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。

附錄 B

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：

				規範条 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		条三(二) 条五(二) 条五(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。	条三(二) 条五(二) 条五(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，

a. 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；

b. 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；

c. 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。

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。而進入生命周期末段的個人資料，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		

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