CONTINUITY

確保營運持續運作的程序與/或流程。

ISO/IEC 27000:2014

能力 COMPETENCE

已展現的知識與技術應用能力。

ISO 9000:2008

機密性 CONFIDENTIALITY

使資訊不可用或不揭露給未經授權個人、個體或流程的性質。

ISO/IEC 27000:2014

遵循性/符合 CONFORMITY

要求的符合程度。

ISO/IEC 27000:2014

後果 CONSEQUENCE

影響目標事件的結果。

備註 1：單一事件可導致多個後果。

備註 2：後果可是確定或不確定的，且在資訊安全領域通常只負向結果。

備註 3：後果可以質化或量化方式呈現。

備註 4：最初的後果可能藉由連環效應而升級。

ISO/IEC 27000:2014

持續改善 CONTINUAL IMPROVEMENT

重複執行的活動來增加符合要求的能力。

ISO 9000:2008

控制措施 CONTROL

包含政策、程序、指引、實務或組織架構等管理風險方法，其本質可為行政、技術、管理或法律。

備註 1：資訊安全控制措施，包含流程、政策、程序、指導綱要、實務或組織架構，以行政、技術、管理或法律等本質來減輕資訊安全風險。

備註 2：控制措施可能不一定都發揮預期或假設的減輕效果

備註 3：控制措施也用作保全或對策的同義詞。

ISO/IEC 27000:2014

矯正 CORRECTION

用以消除所偵測不符合事項的措施。

ISO 9000:2008

矯正措施 CORRECTIVE ACTION

消除所偵測不符合事項或其他非所欲情況的原因所採取的措施。

ISO/IEC 27000:2014

顧客 CUSTOMER

收取產品的組織或個人。

ISO 9000:2008

資料 DATA

用於基本量測值、衍生量測值與/或指標的數值集合。

ISO/IEC 27000:2014

文件化資訊 DOCUMENTED INFORMATION

組織被要求用來控制與維護的資訊，以及儲存該資訊的媒體

備註 1：文件化資訊可以存在於各種型式、媒體，以及來自各種來源。

備註 2：文件化資訊可參考管理系統及其相關流程；為了組織運作所產生的資訊(文件)；結果達成的證據(記錄)。

ISO/IEC 27000:2014

有效性 EFFECTIVENESS

實現所規劃活動與達成所規劃結果的程度。

ISO/IEC 27000:2014

效率 EFFICIENCY

達成結果與資源被使用之間的關係。

ISO/IEC 27000:2014

事件 EVENT

所發生或變更的一組特定情況。

備註 1：事件可有一或多個後果，也可能有多個原因。

備註 2：事件可以是某些事沒發生。

備註 3：事件有時可以是“事故”或“意外”。

ISO/IEC 27000:2014

外部環境 EXTERNAL CONTEXT

組織尋求目標達成的外部環境狀況。

備註：外部環境可包含：

- 國際、國家、區域或當地的文化、社會、政治、法律、法規、財務、科技、經濟、自然與競爭環境狀態；
- 對組織目標達成有影響的關鍵動力與趨勢；以及
- 外部利害相關者的關係及其認知與價值。

ISO/IEC 27000:2014

指標 INDICATOR

提供對基於已識別資訊需求的分析模型所導出的特定屬性進行預測或評估的量測值。

ISO/IEC 27000:2014

個人/當事人 INDIVIDUAL

個人資料的本人。

BS 10012:2009

資訊需求 INFORMATION NEED

用以管理目標、目的、風險與問題必要的理解。

ISO/IEC 27000:2014

資訊處理設施 INFORMATION PROCESSING FACILITIES

所有資訊處理系統、服務或基礎設施，或所放置的實體位置。

ISO/IEC 27000:2014

資訊安全 INFORMATION SECURITY

保存資訊之機密性、完整性與可用性。

備註：此外，也涉及其他性質如鑑別性、可歸責性、不可否認性與可靠性等。

ISO/IEC 27000:2014

資訊安全事件 INFORMATION SECURITY EVENT

系統、服務或網路發生一個已識別狀態，其可能顯示資訊安全政策漏洞或控制措施失效，或是先前可能與安全相關的未知情況。

ISO/IEC 27000:2014

資訊安全事故 INFORMATION SECURITY INCIDENT

單一或連串有顯著機率可能危害營運與威脅資訊安全之非所要或預期的資訊安全事件。

ISO/IEC 27000:2014

資訊安全事故管理 INFORMATION SECURITY INCIDENT MANAGEMENT

資訊安全事故之偵測、通報、評鑑、回應、處理及從中學習的流程。

ISO/IEC 27000:2014

資訊安全管理系統 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

整體管理系統的一部分，其依據營運風險方法，建立、實行、運作、監視、審查、維護與改善資訊安全。

備註：管理系統包含組織架構、政策、規劃活動、責任、實務、程序、流程與資源。

ISO/IEC 27000:2014

資訊系統 INFORMATION SYSTEM

應用系統、服務、資訊科技資產，或其他資訊處理元件。

ISO/IEC 27000:2014

基礎設施 INFRASTRUCTURE

組織運作所需的設施、設備與服務系統。

ISO 9000:2008

資訊 INFORMATION

有意義的資料。

ISO 9000:2008

完整性 INTEGRITY

保護資產的準確性與完整性的性質。

ISO/IEC 27000:2014

關注方 INTERESTED PARTY

對組織績效與成就有利益觀性的個人或群體。

ISO 9000:2008

內部環境 INTERNAL CONTEXT

組織尋求目標達成的內部環境狀況。

備註：內部環境可包含：

- 治理、組織架構、角色與責任；
- 政策、目標，與達成的策略；
- 能力，理解為資源與知識(如資金、時間、人員、流程、系統與科技)；
- 資訊系統、資訊流與決策流程(正式或非正式)；
- 內部利害相關者的關係，及其認知與價值；
- 組織文化；
- 組織採用的標準、指導綱要、與模型；及
- 契約關係的形式與內容。

ISO/IEC 27000:2014

風險等級 LEVEL OF RISK

風險嚴重程度，為後果與可能性的組合

ISO/IEC 27000:2014

可能性 LIKELIHOOD

事情發生的機會。

ISO/IEC 27000:2014

管理 MANAGEMENT

指導與管制組織的協調性活動。

ISO/IEC 27000:2014

管理系統 MANAGEMENT SYSTEM

為確保組織達成目標的指導綱要、政策、程序、流程與相關資源框架。

ISO/IEC 27000:2014

量測值 MEASURE

變數，作為量測結果的數值

備註：“量測值”一詞是基本量測值、衍生量測值與變數的通稱。

ISO/IEC 27000:2014

量測 MEASUREMENT

使用量測方法、量測函數、分析模型與決策準則來取得 ISMS 與控制措施有效性資訊的流程。

ISO/IEC 27000:2014

量測結果 MEASUREMENT RESULTS

一個或多個指標及其說明資訊需求的相關解釋。

ISO/IEC 27000:2014

監視 MONITORING

決定系統、流程或活動的狀態

ISO/IEC 27000:2014

不符合事項 NONCONFORMITY

未滿足要求。

ISO/IEC 27000:2014

不可否認性 NON-REPUDIATION

證明所宣稱事件或措施的發生及其原生個體之能力。

ISO/IEC 27000:2014

物件/對象 OBJECT

透過其屬性量測來描述的項目。

ISO/IEC 27000:2014

目標 OBJECTIVE

欲達成的結果

ISO/IEC 27000:2014

組織 ORGANISATION

具有責任、授權與關係人員與設施的安排組合。

ISO 9000:2008

處理個人資料的法律實體。

範例：自然人、獨資者、公司、合夥人、法人團體、公營機構，志願性組織和慈善機構。

BS 10012:2009

委外 OUTSOURCE

安排外部組織來執行組織的部分功能或流程

ISO/IEC 27000:2014

績效 PERFORMANCE

可量測的結果

ISO/IEC 27000:2014

個人資料 PERSONAL INFORMTION

可識別生存個人之相關資料。

BS 10012:2009

指自然人之姓名、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、社會活動及其他得以直接或間接方式識別該個人之資料。

個人資料保護法 第二條

特種個人資料

有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料。

個人資料保護法 第 6 條

個人資料管理政策 PERSONAL INFORMTION MANAGEMENT POLICY

說明組織整體意象，並經管理高層正式核准之聲明文件，用以維護及改善對個人資料保護法律及良好實務之遵循。

BS 10012:2009

個人資料管理系統 PERSONAL INFORMTION MANAGEMENT SYSTEM

部分有關建制、導入、作業、監控、審核、維護和改善個人資料的管理的整體框架。

BS 10012:2009

政策 POLICY

由理階層正式表達的整體意圖與指示。

ISO/IEC 27000:2014

預防措施 PREVENTIVE ACTION

用以消除潛在不符合事項或其他非所欲情況的原因所採取的措施。

ISO/IEC 27000:2014

程序 PROCEDURE

執行活動或流程的特定方式。

ISO/IEC 27000:2014

流程 PROCESS

一套由輸入轉換為輸出的相互關聯或交互作用的活動。

ISO/IEC 27000:2014

產品 PRODUCT

流程的結果。

ISO 9000:2008

紀錄 RECORD

敘述所達成的結果或提供執行活動證據的文件。

ISO/IEC 27000:2014

可靠性 RELIABILITY

預期的行為與結果一致的性質。

ISO/IEC 27000:2014

要求 REQUIREMENT

已陳述的需求或期望，通常為隱含的或義務的。

ISO 9000:2008

剩餘風險 RESIDUAL RISK

風險處理後所留存的風險。

備註 1：剩餘風險可包含未鑑別風險。

備註 2：剩餘風險也稱為“保留風險”。

ISO/IEC 27000:2014

審查/檢視 REVIEW

未決定主題事務達成目標的適合性、適當性與有效性所採取的活動。

ISO/IEC 27000:2014

風險 RISK

目標不確定性的影響

備註 1：影響為預期的正面與/或負面之偏離。

備註 2：目標可具有不同方面(如財務、健康與安全、資訊安全及環境目標)，並可應用於不同層面(如策略、整體組織、專案、產品及流程)。

備註 3：風險特性通常指潛在事件與後果，或前述兩種的結合。

備註 4：資訊安全風險通常以資訊安全事件的後果與相關發生可能性的組合來表示。

備註 5：不確定性是指對事件後果或可能性的理解或知識相關資訊全部或部分不足的狀態。

備註 6：資訊安全風險與威脅利用資訊資產脆弱性並對組織造成傷害的潛在性有關。

ISO/IEC 27000:2014

風險接受 RISK ACCEPTANCE

接受風險的決策。

ISO/IEC 27000:2014

風險分析 RISK ANALYSIS

理解風險本質並決定風險等級的流程。

備註 1：風險分析提供風險評估與風險處理決策的基礎。

備註 2：風險分析包含風險估計。

ISO/IEC 27000:2014

風險評鑑 RISK ASSESSMENT

風險識別、風險分析與風險評估的整體流程。

ISO/IEC 27000:2014

風險溝通與諮詢 RISK COMMUNICATION AND CONSULTATION

組織執行持續反覆的流程，已提供、分享或取得資訊，並著手與風險管理有關的利害相關者對話。

備註 1：資訊可能與風險的存在、本質、形式、可能性、重要性、評估、可接受性與處理有關。

備註 2：諮詢為組織與其利害相關者在議題上做成決策或決定方向前告知的雙向溝通流程。諮詢一詞意指：

- 與其使用強力不如透過影響力影響決策的流程；及
- 為決策的輸入項目，而非參與決策。

ISO/IEC 27000:2014

風險準則 RISK CRITERIA

用以評估風險顯著性的參考條件/用語。

備註 1：風險準則係依據組織目標與內外環境。

備註 2：風險準則可以由標準、法律、政策與其他要求衍生出來。

ISO/IEC 27000:2014

風險評估 RISK EVALUATION

比較風險分析結果與風險準則來決定風險與/或嚴重程度是否可接受或容忍的流程。

備註：風險評估可協助風險處理的決策。

ISO/IEC 27000:2014

風險識別 RISK IDENTIFICATION

發現、認識與描述風險的流程。

備註 1：風險識別包含風險來源、事件與其發生原因，以及可能後果的識別。

備註 2：風險識別可包含歷史資料、理論分析、接受告知與專家意見，以及利害相關者的需求。

ISO/IEC 27000:2014

風險管理 RISK MANAGEMENT

組織中有關風險的指示與控制的協調性活動。

ISO/IEC 27000:2014

風險管理流程 RISK MANAGEMENT PROCESS

溝通、諮詢、建立前後關係，以及識別、分析、評估、處理、監視與審查風險的管理政策、程序與實務的系統化應用。

ISO/IEC 27000:2014

風險處理 RISK TREATMENT

修正風險的流程

備註 1：風險處理可包含

- 決定不著手或繼續活動以避免風險；
- 接受或增加風險以尋求機會；
- 移除風險來源；
- 改變可能性；
- 改變後果；
- 分攤風險給其他團體(包含合約與風險資金支援)；及
- 藉由已告知的選擇來保留風險。

備註 2：處理負面後果的風險處理有時稱為“風險減輕”、“風險排除”、“風險預防”及“風險降低”。

備註 3：風險處理可創造新風險或修正現有的風險。

ISO/IEC 27000:2014

敏感性個人資料 SENSITIVE PERSONAL INFORMATON

與個人有關的個人資訊，如：

1. 種族或宗族；
2. 政治立場；
3. 宗教或其他信仰；
4. 工會會籍；
5. 身體及心理之健康狀況；
6. 性生活；
7. 犯罪或疑似犯罪，包括有關該犯罪或疑似犯罪的起訴、不起訴或判決確定資訊。

BS 10012:2009

高風險個人資料

對外揭露可能對當事人帶來重大影響的敏感性個人資料，如：

1. 個人資料保護法所稱特種個人資料；
2. 個人銀行帳戶與其他財務資訊；
3. 身分識別碼，如國民身分證統一編號、護照號碼等；
4. 弱勢成人與兒童之個人資料；
5. 個人特徵的詳細說明/個人基本資料。

BS 10012:2009/本規範

規範 SPECIFICATION

敘述要求的文件。

ISO 9000:2008

利害相關者 STAKEHOLDER

可影響、受其影響或自認會受到決策或活動影響的個人或組織。

ISO/IEC 27000:2014

適用性聲明書 STATEMENT OF APPLICABILITY

描述組織 ISMS 相關且適用的控制目標與控制措施的文件化聲明。

ISO/IEC 27000:2014

測試 TEST

依據程序來決定一或多個特性。

ISO 9000:2008

第三者 THIRD PARTY

當考量的議題有問題時，公認獨立於涉及的團體的個人或個體。

Person or body that is recognized as being independent of the parties involved, as concerns the issue in question

ISO/IEC 27000:2014

第三者稽核 THIRD PARTY AUDIT

由外部獨立稽核組織來執行組織的稽核，例如提供符合 ISO 27001 的要求的登錄或驗證的組織。

威脅 THREAT

非所欲事故的潛在原因，其可能導致系統或組織的傷害。

ISO/IEC 27000:2014

高階管理階層 TOP MANAGEMENT

指導與控制組織的最高層個人或團體。

ISO 9000:2008

量測單位 UNIT OF MEASUREMENT

依慣例界定與調整的特定量，與其他相同種類的量來比較，以說明量的規模。

ISO/IEC 27000:2014

脆弱性 VULNERABILITY

能被威脅利用的資產或控制措施的弱點。

ISO/IEC 27000:2014

人員 WORKER

在組織控管下工作的人員。

備註：包括受雇人、臨時人員、契約人員、志工與顧問。

BS 10012:2009