教育體系資通安全管理規範

中 華 民 國 96 年 5 月 30 日

目　　錄

壹、緣起

網路的快速發展，改變了既有的業務處理模式，不單是業界，學校單位也感受到此股新興力量，許多行政工作藉由網路無遠弗屆的特性，加速了程序的進行，提升了整體的效率。然而，如同其他新興產業、領域碰到的問題一樣，相關的法令制定、控制規範，往往跟不上日新月異的變化，因此，不單只是產業界，其實學校單位對於通用性資通安全規範的需求，早時有所聞。鑑於實務界已經發展成熟的資安規範，如 CNS17799、ISP Guide73:2002、BS7799 等，此時此刻，正是為各級學校單位量身訂作規範的時機，如此才能確保各個行政程序的安全性。另外，考量到學校單位的重要性、急迫性以及可分配資源等因素，教育體系最適合進行資通安全管理規範的設計與施測；所以，本規範將以教育體系為對象，期能設計出最適合相關單位施行的管理規範。

貳、簡介

本規範之制定乃為提供教育體系及相關單位之管理階層、資訊業務人員及一般教職人員一套有效建置與管理資訊安全管理系統(Information Security Management System, 以下簡稱 ISMS)模式；評估各單位資安管理上的需求、目標、結果，並考量加入特有之作業程序、規模、架構等因素，量身訂做出有別於業界所採用之 ISMS 規範。為了讓施行資安管理單位能以花費最低成本、人力等資源，採漸進的方式逐步達成可行之規章條款，本規範強調實行度與執行效率，期望能將此資安規範及相關之實施經驗推行到各單位，進而強化 TANet 中各連線學校單位的資通安全。

參、適用範圍

本標準適用於教育部電算中心、部屬館所、縣市網中心、大專院校以及高中職資訊管理單位等資訊業務相關單位(或其他管理單位認為應加入 ISMS 規範範圍之部門)，針對「學術網路系統」以及「行政資訊系統」兩大業務範疇，訂定教育體系所屬機關、學校資訊安全管理規範，以提升資訊安全管理能力。有鑑於上述之單位，無論是層級、位置、規模有著不小的差異，為避免施行單位面對部分規範窒礙難行的問題，本標準將適用單位分為二群，群組屬性為：

一、 第一群：本群適用單位以教育部電算中心、部屬館所、縣市網中心以及公私立大專院校(計網中心及校務行政)等為主；本群所屬單位之特性，適用之規範須遵從較高的嚴謹度，除因規模較小或資源缺乏等限制得以轉換至第二群外，其他不得變更(除了原屬第二群之單位外)。

二、 第二群：本群適用單位以公私立高中職學校(資訊管理單位或因規模、資源

因素轉至本群者及校務行政)為主要對象；適用規範之嚴謹度較為寬鬆，乃為配合此群中所屬單位之規模與經費之故，但亦可根據自身的需求，轉往依循第一群之準則。

肆、目標期程

本規範的最終目標，在於讓所有教育體系與相關單位，在有限的資源下，建置最為合適、有效的 ISMS。有鑑於各單位在資訊業務管理上，受限於人力、經費等各項資源，加上建置 ISMS 過程中須與相關單位以及管理階層多加協調溝通；因此，各單位在正式建置 ISMS 時，建議採階段式進行，以三年為期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，而非耗盡內部資源全力投入的模式；藉由如此的模式，在不過於影響單位運作的情況下，成功建置合適的 ISMS。

伍、引用標準

本規範主要參考 ISO/IEC 27001:2005(E) ISMS 規範內的條款，再依據教育體系與相關單位的特性及需求，設計出較為合適的標準，希冀能有效提升各單位的資通安全程度。下列本標準之參考文件：

- 行政院及所屬各機關資訊安全管理規範。
- ISO/IEC 27001:2005(E) 規範。
- ISO/IEC 17799:2005 資訊技術—安全技術—資訊安全管理之作業要點。
- CNS17799 資訊技術—資訊安全管理之作業要點。

陸、關於適用性聲明(Statement of Applicability)

本標準之設計為適用於教育體系與相關單位，但鑑於類型、規模、資源、業務性質等因素，若本標準列出之任何條款無法適用於某單位時，可考慮予以排除，但必須在不影響該單位提供資訊安全能力與責任之情況下，並提出理由。在建置完該單位之 ISMS 後，必須提出符合的適用性聲明，其中應包含選擇之控制目標與控制措施項目與理由，以及排除條款之內容、理由，作為稽核時的依據。

柒、用詞解釋

- 資產(Asset)
  對組織有價值的任何事物。
  [CNS_(ISO/IEC 13335-1:2004)]

- 可用性(Availability)
  經授權個體因應需求之可存取及可使用的性質。
  [CNS_(ISO/IEC 13335-1:2004)]
- 機密性(Confidentiality)
  使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。
  [CNS_(ISO/IEC 13335-1:2004)]
- 資訊安全(Information Security)
  保存資訊的機密性、完整性及可用性。
  [CNS 17799:2002]
- 資訊安全事件(Information Security Event)
  系統、服務或網路發生一個以識別的狀態，其指示可能的資訊安全政策違例或保護措施失效，或是可能與安全相關而先前未知的狀況等。
  [CNS_(ISO/IEC TR 18044:2004)]
- 資訊安全管理系統(Information Security Management System, ISMS)
  整體管理系統的一部分，以營運風險導向(作法)為基礎，用以建立、實作、運作、監視、審查、維持及改進資訊安全。
  備考：管理系統包括組織架構、政策、規劃活動、職責、實務、程序、過程及資源。
  [CNS 17800:2002]
- 完整性(Integrity)
  保護資產的準確度(Accuracy)和完全性(Completeness)的性質。
  [CNS_(ISO/IEC TR 18044:2004)]
- 風險評估(Risk Evaluation)
  把估計的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。
  [CNS 14889]
- 適用性聲明(Statement of Applicability)
  描述與組織之ISMS相關且對其適用之各項控制目標與控制措施的已文件化聲明。
  [CNS 17800:2002]

捌、關於資訊安全管理系統(ISMS)建置步驟

本標準在於協助施行單位開發、實施、維護及持續改進一完善之ISMS，其可分為以下幾個步驟：

三、 ISMS之建立：依據該單位之類型、規模、資源、業務性質等特性，定義ISMS之範圍；考慮相關法律、法規以及合約之要求，於適度評估風險及應對措施後，訂出經由管理階層核准之ISMS政策，並擬定一份適用性聲明書文件。

四、 ISMS 之實施與操作：施行單位應確實實施控制措施，以符合控管的目標，並執行訓練與認知計畫，確保偵測安全事件的能力，以及迅速回應和應對處理的時效。

五、 ISMS 之監控及審查：施行單位應針對 ISMS 進行監控程序與其他控制措施，即時鑑別資安事件的發生、處理順序與解決方法；定期審查 ISMS 之有效性(建議一學年至少一次)，並將相關有顯著影響之活動與事件記錄下來。

六、 ISMS 之維持及改進：施行單位應定期實行改進活動，採取適當的矯正與預防措施，並得到管理階層之同意，並確保各項措施達到預期目標。

玖、關於資訊安全管理系統(ISMS)建置需求

七、 文件要求：關於 ISMS 文件化(電子檔案或紙本)，必須包含安全政策、安全目標、ISMS 範圍、適用性聲明、資安事件記錄以及其他有助於提升 ISMS 成效之文件；上述之文件需接受保護與管制，並定期的審查及更新，確保文件之最新版本；任何過其文件需保留或銷毀，應予以適當的鑑別。

八、 管理階層責任：施行單位之管理階層，最為重要的是給予承諾及實際的支持，並適度的提供資源以助 ISMS 程序的進行，必要時審查 ISMS 的控制措施與有效性；另外，確保於 ISMS 範圍內之員工，具備足夠之能力及認知，並定期進行教育訓練。

九、 管理階層審查：管理階層應在規劃期間內，審查該單位的 ISMS 與適用範圍，確保其持續的適用性、適切性及有效性；其中應審查包含變更需求與改進時機，並將其結果確實文件化。

十、 ISMS 之改進：ISMS 的改進是持續的，必須藉由各資安事件與審查結果，做出適度的反應與改進，持續系統之有效性；另外，對應的矯正措施以及防範未然的預防措施，亦須予以制定並文件化。

上述捌、玖兩節的規範，施行單位必須確實執行，不得因任合因素而有所簡化，甚至避免，並將其中過程適度文件化，留存紀錄待查，如此才得由教育部宣告該施行單位之 ISMS 符合本標準規範。

附錄 A

控制目標與控制措施

本標準列出之控制目標及控制措施乃參考ISO17799:2005 第 A.5 至 A.15 和行政院及所屬各機關資訊安全管理規範中列出之項目，另並依據教育體系與相關單位既有之屬性與特點，保留符合各層級單位之項目。各單位應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。

相關的條款針對其適用對象，除一體適用不予標註的項目外，將加以註記較適用於第一群之說明，避免歸屬第二群之單位於施行上的困難(但為避免此「建議適用」造成資安威脅的挑戰，第二群單位仍需考量該適用第一群條款之納入必要性)；另外，針對連線單位的「學術網路系統」及「行政資訊系統」，亦將註記該條款適用的系統，若無加註的部份，為兩套系統需遵守之項目。

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致單位上下外，不斷的評估、檢視已制定資安政策的合適性與否，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：

				ISO27001:2005(E)
A.5 資訊安全政策訂定與評估				A.5
控制目標	A.5.1	資訊安全政策訂定與評估		A.5.1
控制項	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.5.1.1
	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.5.1.2

(一) 資訊安全政策訂定與評估(A.5.1)

1. 資訊安全政策制定(A.5.1.1)

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。

施行單位制定資訊安全政策，應說明管理階層的承諾及該單位管理資訊安全的方法，應涵括下列事項：

(1) 資訊安全之定義、整體目標、範圍，及進行資訊共享時，其安全機制的重要性。

(2) 資訊安全政策應包含法令及契約對施行單位資訊安全的要求與規定。

(3) 資訊安全政策應包含資訊安全教育及訓練的要求。

(4) 資訊安全政策應包含業務永續運作規劃之政策。

(5) 員工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。

(6) 發生資安事件之通報作業程序、規定及說明。

(7) 施行單位資安政策及規範人員資安角色與責任的相關規定，應載明於人員工作說明書或相關作業手冊中。

(8) 施行單位員工如違反資安相關規定，應依紀律程序處理。

(9) 支援此一政策所需的參考文件，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。

(10) 資訊安全政策應為一般政策文件的一部份，若此文件會被分送至組織以外的地方，必須小心敏感性文件是否外洩。

2. 資訊安全政策評估(A.5.1.2)

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。施行單位應評估資訊安全政策，應涵括下列事項：

(1) 資訊安全評估對象應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) 資訊系統管理者應配合定期(建議一學期一次)資安評估作業，檢討相關人員是否遵守施行單位之資安政策、規範與其他規定。

(3) 應定期(建議一學期一次)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) 審查輸入事項建議包括：

a. 利害關係方的反應

b. 客觀第三者審查的結果

c. 預防措施及改進對策狀態

d. 前次評估的結果

e. 資訊安全政策遵行及執行效果

f. 影響組織管理資訊安全的改變，包括組織環境、營運事項、可用資源、合約、法規及技術等改變

g. 威脅、弱點的新趨勢。

h. 已回報的安全事件。

i. 相關權責單位提供的建議。(例如消防單位)

(5) 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。審查產出結果建議包括下列相關的決定及對策：

a. 組織資訊安全管理方法及程序的改善。

b. 控制目標及安控措施的改善。

c. 資源及責任分配的改進。

(6) 評估應記錄備查。

(7) 修訂過的政策應獲得管理階層的批准。

A.6

資訊安全組織

在組織資安政策建立完成後，執行組織因應而生，為的是各項既定政策的落實及推動；因此，組織推動資訊安全施行單位應指定適當權責之高層主管人員(類似資訊長的角色)，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，召開資安會報、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，確保資安措施正常運作，建立起一完善、安全之環境，降低組織資安威脅的機率。

本章節主要的內容可參照下表：

				ISO27001:2005(E)
A.6 資訊安全組織				A.6
控制目標	A.6.1	資訊安全組織推動與權責		A.6.1
控制項	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.6.1.1 A.6.1.2 A.6.1.3
	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
	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.6.1.5 A.8.1.3
	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.6.1.6
	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.6.1.7
	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.6.1.8
控制目標	A.6.2	施行單位外部人員存取安全管理		A.6.2
控	A.6.2.1	施行單位	面對外部人員存取施行單位資訊處理設施的	A.6.2.1

制項		外部人員存取之安全掌控	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。	A.6.2.2 A.6.2.3

(一) 資訊安全組織推動與權責(A.6.1)

1. 資訊安全組織推動以及權責之分配(A.6.1.1)

   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。

   定期(建議一學期一次)召開之資訊安全會報權責應包含：

   (1) 訂定資訊安全角色與資訊安全管理權責分工，賦予相關人員應有之安全權責，包含資安相關政策、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) 評估資訊安全事件審查及監視的結果，並針對資訊安全事件提出適當的行動方案。

2. 資訊設施使用之授權(A.6.1.2)

   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。

   在資訊處理設備的移轉、授權部分，應確保：

   (1) 在業務以及技術上皆通過權責人員的安全評估，並經主管核准，才得以授權使用。

   (2) 需進行評估以及授權工作場所使用個(私)人資訊處理設施，例如：筆記型電腦、PDA 等設備，避免可能造成的新弱點。

3. 保密條款之簽訂(A.6.1.3)

   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。

   有關保密條款之簽訂：

   (1) 施行單位之員工應簽署相關之保密合約，確保其了解應有之資安責任以及相關限制條件。

   (2) 當該職掌人員因故有所變更時，可視需求重新檢視保密條款之適切性。

4. 跨單位合作及協調(A.6.1.4)

   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，應達到：

   (1) 與資安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，應予以適當的限制，防止敏感性資訊遭未經授權之存取。

5. 資訊安全諮詢與顧問(A.6.1.5)

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，應考量：

(1) 施行單位資安人力、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。

6. 資訊安全政策的獨立檢視(A.6.1.6)

機關制訂之資訊安全政策，應進行獨立及客觀的評估。

在資安政策評估上，應考量：

(1) 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。

(二) 施行單位外部人員存取安全管理(A.6.2)

1. 施行單位外部人員存取之安全掌控(A.6.2.1)

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，應包含：

(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，應條列資安規定、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。(較適用於第一群)

A.7

資訊資產分類與管制

施行單位內有多少資訊資產？其資訊安全等級與分類為何？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，將有助於資產保管的執行效率，降低受危害的可能，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，使其符合資安政策，降低可能的威脅及危險。

本章節主要的內容可參照下表：

				ISO27001:2005(E)
A.7 資訊資產分類與管制				A.7
控制目標	A.7.1	資訊資產分類與責任分屬		A.7.1 A.7.2
控制項	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.7.1.1 A.7.1.2 A.7.1.3
	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.7.2.1 A.7.2.2

(一) 資訊資產分類與責任分屬(A.7.1)

1. 資訊資產目錄建立(A.7.1.1)

應製作所有資訊資產之清冊，並定期維護、更新。

資訊資產之清冊應達到：

(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，並定期維護與更新其內容。

(2) 資訊資產參考項目如下：

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應指定專責單位保管，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應該被確認，並以書面或其他方式記錄後確實執行。

2. 資訊安全等級分類(A.7.1.2)

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。

資訊資產分類原則，應包含：

(1) 資訊安全之等級分類原則如下所示：

a. 應建立資訊安全等級之分類標準，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. 機關資訊安全分類，依據國家機密保護、電腦處理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. 界訂資安等級之責任，應由資料的原始產生者或是由指定的系統所有者負責。

d. 當須執行或參考其他單位訂定之資安等級分類時，應特別注意其與本機關的資訊安全等級分類，在定義及標準上是否相同。

(2) 應納入安全等級分類之項目，包括書面報告、磁性媒體、電子訊息及檔案資料等，並標示適當的安全等級以利使用者遵循。

A.8

人員安全管理與教育訓練

再怎麼嚴密完整的政策與控制措施，缺乏觀念正確、訓練有素的執掌人員執行，亦是惘然。因此，施行單位所屬相關人員需針對其擔負的資安責任，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安措施，降低可能的資安風險。

本章節主要的內容可參照下表：

				ISO27001:2005(E)
A.8 人員安全管理與教育訓練				A.8
控制目標	A.8.1	聘任前之處理		A.8.1
控制項	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.8.1.1
控制目標	A.8.2	聘用中之處理		A.8.2
控制項	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.8.2.2
	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.8.2.3
控制目標	A.8.3	結束聘任或改變職務		A.8.3
控制項	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.8.3.1
	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.8.3.2
	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.8.3.3

(一) 聘任前之處理(A.8.1)

1. 所屬角色與責任(A.8.1.1)

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。

其原則應包括：

(1) 符合資訊安全政策。

(2) 保護資產防止未授權的存取、洩漏、更改、破壞或干擾。

(3) 確保每項行動規範中，個人的責任。

(4) 安全角色及責任應在聘用前即應明確定義並與應徵者清楚地溝通(由廠商聘用亦同)。

(二) 聘用中之處理(A.8.2)

1. 資訊安全教育訓練(A.8.2.1)

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。

有關資安教育與訓練的部份：

(1) 應定期(建議一學年至少一次)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，提高員工資安意識，並遵守資安規定。

(2) 施行單位同意及授權使用者存取系統前，應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，應確保其對資安政策、相關控制及程序有一定的了解，並清楚其資安責任。

2. 違反規定之處理(A.8.2.2)

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) 結束聘任或改變職務(A.8.3)

1. 結束聘用之處理(A.8.3.1)

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。

關於結束聘任後或改變職務，應：

(1) 視需求在合約中載明結束聘用後其責任及義務仍然有效的規定。

(2) 人員已離職或調職，應通知相關員工、合約商及第三方使用者。

2. 資產繳回(A.8.3.2)

資產繳回應有正式的離職程序，顯示其已繳回單位資產。

資產的繳回應：

(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，應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，應確實進行移轉或紀錄。

3. 存取權移除(A.8.3.3)

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。

移除或改變的存取權限應：

(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應該被降低或是移除。

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

A.9

實體與環境安全

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，軟硬體的防護措施也需徹底實行，以有效降低資安事件發生的機率。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：

				ISO27001:2005(E)
A.9 實體與環境安全				A.9
控制目標	A.9.1	區域之安全		A.9.1
控制項	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.9.1.1
	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。	A.9.1.2
	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。	A9.1.3 A9.1.4 A9.1.5
控制目標	A.9.2	設備之安全		A.9.2
控制項	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、災害以及未授權存取所造成的可能損失。	A.9.2.1
	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.9.2.2
	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。 —較適用於第一群	A.9.2.3
	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.9.2.4
	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.9.2.6

	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.9.2.7

(一) 區域之安全(A.9.1)

1. 實體環境安全(A.9.1.1)

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，應：

(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. 人員進出控制(A.9.1.2)

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，應確保：

(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應予適當管制，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。(較適用於第一群)

(3) 員工離職後，應立即撤銷進入管制區的權利。

3. 資訊處理設施安全(A.9.1.3)

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。

為確保區域之安全性，採取的控制措施與指引應包含：

(1) 資訊處理設施所在區域應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。(較適用於第一群)

(2) 資訊處理設施應遠離大眾或是公共運輸系統可直接進出的地點。(較適用於第一群)

(3) 資訊處理設施應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。

(4) 危險性及易燃性物品應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應存放在電腦機房內。

(5) 備援作業用的設備及備援媒體，應存放在安全距離以外的地點。(較適用於第一群)

(6) 應安裝適當的安全偵測及防制設備，各項安全設備應依廠商的使用說明書定期檢查，並針對相關員工進行適當的安全設備使

用訓練。(較適用於第一群)

(7) 設備安全緊急處理作業程序應以書面方式記載，並定期(建議一學期一次)演練及測試。(較適用於第一群)

(二) 設備之安全(A.9.2)

1. 設備安置地點之保護措施(A.9.2.1)

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) 設備應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，應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，應考量與一般設備區隔，安置在獨立的區域。(較適用於第一群)

(3) 應檢查及評估火災、煙、火、灰塵、震動、化學效應、電力供應、電磁輻射等可能的風險。(較適用於第一群)

(4) 電腦作業區應禁止抽菸及飲用食物。

2. 電源供應(A.9.2.2)

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。

有關於資訊處理設備電源供應，應：

(1) 防止斷電或其他電力不正常導致的傷害；電源供應應依據製造商提供的規格設置。

(2) 應考量安置預備電源，並考量使用不斷電系統。

(3) 將不斷電系統失效之後的應變措施納入資安事件緊急處理應變計畫；不斷電系統應依據製造廠商的建議，定期進行測試。

(4) 應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。

3. 電纜線安全防護(A.9.2.3) ─較適用於第一群

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應予適當的保護，其保護原則如下：

(1) 連接資訊設施的電源及通信線路，應盡可能地下化；如不能地下化，應視需求採取足夠的替代保護措施。

(2) 應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，應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. 設備之維護(A.9.2.4)

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，應：

(1) 應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) 應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，應採取適當的控制措施。(例如：將內部敏感性的資料移清除)

5. 設備報廢與再使用(A.9.2.5)

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：

(1) 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。

6. 預防未經授權之移動(A.9.2.6)

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，應：

(1) 在沒有管理人員授權的情況下，設備、資訊或是軟體不應被帶離所屬區域。

A.10

通訊與作業安全管理

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。此部份為整個規範中最為繁複的章節，牽扯範圍之廣泛非其他節能比擬，其重要性可見一般。

本章節主要的內容可參照下表：

				ISO27001:2005(E)
A.10 通訊與作業安全管理				A.10
控制目標	A.10.1	作業程序與責任		A.10.1
控制項	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.10.1.1
	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。	A.10.1.2
	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授權修改或誤用之機會。 —較適用於第一群	A.10.1.3
	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。 —較適用於第一群	A.10.1.4
控制目標	A.10.2	資訊作業委外服務之安全管理		A.10.2
控制項	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理責任，納入契約條款。	A.10.2.1
	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。	A.10.2.2
	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。 —較適用於第一群	A.10.2.3
控制目標	A.10.3	系統規劃與驗收		A.10.3

控制項	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。 —較適用於第一群	A.10.3.1
	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。	A.10.3.2
控制目標	A.10.4	電腦病毒、惡意軟體		A.10.4
控制項	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.10.4.1
控制目標	A.10.5	備份作業之管控		A.10.5
控制項	A.10.5.1	資料備份	重要資訊與軟體應進行定期的備份。	A.10.5.1
控制目標	A.10.6	網路安全管理 —較適用於學術網路系統		A.10.6
控制項	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。	A.10.6.1
	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。	A.10.6.2
控制目標	A.10.7	儲存媒體的處理與安全		A.10.7
控制項	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。	A.10.7.1
	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.10.7.2
	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
	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

控制目標	A.10.8	資訊與軟體交換		A.10.8
控制項	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.10.8.1 A.10.8.2
	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。	A.10.8.4
	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.10.8.5
	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。	A.10.9.3
控制目標	A.10.9	系統存取及應用之監督		A.10.10
控制項	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。	A.10.10.1
	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.10.10.2
	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.10.10.3
	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。	A.10.10.4
	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.10.10.5
	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.10.10.6

(一) 作業程序與責任(A.10.1)

1. 作業程序文件化(A.10.1.1)

安全政策所規定之作業程序，應文件化並定期維護。

關於作業程序之訂定，應：

(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；作業程序應視為正式文件，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。(較適用於第一群)

2. 作業變更之管理(A.10.1.2)

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，應：

(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。(較適用於第一群)

c. 評估作業變更之可能衝擊。(較適用於第一群)

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. 資訊安全責任之分散(A.10.1.3)—較適用於第一群

職務與責任範圍需予區分，降低資訊或服務遭未授權修改或誤用之機會。

資安責任之分散應：

(1) 對關鍵性資訊業務，分散資安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) 應在資訊人力許可下,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。

4. 系統發展、測試及實務作業之分散(A.10.1.4) —較適用於第一群

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，應：

(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，應考量下列措施：

a. 軟體從開發轉移至實作狀態的規則，應予界定並文件化。
b. 系統發展及實際作業的軟體，應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應盡可能分開。
d. 編輯器及其他公用程式不再使用時，不應與作業系統共同存放在一起。

(二) 資訊作業委外服務之安全管理(A.10.2)

1. 資訊作業服務之管控(A.10.2.1)

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理責任，納入契約條款。

納入資訊委外服務契約的資訊安全事項包括：

(1) 應留在施行單位內部處理之機密性、敏感性或是關鍵性的應用系統項目。

(2) 應經施行單位核准始得執行的事項。

(3) 廠商如何配合執行機關業務永續運作計畫。(較適用於第一群)

(4) 廠商應遵守的資訊安全規範及標準，及評鑑廠商是否遵守資訊安全標準的衡量及評估作業程序。

(5) 廠商如何處理及通報資訊安全事件的責任及作業程序。

2. 服務之監控與審查(A.10.2.2)

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。

應考慮下列安控措施：

(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。(較適用於第一群)

(5) 解決和管理所有界定的問題。

3. 廠商服務異動(A.10.2.3)—較適用於第一群

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。

服務異動之管理程序應包含：

(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。

(三) 系統規劃與驗收(A.10.3)

1. 系統作業容量之規劃(A.10.3.1)—較適用於第一群

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應包含：

(1) 應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) 應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，應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；主管人員應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) 應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。

2. 新系統上線作業之安全評估(A.10.3.2)

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。

新系統上線作業之安全評估應包含：

(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，應執行：

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，和資安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。(較適用於第一群)

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，應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。

(四) 電腦病毒、惡意軟體(A.10.4)

1. 電腦病毒及惡意軟體之控制(A.10.4.1)

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，應：

(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，提升員工的資安警覺，健全系統存取控制機制。

(3) 惡意程式的防範應考量下列原則：

a. 建立軟體管理政策，規定各單位及使用者應遵守軟體授權規定，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：

- 防制軟體應定期更新。
- 使用防制軟體事前掃瞄電腦系統及資料儲存媒體，偵測有無受到感染。
- 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。

- 應充分了解防制軟體的特性及功能。
- 定期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，應立即調查找出原因。
- 對來路不明及內容不確定的儲存媒體，應在使用前詳加檢查。
- 應建立防制攻擊事件及回復作業的管理程序，並訂定相關人員的責任。
- 應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。

(五) 備份作業之管控(A.10.5)

1. 資料備份(A.10.5.1)

重要資訊與軟體應進行定期的備份。

關於資料備份，應：

(1) 準備適當及足夠的備援設施，定期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，應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，應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. 備份資料應有適當的實體及環境保護。(較適用於第一群)

d. 應定期測試備份資料，確保其可用性。

e. 資料的保存時間以及永久保存的需求，應由資料擁有者研提。

f. 應定期檢查測試回復程序，確保回復程序能在指定時間內完成復原作業程序。(較適用於第一群)

g. 重要機密的資料備份，應使用加密方式來保護。(較適用於第一群)

(六) 網路安全管理 (A.10.6)—較適用於學術網路系統

1. 網路安全規劃與管理(A.10.6.1)

應實施網路控制措施，維護網路安全。

網路安全規劃與管理，包含：

(1) 網路安全規劃：

a. 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。

b. 加強跨單位間電腦網路系統之網路安全管理。(較適用於第

一群)

c. 利用公眾網路或無線網路傳送敏感性資料，應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。(較適用於第一群)

d. 網路安全管理應考量：(較適用於第一群)

- 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. 網路服務之安全控制(A.10.6.2)

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。

網路服務安全應包括：

(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，應確認廠商提供約定服務的安全管理能力。

(七) 儲存媒體的處理與安全(A.10.7)

1. 電腦媒體之安全管理(A.10.7.1)

電腦儲存媒體、可攜式媒體或印出報表，應制定控管措施。

應包含：

(1) 可隨時攜帶及移動的儲存媒體，應建立使用管理程序，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，不應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，應將儲存的內容消除。

(4) 對於要帶離機關辦公場所的儲存媒體，應建立書面的授權規定，並建立使用紀錄，以備日後稽核之用。(較適用於第一群)

(5) 儲存媒體應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，應在別處再作儲存，以免資料遺失。

(7) 應登記可攜式媒體來減少資料遺失的機會。

(8) 可攜式媒體應在公務理由上才可使用。

2. 電腦媒體處理之安全(A.10.7.2)

應訂定電腦媒體的處理作業程序，以降低可能的安全風險。

處理作業程序包含：

(1) 應建立需以安全方式處理的儲存媒體清單，包括：
   a. 輸入文件，例如電傳文件。
   b. 複寫紙。
   c. 書出報告。
   d. 磁帶。
   e. 可攜帶的磁片或是磁帶。
   f. 作業程序目錄。
   g. 測試資料。
   h. 系統文件。
(2) 非重複性使用之媒體，應以安全方式處理，如燒毀、碎紙機處理或是將資料從媒體中完全清除。
(3) 儲存媒體應依製造廠商提供的保存規格，存放在安全的環境。
(4) 機密性及敏感性資料處理過程，應以書面記錄之，以利事後查考與稽核之用。
(5) 防止大量非機密性資料彙總成為敏感性或機密性資料。(較適用於第一群)

3. 資料檔案之保護(A.10.7.3)

重要資料檔案應進行控管，並安全的保存。

保護原則有：

(1) 應保護重要資料檔案，以防止遺失、毀壞、被偽造或竄改。重要資料檔案應依相關規定，以安全方式保存。
(2) 超過法定保存期限的資料檔案，可依相關規定刪除或銷毀，但事前應考量可能造成的不利影響。
(3) 資料檔案的管理，應遵循下列原則：
   a. 訂定檔案保存、儲存、處理等指導原則作為執行的依據。
   b. 檔案保存期限應依檔案型態及法定保存期限之規定擬定。
   c. 應建立及維護重要資訊資源的目錄。
   d. 應採行適當的措施，保護機關的重要檔案及資訊，防止資料遺失、毀壞及被偽造或竄改。
(4) 必要時研訂重要性資料檔案的輸入及輸出媒體之安全作業程序，包括：
   a. 輸出及輸入資料檔案之處理程序及標示。
   b. 依授權規定，建立收受重要資料檔案的正式收文紀錄。
   c. 確保輸入資料之真確性。
   d. 儘可能要求收受者提出傳送之媒體已送達的收訖證明。
   e. 重要資料檔案的分發對象，應以最低必要的人員為限。

f. 為提醒使用者注意安全保密，應在資料上明確標示資料機密等級。
g. 必要時評估重要性資料檔案的發文清單，及檢討其內容。
h. 應確保資訊系統內部資料與外部資料之一致性。

4. 系統文件之安全(A.10.7.4)

重要系統文件應受到保護，避免未授權之存取。

重要系統文件之保護，包括：

(1) 系統流程、作業流程、資料結構及授權程序等系統文件，應予適當保護，防止系統文件遭未授權存取與不當利用。

(2) 系統文件的安全保護措施如下：

a. 系統文件應鎖在安全的儲櫃或其他安全場所。
b. 系統文件的發送對象，應以最低必要的人員為限，且應經系統擁有者的授權。
c. 電腦產製的文件，應與其他應用檔案分開存放，且建立適當的存取保護措施。

(八) 資訊與軟體交換(A.10.8)

1. 資訊與軟體交換安全政策與協定(A.10.8.1)

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，應訂定正式的協定，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，應考量：

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。

2. 電子郵件安全管理(A.10.8.2)

應制定電子郵件使用政策，並實施控制措施降低安全風險。

有關電子郵件安全管控，包括：

(1) 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。

(2) 依施行單位安全政策及規定，明訂電子郵件使用規定。

(3) 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。

(4) 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。

(5) 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。

(6) 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。

(7) 電子郵件附加檔案，應事前檢視內容有無錯誤後方可傳送。

(8) 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。

3. 電子辦公系統安全(A.10.8.3)

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。

有關電子辦公系統之安全，應：

(1) 訂定電子辦公系統的使用政策及指導原則，以確保單位實施辦公電子化在業務及系統上之安全。

(2) 電子辦公系統應考量之安全事項如下：

a. 電子辦公系統如未能提供適當及足夠的安全保護措施，不應將敏感性資料列入系統目錄。

b. 應訂定單位資料流通及分享的政策及管理措施。(例如：應訂定單位的電子布告欄系統應用政策)。

c. 對於特定個人(如單位主管或負責處理機密性或敏感性資訊的人員)的行程資訊等，不宜開放供開存取，並予以適當的限制。(較適用於第一群)

d. 評估以電子辦公系統處理單位重要業務的適當性。

e. 應建立被授權使用電子辦公系統的相關人員名錄，並建立使用者存取系統權限等資訊。

f. 特定的電子辦公設施，應限制只有特定人員才能使用。

g. 應訂定系統儲存資訊的保管作業及備援作業規定。

h. 電腦當機的備援作業規定。(較適用於第一群)

4. 對外公告資訊之管理(A.10.8.4)

對外公告資訊前應有正式授權程序，並避免未授權之竄改。

關於對外公告資訊管理，應：

(1) 對外開放的資訊系統，應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)，應做適當的存取控管，以維護系統正常運作。

(九) 系統存取及應用之監督(A.10.9)

1. 事件記錄(A.10.9.1)

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。

系統稽核軌跡應包括下列事項：

(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。(較適用於第一群)

(9) 檔案存取及存取類型(較適用於第一群)

(10) 網址及通信協定(較適用於第一群)

(11) 存取權限提昇警報(較適用於第一群)

(12) 保護系統的執行與撤銷(例如防毒系統及入侵偵測系統)(較適用於第一群)

2. 系統使用之監控(A.10.9.2)

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。

系統使用監督應考量：

(1) 系統存取失敗情形。

(2) 檢查系統登入的模式，確定使用者識別碼是否有不正常使用或是被重新使用的情形。

(3) 查核系統存取特別權限的帳號使用情形及配置情形。

(4) 追蹤特定的系統交易處理事項。(較適用於第一群)
(5) 敏感性資源的使用情形。(較適用於第一群)
(6) 監督作業應經權責主管人員之正式授權。

3. 記錄的保護(A.10.9.3)

單位應保護未授權的變更及防止記錄設備操作發生問題。

記錄保護之內容應包括：

(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。

4. 系統管理者與作業人員之記錄(A.10.9.4)

應忠實紀錄系統管理者與作業人員之相關操作記錄。

操作記錄應包含：

(1) 應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，應定期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。(較適用於第一群)

5. 系統錯誤事項之紀錄(A.10.9.5)

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。

其中應包含：

(1) 系統發生作業錯誤時，應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，應正式記錄下來，以供日後查考。
(3) 應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. 應檢查錯誤情形的紀錄，確保系統作業錯誤已經改正。
    b. 應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。

6. 系統時鐘應予同步 (A.10.9.6)

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.11

存取控制安全

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：

				ISO27001:2005(E)
A.11 存取控制安全				A.11
控制目標	A.11.1	使用者存取控制		A.11.1
控制項	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.11.2.1
	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。 —較適用於第一群	A.11.2.2
	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.11.2.3
	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。 —較適用於第一群	A.11.2.4
控制目標	A.11.2	使用者責任		A.11.3
控制項	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。	A.11.3.3
控制目標	A.11.3	網路存取控制措施		A.11.4
控制項	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。	A.11.4.1
	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.11.4.2

	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
	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
	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
	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
控制目標	A.11.4	作業系統存取控制		A.11.5
控制項	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.11.5.1
	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.11.5.3
	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。 —較適用於第一群	A.11.5.4
	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
控制目標	A.11.5	應用系統的存取控制 —較適用於行政資訊系統		A.11.6
控制項	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.11.6.1
	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
控制目標	A.11.6	行動式電腦作業與遠距工作管理 —較適用於第一群		A.11.7
控制項	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。 —較適用於第一群	A.11.7.1

	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。 —較適用於第一群	A.11.7.2

(一) 使用者存取控制(A.11.1)

1. 使用者註冊管理(A.11.1.1)

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。

關於使用者註冊管理，應：

(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，應考量：

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，以及符合資安政策與規定。

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. 應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，應盡速註銷其系統存取權利。

h. 應定期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應重新配予其他的使用者。

2. 系統存取特別權限管理(A.11.1.2)—較適用於第一群

限制與控管特許權限的分配及使用方式。

關於特許權限的限制與控管，應：

(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. 應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. 應依執行業務的需求，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，應以執行業務及職務所必要者為限。

c. 應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，應將系統存取

特別權限之授權資料建檔。

d. 應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，應避免以特別權限執行。

f. 特別權限應授予正常營運使用之外的使用者。

3. 一般通行碼之控管(A.11.1.3)

應建立使用者通行碼之管理制度。

通行碼之控管應考量：

(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，應確保工作群組的通行碼，僅限群組成員使用。

(2) 為維護通行碼的機密性，應以配予臨時性通行碼並強迫使用者立即更改通行碼的方式處理：使用者忘記通行碼時，可提供臨時性的通行碼，以利系統辨認使用者。

(3) 應以安全的方式將臨時的通行碼交付使用者，避免經由第三者，或是以未受保護的電子郵遞等電子方式交付給使用者，並建立確認收到之機制。

(4) 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。

4. 系統存取權限之評估(A.11.1.4)—較適用於第一群

施行單位應定期審查使用者存取權限。

使用者存取權限的審查應：

(1) 定期(建議一學期一次)檢討及評估使用者的存取權限。

(2) 當人員實施內部調動時，應重新審查使用者存取權限。

(3) 定期(建議半學期一次)檢討特別權限之核發情形。

(二) 使用者責任(A.11.2)

1. 桌面淨空之安全管理(A.11.2.1)

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。

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，應存放在櫃子內。

(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，應以上鎖、通行碼或是其他控制措施保護。

(4) 應該考量保護一般郵件進出的地點，以及無人看管的傳真機。(較適用於第一群)

(5) 當列印敏感性或分類機密資訊後，應立即從印表機上取走。

(三) 網路存取控制措施(A.11.3)

1. 網路服務之限制(A.11.3.1)

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。

關於網路服務之限制，應：

(1) 依施行單位業務存取控制規定，制定個別使用者或是特定端末機存取電腦及網路服務之安全規定。

(2) 使用者應在授權範圍內存取網路系統服務事項。

(3) 適當控制使用者端末機連接系統之線路，減少未授權存取之風險。

(4) 建立專用性通道，防止未授權使用者從不同管道進入系統。(較適用於第一群)

(5) 建立專用性通道考量如下：(較適用於第一群)

a. 指定專線及電話號碼。

b. 自動將通訊埠連上特定應用系統及安全通道。

c. 限制使用者只能選擇特定的路線。

d. 防止無限制的網路漫遊。

e. 強制外部使用者使用指定的應用系統、安全閘道。

f. 透過安全閘道(如防火牆)，主動控制被允許的起訖點通訊線路。

(6) 網路系統管理人員應負責網路安全規範的擬訂，執行網路管理工具之設定與操作，確保系統與資料的安全性與完整性；包括：

a. 網路系統管理人員應負責製發帳號，供授權的人員使用；除非有特殊情況，不得製發匿名或多人共享的帳號。

b. 提供給內部人員使用之網路服務，與開放業務相關人員從遠端登入內部網路系統的網路服務，應執行嚴謹的身分辨識作業，或使用防火牆代理伺服器進行安全控管。

c. 如果系統使用者已非正式授權的使用者時，網路系統管理人員應立即撤銷其使用者帳號；離(休)職人員應依單位資安規定及程序，取消存取網路之權利。

d. 網路系統管理人員未經權責主管人員許可，不得閱覽使用者私人檔案；但若發現可疑的網路安全情事，得依授權規定使用自動搜尋工具檢查檔案。

e. 網路系統管理人員未經使用者同意，不得增加、刪除及修改私人檔案。如有特殊緊急狀況須刪除私人檔案，應以電子郵件或其他方式是先知會檔案擁有者。

f. 對任何網路安全事件，網路系統管理人員應立即向機關內部或機關外部設置之電腦安全事件緊急處理小組反應。

g. 網路系統管理人員只能由系統終端機登入主機，並保留所有登入、登出紀錄。

h. 網路系統管理人員不得新增、刪除、修改稽核資料檔案，以避免違反安全事件發生時，造成追蹤查詢的困擾。

(7) 網路使用者管理之管理應包括：

a. 被授權的網路使用者(以下簡稱網路使用者)，只能在授權範圍內存取網路資源。

b. 網路使用者應遵守施行單位之網路安全規定，了解自己應負的責任；如有違反網路安全之情事，依規定及相關法規處理，並限制或撤銷其網路資源存取權利。

c. 網路使用者不得將自己的登入身分識別與登入網路的密碼交付他人使用。

d. 應禁止網路使用者以任何方式竊取他人的登入身分與登入網路通行碼。

e. 應禁止網路使用者以任何儀器設備或軟體工具竊聽網路上的通訊。

f. 禁止網路使用者在網路上取用未經授權的檔案。

g. 網路使用者不得將色情檔案建置在單位網路，亦不得在網路上散撥不適於存取資訊之文字、圖片、影像、聲音等資訊。

h. 應禁止網路使用者發送電子郵件騷擾他人，導致其他使用者的不便與不安。

i. 應禁止網路使用者發送匿名信，或偽造他人名義發送電子郵件。

j. 網路使用者不得以任何手段蓄意干擾或妨害網路系統的正常運作。

k. 施行單位外部取得正式授權的電腦主機或網路設備，與內部網路連線作業時，應遵守網路安全規定及連線作業程序。

(8) 主機安全之防護應包含：

a. 機關存放機密性及敏感性資料之大型主機或伺服器主機(如 Domain Name Server 等)，除作業系統既有的安全設定外，應規劃安全等級較高之密碼辨識系統，以強化身分辨識之安全機制，防止遠端撥接或遠端登入資料經由電話線路或網際網路傳送時，被偷窺或截取(如一般網路服務 HTTP、Telnet、FTP 等的登入密碼)，及防制非法使用者假冒合法使用者身份登入主機進行偷竊、破壞等情事。

b. 為提升大型主機或伺服器主機連線作業之安全性，應視需要使用電子簽章及電子信封等安全控管技術，建立安全及

可信賴的通信管道。

(9) 防火牆之安全管理應包含：

a. 施行單位與外界網路連接的網點，應加裝防火牆，以控管外界與內部網路之間的資料傳輸與資源存取。

b. 防火牆應具備網路服務的轉送伺服器(即代理伺服器，Proxy Server)以提供 Telnet、FTP、WWW、Gopher 等網路服務的轉送與控管。

c. 施行單位網路防火牆的安裝與網路架構之規劃及設置，應依據訂定的資訊安全規定與資訊安全等級分類，以最經濟有效的方式配置。

d. 防火牆應由網路系統管理人員執行控管設定，並依單位制定的資訊安全規定、資訊安全等級及資源存取的控管策略，建立包含身分辨識機制、來訊服務(Incoming Service)、去訊服務(Outgoing Service)與系統稽核的安全機制，有效地規範資源被讀取、更改、刪除、下載或上傳等行為以及系統存取權限等資訊。

e. 網路系統管理人員應由系統終端機登入防火牆主機，禁止採取遠端登入方式，避免登入資料遭竊取，危害網路安全。

f. 防火牆設置完成時，應測試防火牆是否依設定的功能正常且安全的運作。如有缺失，應立即調整系統設定直到符合既定的安全目標。

g. 網路系統管理人員應配合施行單位之資訊安全政策和規定的更新，以及網路設備的變動，隨時檢討及調整防火牆系統的設定與系統存取權限，反應最新的狀況。

h. 施行單位之防火牆系統軟體應定期更新版本。

(10) 軟體輸入控制應包含：

a. 應禁止網路使用者使用非法軟體。

b. 經由網際網路下載軟體，宜由網路系統管理人員事前測試及掃描，確認安全無虞後方可安裝及執行。

c. 應考量在網路上各檔案伺服器安裝防毒軟體。

d. 網路使用者應定期(建議一個月至少一次)以電腦病毒掃描工具執行病毒掃描，並了解病毒與惡意執行檔可能入侵的管道，採取防範措施。

e. 網路使用者如偵測到電腦病毒入侵或其他惡意軟體，應立即通知網路管理者；網路管理者亦應將以遭病毒感染的資料及程式等資訊隨時提供使用者，避免電腦病毒擴散。

f. 電腦設備如遭病毒感染，應立即與網路離線，直到網管人員確認病毒已消除後，才可重新連線。

2. 遠端使用者身份鑑別(A.11.3.2)—較適用於第一群

遠端連線使用者之存取需進行身分鑑別。

使用者身份鑑別應：

(1) 針對開放單位以外的使用者從公眾網路，或從單位內部網路以外的的網路進行連線作業，建立遠端使用者身份鑑別機制，降低未經授權存系統的風險。

(2) 可考量使用「詰問及回應」(Challenge/Response)、「時間同步」(Time Synchronize)或資料加密(非對稱型)等安全技術，鑑別網路使用者之身分。

(3) 考量存取無線網路的身分鑑別。

3. 診斷埠(Diagnostic Ports)存取控制(A.11.3.3)—較適用於第一群

診斷埠的存取行為必須嚴密控管。

關於診斷埠的存取應：

(1) 採取特別的安全控管機制，提供維修服務廠商以遠端登入方式，進入施行單位電腦網路系統進行維修的通信作業埠。

4. 網路分隔控制(A.11.3.4)—較適用於第一群

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，應：

(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，每一領域應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。

5. 網路連線控制(A.11.3.5)—較適用於第一群

使用者連線能力應視需求予以限制。

限制使用者連線能力之控制，可考量：

(1) 為確保系統安全，跨單位之網路系統可限制使用者之連線作業能力。

(2) 限制網路連線作業能力之安全控制措施如下：

a. 只允許使用特定協定。

b. 限制檔案傳輸方向(單向或雙向)。

c. 使用互動式的系統存取。

d. 限制只能在特定的時間或日期進行系統存取。

6. 網路路由控制(A.11.3.6)—較適用於第一群

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。

路由控制措施應：

(1) 針對共享網路系統(尤其是跨單位的網路系統)，建立網路路由的控制，確保電腦連線作業及資訊流動不會影響應用系統的存取政策。

(2) 建立實際來源及終點位址之檢查機制；網路路由控制可以硬體或軟體方式執行,並應事先評估了解不同方式的安全控制能力。

(四) 作業系統存取控制(A.11.4)

1. 系統登入程序(A.11.4.1)

使用者存取電腦系統應經由安全的系統登入程序。

登入程序建議應具備下列功能：

(1) 不應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,必要時應顯示"只有被授權的使用者才可存取系統"等警告性的資訊。

(3) 系統不應在登入程序中，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，系統不應顯示那一部分資料是正確的，那一部分資料是錯誤的。

(5) 應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，系統並應：

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，應強迫必須間隔一段時間之後才能再次登入。

c. 應中斷資料連結作業。

(6) 在系統登入被拒絕後，應立即中斷登入程序，並不得給予任何的協助。

(7) 應限制系統登入程序的最長及最短時間，如果超出時間限制，系統應自動中斷登入。

(8) 在成功登入系統後，應顯示下列的資訊：

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。

2. 使用者通行碼管理(A.11.4.2)

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，應：

(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；系統應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(建議使用最少六位長度的通行碼)。
(4) 要求使用者定期更改通行碼(建議三個月一次，最長不宜超過一學期)
(5) 以更頻繁的次數定期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，應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，系統不應顯示使用者的密碼資料。
(9) 使用者密碼應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。(較適用於第一群)
(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。

3. 系統公用程式管理(A.11.4.3)—較適用於第一群
系統上公用程式的使用，應予限制並控管。
關於系統公用程式的管理，應：
(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. 將系統公用程式與應用系統分離。
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。

4. 連線作業時間之控制(A.11.4.4)—較適用於第一群

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，應：

(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. 應限制連線的網址。

d. 限制經過一段時間後必需重新認證。

(五) 應用系統的存取控制(A.11.5)—較適用於行政資訊系統

1. 資訊存取限制(A.11.5.1)

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。

關於資訊以及應用系統功能的存取限制措施，應：

(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，應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. 機密及敏感性系統之獨立作業(A.11.5.2)

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。

設立專屬的電腦作業環境，應考量：

(1) 由系統擁有者決定應用系統是否屬於機密性或敏感性系統，並以書面記載。

(2) 機密性或敏感性的應用系統需在分享式的電腦環境中執行時，應界定其他需共享資源的系統項目，並經系統擁有者的同意。

(六) 行動式電腦作業與遠距工作管理(A.11.6)—較適用於第一群

1. 行動式電腦作業控制(A.11.6.1)—較適用於第一群

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。

關於行動式電腦設施的控制措施及政策：

(1) 應適用單位既訂之資訊處理設施的相關控制措施及政策，防止未授權存取以及毀壞、竊取、洩漏等違反資安情事的發生。

2. 遠距工作管理(A.11.6.2)—較適用於第一群

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。

關於遠距工作活動的控管，應：

(1) 適用單位既訂之作業控制措施，降低各種可能的資安風險。

(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.12

系統開發與維護之安全

系統開發與維護應納入資安方面的考量，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，在不違反各資安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：				ISO27001:2005(E)
A.12 系統開發與維護之安全				A.12
控制目標	A.12.1	系統安全要求 —較適用於行政資訊系統 —較適用於第一群		A.12.1
控制項	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。 —較適用於第一群	A.12.1.1
控制目標	A.12.2	應用系統安全 —較適用於行政資訊系統		A.12.2
控制項	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
	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
	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
	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
控制目標	A.12.3	加密控制措施 —較適用於第一群		A.12.3
控制項	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。 —較適用於第一群	A.12.3.1
	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。 —較適用於第一群	A.12.3.2

控制目標	A.12.4	系統檔案安全		A.12.4
控制項	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.12.4.1
	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。 —較適用於第一群	A.12.4.2
	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。 —較適用於第一群	A.12.4.3
控制目標	A.12.5	開發與支援作業的控制 —較適用於第一群		A.12.5
控制項	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。 —較適用於第一群	A.12.5.1
	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。 —較適用於第一群	A.12.5.2
	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。 —較適用於第一群	A.12.5.3
	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
	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。 —較適用於第一群	A.12.5.5
控制目標	A.12.6	系統弱點管理 —較適用於第一群		A.12.6
控制項	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。 —較適用於第一群	A.12.6.1

(一) 系統安全要求(A.12.1)—較適用於行政資訊系統—較適用於第一群

1. 安全需求分析及規格訂定(A.12.1.1)—較適用於第一群

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，應：

(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，皆應明定資訊安全需求，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，亦應進行相同的安全需求。

(3) 系統的安全需求及控制程度，應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，應特別考量：

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. 應於相關文件規定資安控制措施，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。

(二) 應用系統安全(A.12.2)—較適用於行政資訊系統

1. 資料輸入之驗證(A.12.2.1)

輸入應用系統之資料須確認其正確性與適當性。

在輸入資料的確認，應考量：

(1) 檢查是否有以下錯誤：

a. 是否有超出設定範圍的數值。

b. 資料檔案是否有錯誤的文數字。

c. 資料是否有損毀或是不正確。

d. 是否有超定數值的上下限。

e. 是否有未經授權資料或是不一致的控制性資料。

(2) 應定期檢查主要欄位或資料檔案的內容，確保資料的有效性及真確性。

(3) 檢查輸入的書面資料有無被竄改情事。

(4) 建立資料驗證程序及資料被錯誤更正的作業程序。

(5) 明定資料輸入過程中相關人員的責任。

(6) 建立關於資料輸入處理作業的紀錄。

2. 系統內部作業處理之驗證(A.12.2.2)—A.12.2.2

系統需建立確認檢查機制，以偵知所處理資料的塗改。

關於系統作業處理的驗證機制，應：

(1) 建立驗證資料正確性的作業程序，避免正確輸入資料到應用系統中，卻因系統處理錯誤或是人為因素而遭破壞。

(2) 系統內部作業是否採取特別的資料處理控制程序，應視應用系統的性質及資料遭破壞，對機關業務的影響程度而定。

(3) 系統作業處理驗證方法如下：

a. 利用系統提供的功能，做資料處理作業控制或批次控制，以達到檔案資料更新處理後的一致性。

b. 比對本次開始作業與前次結束作業的檔案資料是否一致。
c. 查證系統產生的資料是否正確。
d. 在中央及遠端電腦系統之間，應檢查資料、下載及上傳軟體或軟體更新後系統的真確性。

3. 訊息真確性之鑑別(A.12.2.3)—較適用於第一群

必要時應採用訊息鑑別機制，保護訊息內容的完整性。

訊息鑑別機制應：

(1) 利用訊息鑑別技術，偵測資料內容是否遭受未經授權的竄改，或驗證傳送訊息內容是否遭受破壞。
(2) 對重要的應用系統，應使用訊息鑑別技術保護資料內容的真確性。

4. 資料輸出控管(A.12.2.4)

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。

關於應用系統資料輸出的確認，應：

(1) 適用單位制定之資訊保護措施，確保處理內容及程序的正確性及適當性。

(三) 加密控制措施(A.12.3)—較適用於第一群

1. 資料加密(A.12.3.1)—較適用於第一群

必須發展加密控制措施保護資訊之政策。

資訊保護政策應：

(1) 對高敏感性的資料，應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，應進行風險評估，以決定採取何種等級的安全保護措施。
(3) 使用加密技術時，如機關資訊專業人力及經驗不足，可借重外界的學者專家提供技術諮詢服務。
(4) 應遵守權責主管單位訂定的資料保密規範，及使用權責主管單位檢驗合格或認可的加密模組，以確保加密技術產品的安全功能。

2. 憑證機構之技術安全(A.12.3.2)—較適用於第一群

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，應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，應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，應依權責主管單位建議之參考值及視系統的安全需求設定。
(4) 機關對外採購加密技術時，應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。

(四) 系統檔案安全(A.12.4)

1. 作業軟體控制(A.12.4.1)

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。

作業軟體之控管上，應：

(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，應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，不應在作業系統執行。

d. 設定檔控制系統可控管所有實作軟體和系統文件。

e. 在變更實作前應建立回寫策略(rollback)。

f. 應建立應用程式的更新稽核紀錄。

g. 舊有軟體的版本應該被儲存，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。

2. 系統測試資料之保護(A.12.4.2)—較適用於第一群

系統之測試資料須予以保護與控管。

關於系統測試資料：

(1) 應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，應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，應：

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，應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，真實資料應立即從測試系統中刪除。真實資料的複製情形應予以記錄，以備日後稽核之用。

3. 原始程式庫資源之存取控制(A.12.4.3)—較適用於第一群

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。

原始程式庫的存取應：

(1) 應用程式原始碼資料庫應儘可能不要存放在作業系統的檔案中。

(2) 應用程式原始碼應指定專人控管。
(3) 不應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，應與實務作業之程式原始碼資料庫區隔，不應放置在一起。
(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，應由原始碼資料庫管理人員執行。
(6) 程式目錄清單應放置在安全的環境中。
(7) 應建立所有存取程式原始碼資料庫的稽核軌跡。
(8) 舊版的原始程式應妥慎典藏保管，詳細記錄使用的明確時間，並應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，應依嚴格的變更控制程序進行。

(五) 開發與支援作業的控制(A.12.5)—較適用於第一群

1. 變更作業之控制程序(A.12.5.1)—較適用於第一群

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應：

(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，應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，皆應獲得權責主管人員的同意。
(2) 建立變更控制程序，應考量的事項如下：
   a. 規定系統使用者提出變更需求之權責，以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. 應找出系統變更作業需要修正的電腦軟體、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，應取得權責主管人員之核准。
   f. 在執行變更作業前，應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，應立即更新，舊版的系統文件亦應妥善保管及處理。
   h. 應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，皆應建立稽核紀錄。

2. 作業系統變更之技術評估(A.12.5.2)—較適用於第一群

應用系統必須有所變更時，需進行必要之技術審核及測試。

作業系統變更之技術評估應：

(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，應考量：

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，應納入年度計畫及預算。

c. 作業系統的變更應即時通告相關人員，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。

3. 套裝軟體變更限制(A.12.5.3)—較適用於第一群

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應：

(1) 廠商提供的套裝軟體，應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，應考量：

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. 應取得套裝軟體開發廠商的同意。

c. 應考量標準化的系統更新方式，請廠商進行必要的變更。

d. 應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。

4. 資訊洩漏控制(A.12.5.4)—較適用於第一群

預防施行單位資訊遭洩漏的危機，制定適當的控管措施。

應考慮下列事項：

(1) 掃描對外連線的媒體及通訊以發現隱藏資訊。

(2) 隱藏、調整系統及通訊狀態以減少系統資訊被偵測的機率。

(3) 選用高安全等級的系統和軟體，例如使用國際認證評價的產品。

(4) 在法律或規章允許下，定期實施人員和系統行為的監控。

5. 軟體委外開發(A.12.5.5)—較適用於第一群

軟體之委外、使用需採取適當之管制及檢查。

在軟體委外開發時應考慮：

(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。

(6) 注意防止可能之隱秘通道和木馬程式。

(六) 系統弱點管理(A.12.6)—較適用於第一群

1. 系統弱點控制(A.12.6.1)—較適用於第一群

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) 應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、資產追踪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應明確定義。

(3) 一旦確認潛在的系統弱點，應採取相關措施。(例如修補漏洞)

(4) 若使用修補檔，應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。修補檔應在安裝前應經過測試。若無修補檔，則應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. 相關的稽核記錄應保持，以便後續使用。

e. 高風險系統優先考量前述安控措施。

A.13

資訊安全事件之反應及處理

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，當資安事件發生時，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：

				ISO27001:2005(E)
A.13 資訊安全事件之反應及處理				A.13
控制目標	A.13.1	資訊安全事件與弱點之通報		A.13.1
控制項	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.13.1.1
控制目標	A.13.2	資訊安全事件之管理		A.13.2
控制項	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.13.2.1
	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.13.2.2
	A.13.2.3	A.13.2.3	電腦稽核軌跡及相關的證據，應以適當的方法保護。	A.13.2.3

(一) 資訊安全事件與弱點之通報(A.13.1)

1. 資訊安全事件與弱點通報(A.13.1.1)

資安事件需即刻進行通報。

施行單位應：

(1) 建立資安事件與弱點的正式通報程序及管道，訂定接受資安事件通報應採行之行動及措施。

(2) 如發現或懷疑有資安事件時(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)，應依已訂定之通報管道迅速通報權掌人員立即處理。

(3) 相關人員應確實明瞭各種資安事件的反應及報告程序。

(4) 系統安全上的弱點，應由專業人員處理，不應任由系統使用者自行修改。

(二) 資訊安全事件之管理(A.13.2)

1. 資安事件處理責任與程序建立(A.13.2.1)

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。

資安事件的反應與處理作業的程序包括：

(1) 針對各項資安事件，進行適當的處理程序；資安事件可能包括：

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應納入：

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. 從資安事件中學習(A.13.2.2)

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。

關於資安事件的發生過程與紀錄，應：

(1) 針對整體資安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。

3. 資安事件證據之收集(A.13.2.3)

電腦稽核軌跡及相關的證據，應以適當的方法保護。

適當保存證據，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。

A.14

業務永續運作管理

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：

				ISO27001:2005(E)
A.14 業務永續運作管理 —較適用於第一群				A.14
控制目標	A.14.1	永續運作管理之規劃 —較適用於第一群		A.14.1
控制項	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。 —較適用於第一群	A.14.1.1 A.14.1.4
控制目標	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。 —較適用於第一群	A.14.1.5

(一) 永續運作管理之規劃(A.14.1)—較適用於第一群

1. 業務永續運作之規劃程序(A.14.1.1)—較適用於第一群

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。

關於永續作業規劃及架構建立，應：

(1) 建立跨部門的業務永續運作計劃程序，研訂及維護機關業務持續運作之計畫。

(2) 業務永續運作的規劃作業，應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) 機關業務永續運作計畫，應考量下列事項：

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. 應就緊急應變程序及作業流程，進行員工教育及訓練。

f. 應測試緊急應變計畫。

g. 應定期更新緊急應變計畫。

(4) 應建立及維持單一的永續作業計畫架構，使各種不同層次及等級的計畫相互連貫，並應訂定測試計劃及維護計畫之優先順序。

(5) 每項業務之永續運作計畫，應明定行動之條件，以及員工執行計畫之責任；機關研擬新的資訊計劃，應與機關緊急應變計劃程序相一致。

(6) 在業務永續運作之整體架構內，應訂定不同層次及等級的計畫，每一層次及等級的計畫，應涵蓋不同的計畫重點及負責回復作業的人員安排。

(7) 業務永續運作計畫，應考量的作業程序為：

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，應立即採取的行動。

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。

(8) 每一層次的計畫以及每一項個別計畫，都應指定一位計畫執行督導人員。

(9) 緊急應變作業、人員預備作業及回復計畫等，應指定適當的單位或人員負責。

(10) 技術服務的預備作業安排，應由技術服務提供者負責。

2. 永續運作計畫之測試及更新(A.14.1.2)—較適用於第一群

永續運作計畫應進行測試與維護，確保該計畫的有效性。

永續運作計畫的測試應：

(1) 業務永續運作計畫可能因事前的假設不正確、規劃不周全或設備及人員的職務調整變更，而無法發揮預期的作用，應定期測試及演練，以確保計畫的有效性，並使相關人員確實了解計畫的最新狀態。

(2) 應擬定測試作業的時程，定期進行測試，使應變計畫維持在有效及最新的狀態；測試計畫可以定期測試個別計畫的方式進行，以減少測試完整計畫的需求及頻率。

A.15

相關法規與施行單位政策之符合性

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：				ISO27001:2005(E)
A.15 相關法規與施行單位政策之符合性				A.15
控制目標	A.15.1	法規之遵守		A.15.1
控制項	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，了解與資訊處裡設施、軟體系統的關係，並予以書面或其他方式留存。	A.15.1.1
	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.15.1.2 A.15.1.3 A.15.1.4 A.15.1.5
控制目標	A.15.2	安全政策與技術符合性之檢驗		A.15.2
控制項	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.15.2.1
	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。	A.15.2.2
控制目標	A.15.3	系統稽核的考量		A.15.3
控制項	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.15.3.1
	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

(一) 法規之遵守(A.15.1)

1. 適用法規之鑑別(A.15.1.1)

   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，了解與資訊處裡設施、軟體系統的關係，並予以書面或其他方式留存。

2. 適用法規之遵循(A.15.1.2)

   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。

(二) 安全政策與技術符合性之檢驗(A.15.2)

1. 確保遵守安全政策與規範(A.15.2.1)

   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。

2. 資訊系統符合性審查(A.15.2.2)

   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。

(三) 系統稽核的考量(A.15.3)

1. 系統稽核控制(A.15.3.1)

   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。

2. 系統稽核工具之保護(A.15.3.2)—A.15.3.2

   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。

附錄 B

刪除之規範與控制項

一、刪除之規範

在參考 ISO17799:2005 原始規範後，為考量教育體系與相關單位的特性，特地簡化所有條款之內容，僅留下必要且適用於本規範施行對象需求之項目，希望藉此予以建構 ISMS 之單位一定的彈性空間，便於進行 ISMS 的所有程序，在不過於耗費資源，又不暴露單位於資安危機的情況下，降低資安事件的發生，提升 ISMS 之有效性。

二、刪除之控制項

編號	項目	內　　容	刪除之原因
A.6.1.1	管理階層資訊安全會報	管理階層資訊安全會報可確保有明確方向，且管理階層能表現對於資訊安全相關計畫的支持。	由於此三項皆需要管理階層的居中協調，召開討論會議才能將相關的工作、責任進行分配，所以，為簡化控制項目，將此三項合併為一項控制項。
A.6.1.2	資訊安全協調工作	學校應視需要，責成相關單位代表組成跨部門管理會報，負責協調資訊安全控制措施之執行。	
A.6.1.3	資訊安全責任的配置	資產之個別保護及執行特定安全程序的責任應明確劃分。	
A.6.2.1	鑑別來自施行單位外部存取之風險	外部單位存取學校資訊處理設施之風險應予評鑑，並實施適當安全控制措施。	關於外部單位存取風險的控制項目，鑒於相關單位鮮少存在類似的業務，因此將風險控制與合約要求合併為一項，在必要時才限定施行單位必須進行相關的動作。
A.6.2.2	服務施行單位外部存取之安全要求	在予以外部單位存取學校資訊或資產前，應紀錄所有被定義出的安全需求。	
A.6.2.3	第三方合約中之安全要求	第三方存取學校資訊處理設施之相關事宜應有正式合約，規定所有必要安全要求。	

A.7.1	資產可歸責性	為維護學校資產進行適切的保護。	在此將A.7.1及A.7.2合併成一控制項，簡少項目數，以利使用者查閱。
A.7.2	資訊分類	確保資訊資產獲得適當之保護層級。	
A.7.1.1	資產清冊	應製作所有與每一資訊系統相關重要資產之清冊並維護。	由於此三項皆與資產的紀錄、保護、管理有關，所以在此與以合併，但仍保有既有的控制項目。
A.7.1.2	資產保管	所有資訊系統或服務之資產應指定專責單位保管。	
A.7.1.3	資產可接受使用	資訊資產或服務之相關資產,應確認其可接受的使用方式，並予以記錄。	
A.7.2.1	分類指引	資訊分類與相關保護控制措施應考量單位分享或限制資訊之需求,以及與該需求有關之業務衝擊。	標示、分類以及相關控制措施應是相輔相成之控制措施，缺其一則有資安危機之風險，故將其二項合併為一項，但保有原始兩項內容之要求。
A.7.2.2	資訊標示與處理	應制訂一套和學校所採用分類方式相符之資訊標示與處理流程。	
A.8.1.2	人員篩選及政策	正職員工、承包商及臨時雇員在申請工作時即應進行背景檢查。	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。
A.6.1.5	保密協議	員工應簽署保密條款,作為聘僱首要條件與限制之一部分。	保密條款的簽訂應包含相關聘任條件與限制的內容，故在此將兩項合併，避免造成施行單位的過度負擔。
A.8.1.3	聘用條件與限制	聘僱條件與限制應說明員工對資訊安全之責任。	
A.8.2.1	管理階層責任	管理階層應要求員工、合約商以及第三方使用者遵守單位的資安政策與程序。	管理階層的要求可以藉由契約以及各項報告得到監督的效果，因此予以省略。
A.9.1.3	辦公處所及設施之保護	應設立保全區域，以提供特殊安全需求，保護辦公室、房間及設施。	此三項目屬保護、防範的措施，考量施行單位的能力許可，在此將三項所包含的各項防範措施，合併成一項。
A.9.1.4	預防外部與環境威脅	預防火災、水災、地震、等自然災害以及人為災害的可能性。	
A.9.1.5	在保全區域內工作	在保全區域內工作時應採取額外控制措施及指引，以強化該保全區域之安全性。	
A.9.1.6	隔離的收	裝卸區應予管制，若可能，應與資訊處理	考量施行單位業務的需求以及

	發與裝卸區	設施隔離，避免遭未授權進入。	空間的限制，加上只要確實建立安全區域，配合適當的控制措施，無須額外建立裝卸區，因此予以刪除。
A.9.2.5	場外設備之安全	學校區域外之設備,應使用安全流程及控制措施，以保護其安全。	一般施行單位顯少擁有區域外設備之情事，若有也是委託相關單位或廠商管理，故無須在額外擔負區域外設備之安全職責。
A.10.4.2	可攜式程式之控管	為防制未經授權的可攜性程式執行,應制定資安政策來對可攜性程式實施授權。	針對一般程式或軟體已有控管之措施，另也限定施行單位人員在非授權下的行為，所以此項目予以刪除。
A.10.8.1	資訊交換政策與程序	應針對所有類型的資訊交換制定正式的政策及程序。	資訊與軟體交換協定可制定於政策及程序之內，因此，將此兩項予以合併。
A.10.8.2	交換協定	在單位以及外部單位之間建立資訊與軟體交換協定。	
A.10.8.3	儲存媒體運送過程之安全	運送之儲存媒體應予保護,防止未授權遭存取、誤用或毀損。	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。
A.10.9	電子商務服務	確保電子商務服務的安全,以及被安全的使用。	由於 10.9.1 和 10.9.2 予以刪除，而 10.9.3 內容可與 10.8 合併，因此將 10.9 刪除。
A.10.9.1	電子商務	制定包括電子資料交換、電子郵件和線上交易等電子商務行為之控管措施。	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，因此予以刪除。
A.10.9.2	線上交易	線上交易資訊應保護防止不完全的傳送、誤傳、未授權的資訊變更、洩露、複製及重傳。	線上交易亦屬於電子商務的一環，因此依據上一條款之理由，予以刪除。

A.11.1	存取控制之營運要求	管制資訊之存取行為	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
A.11.1.1	存取控制政策	存取控制之企業要求應予鑑定及文件化,存取行為應僅限於存取控制政策內定之範圍。	
A.11.3.1	使用者通行碼管理	使用者選擇及使用通行碼時,應遵守機關資訊安全規定。	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。
A.11.3.2	無人看管之資訊設備	應要求使用者確保無人看管之資訊設備有適當保護措施。	無人設備已制定保護措施條款，使用者職責亦已制定，此條款可予刪除。
A.11.4.3	網路設備鑑別	應用網路設備的鑑別器指示是否可以被允許連接至網路	這部份的設備在各連線學校中，較少有應用的機會，所以予以刪除。
A.11.5.2	使用者識別與身份鑑別	所有使用者應有專屬識別符碼(使用者識別序號），以便追蹤責任歸屬。應選擇一適切的身分鑑別技術,以證實使用者宣稱之身分。	在一般施行單位的環境，使用者身份的鑑別技術難以實行高精密度的驗證流程，加上已有存取管理條款規定使用者註冊的流程，因此將此項刪除。
A.11.5.5	終端機自動關機時間	終端機若置於危險場所或所登入之系統風險極高,則閒置時應於一定時間後自動關機，避免遭未經授權存取。	一般施行單位鮮少會有所謂的危險場所或是將終端機設立在該環境內，加上未授權存取已有條款控制，所以在此予以刪除。
A.13.1.1	通報安全事件	安全事件應循適當管理途徑儘快通報。	由於安全事件或安全弱點皆需盡速進行通報程序，所以將兩項予以整合。
A.13.1.2	通報安全弱點	應要求資訊服務之使用者在注意到系統(服務)有任何明顯(可疑)安全弱點(威脅)時逕行通報。	
A.14.1.1	營運持續管理過程	全組織持續營運措施之制定與維護作業，應有管理之過程。	營運持續規劃框架須予以建立，再行訂定管理過程，故在此

A.14.1.4	營運持續規劃框架	應維持單一營運持續計劃之框架,以確保所有計畫皆一致,並鑑別測試及維護之優先順序。	將兩項合併。
A.14.1.2	營運持續及衝擊分析	為整體的達成營運應根據適當風險評鑑制訂持續，一份策略計畫。	一般施行單位較難進行專業之風險評鑑，應只須定期修改、維護永續運作計畫即可，因此予以刪除。
A.14.1.3	持續計畫之撰寫及實施	應擬訂計畫以在重要企業過程中斷或失效時，維護或即時恢復企業營運。	由於永續運作計畫之擬定本意就是於中斷或失效時即時恢復運作，所以此項有所重複，予以刪除。
A.15.1.2	智慧財產權	應實施適當流程,以確保遵守有關智慧財產權資料之使用及專利軟體產品使用之法律限制。	此四項皆是關於遵守各項法律條款以及採取適當控制措施之項目，故在此與以合併。
A.15.1.3	組織紀錄之保護	組織重要紀錄應予保護，以防止遺失、損毀及偽造。	
A.15.1.4	個人資訊的資料保護及隱私	應根據相關法令採取控制措施保護個人資訊。	
A.15.1.5	預防資訊處裡設施遭誤用	資訊處理設施之使用需經管理階層授權,且應採取控制措施防止該設施之不當使用。	
A.15.1.6	密碼控制措施之規定	應有控制措施以確保符合國家協議、法律規範,或以其他工具管制密碼控制措施之存取或使用。	在系統開發與維護之安全一項已有類似的密碼控制措施政策可規範之，故在此予以刪除。