國立雲林科技大學

資訊安全與個人資料保護稽核作業計畫書

提報單位

資訊中心

中華民國 102 年 8 月 6 日

目錄

壹、總則

一、目的

資訊安全與個人資料保護稽核作業目的為：

(一)、確保本校資訊安全管理制度之推動，建立適當管理架構，有效分配資訊安全責任，落實資訊安全政策之推行、協調各項資訊安全措施之實施，確保資訊安全制度之防護水準。

(二)、因應個人資料保護法的施行，為遵守個人資料之蒐集、處理及利用之生 命週期規範，以避免人格權受侵害，促進個人資料之合理使用。

二、依據

99 學年度第 2 學期第 1 次內部控制專案小組會議紀錄辦理事項。

三、目標

利用內部控制資訊安全機制，有效運用資訊資源，採行適當安全管理控制措施下，每學期抽查 10~15 個單位執行稽核作業，維持並持續改善本校資訊安全，保護資訊資產的機密性、可用性與完整性；及落實個人資料保護規範，避免個資外洩，保障個人的隱私權。

四、稽核準則

稽核項目為個人電腦使用安全設定、資產(個資)盤點、軟體使用安全、單位伺服器、委外廠商管理、實體與環境安全、個人資料保護、通訊與作業、資訊安全事件、法規遵循性；稽核作業依據下列相關規定為基礎引申訂定之：

(一)、教育部「校園通用資安管理原則」。

(二)、「102 年度教育機構個人資料保護工作事項」。

(三)、「教育體系資通安全管理規範」與個資相關重點。

(四)、教育部所屬機關及各級公私立學校資通安全工作事項。

(五)、視教育部訂定之相關規定修訂本校之作業規範。

五、稽核範圍

本校一、二級單位辦公室與實驗室(含電腦教室)

六、稽核進行方式

(一)、每學期辦理 1~2 次稽核說明教育訓練。

(二)、稽核小組擬定稽核計畫，陳請資安長核定。

(三)、每學期抽查 10~15 個單位，並以發生資安事件及擁有大量個資檔案之單位列為優先稽核。

(四)、受稽單位需針對稽核缺失擬定矯正預防處理計畫與執行改善措施。

七、稽核成員:

稽核小組：由資訊中心 2~3 人組成，成員須接受過資安相關稽核訓練者。

八、教育訓練與人員職責

(一)、教育訓練業務負責單位：資訊中心

(二)、教育訓練期程

每學期辦理 1~2 次稽核說明教育訓練。

(三)、資安與個資聯絡人

各單位主管指派一名，參加稽核規範教育訓練，瞭解資訊安全管理制度概念及實作方法,爾後協助組織內部人員實施資安規範與紀錄，配合資安與個資稽核作業,協助將資訊風險降低至可接受之程度內，期能建立一個較安全、可靠的資訊安全環境。

(四)、其他人員：接受資訊安全教育訓練與執行資訊安全防護措施。

九、資安與個資保護網頁專區

資訊中心設置網頁專區，供大眾閱覽資訊安全與個人資料保護相關資訊。

網址：http://isms.yuntech.edu.tw

十、獎勵及改善

(一)、獎勵標準

各單位資安與個資聯絡人，於原有業務外再協助配合資通安全管理作業，擬由資訊中心依表現情形，簽請獎勵建議。

(二)、矯正預防處理時機

1. 平日執行安全規範發現之缺失，由單位自行填寫並改善後，存檔備查。
2. 稽核時發現之缺失,應於十個工作天內填寫「矯正與預防處理單」（表單編號：YUNTECH-ISPI-D-019）回覆資訊中心，列為追蹤稽核項目。

貳、資訊安全政策

一、目的

為建立安全及可信賴的資訊環境，以確保資訊資產的機密性、可用性與完整性，採取適當的控制措施，確保資訊的適當安置及資訊安全實務作業的可行性與有效性。

二、目標

為維護本校資訊資產之機密性、完整性與可用性，保障使用者資料隱私之安全。期藉由共同努力以達成下列目標：

1. 保護本校業務服務之安全，機密性資料須確保需經授權人員才可存取資訊，以確保其機密性。
2. 保護本校業務服務之安全，避免未經授權之修改，以確保其正確性與完整性。
3. 確保本校各項業務服務之執行須符合相關法令或法規之要求。

三、責任

1. 管理階層應積極參與及支持資訊安全管理制度,並透過適當的標準和程序以實施本政策。
2. 本校之內部人員、委外服務廠商與訪客等應遵守本政策。
3. 本校之內部人員、委外服務廠商與訪客等有責任透過適當通報機制,通報資訊安全事件或弱點。
4. 任何危及資訊安全之行為,將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行議處。

四、資訊安全管理範圍

本政策適用範圍為本校之內部人員、委外服務廠商與訪客等。

資訊安全管理範疇涵蓋九項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校造成各種可能之風險及危害，各領域分述如下：

1. 個人電腦資訊安全守則
2. 伺服器資訊安全管理
3. 資產(個資)盤點及業務流程
4. 個人資料保護管理
5. 通訊與作業管理
6. 實體與環境安全控管
7. 委外廠商管理
8. 資訊安全事件處理
9. 法規遵循性

參、資通安全與個人資料保護注意事項

一、個人電腦使用安全守則

個人電腦定義：含桌上型電腦、共用之公共電腦、可攜式電腦、伺服器等。

(一)、個人電腦使用原則：

1. 時常檢查電腦是否有不明程式啟動執行。
2. 不要開啟無法確定及不必要的服務，如.exe, .scr, .vbs…等，避免遭受植入木馬程式。
3. 定期檢視更新系統安全修補、防毒軟體及防毒碼，保持更新至最新狀態，勿自行關閉系統自動更新程式，以維持系統正常運作。
4. 公務電腦設備不可任意架站或做私人、營利用途。
5. 電腦設備應隨時保持清潔，避免髒污、灰塵造成設備損壞或公共危安，下班前，不需使用之設備應先行關機始得離去，電腦關機應依正常程序操作。
6. 電腦附近應避免放置茶水、飲料、細小文具用品等物品，以免造成電腦設備損壞。
7. 桌面勿放置 IP、序號、帳號、密碼及個資等文件，長時間離開座位時重要資料及可攜式媒體請置放於安全場所。
8. IE、Firefox 等相關瀏覽器安全等級應設定為中級或更高，並關閉快顯功能、ActiveX 等主動執行功能及封鎖彈跳視窗，執行特殊程式時如須先降低安全性或需加裝外掛功能，請先進行安全檢查及管理。
9. 電子郵件軟體應關閉收信預覽功能，請勿任意開啟不明來源的電子郵件，爲避免惡意連結及圖片危害請使用文字模式閱讀信件。(請參閱「郵件軟體防護安全設定」，http://webmail.yuntech.edu.tw/mailpre.pdf)
10. 個人電腦不使用時，需採用密碼保護、鎖定或登出離線等安全措施。
11. 電腦應採用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 10 分鐘以內。
12. 非公務必要使用時，請勿開啟網路芳鄰分享目錄與檔案，並停用 Guest 帳號。
13. 使用文書處理軟體(包括 Word、Excel、PowerPoint 等)應將巨集安全性設定為高級或更高，若執行特殊程式時如須降低安全性，請先執行安全性評估作業。
14. 禁止使用點對點互連(P2P)、tunnel相關工具或任何有危害單位網路、設備 及造成網路壅塞佔用頻寬等軟體及架站軟體(FTP)作私人用途。係因教學與研究所需使用P2P軟體，請依學校規定另外提出申請。
15. 安裝 Win7 作業系統之電腦連線至網路時，網路位置應設定為公用網路。此安全等級將不讓周圍的其他電腦看到，並有助保護電腦不受網際網路上任何惡意軟體的危害。
16. 使用個人電腦設備儲存、處理、傳輸機密資料（含個人資料）時，應作加密機制處理。
17. 應定期備份個人電腦設備內重要文件及資訊，各種備份工具(如軟碟、磁帶、

抽取式硬碟等），需存放於安全之地點。

18. 個人電腦請關閉插入可攜式儲存媒體或光碟時之自動執行功能（Autorun）。
19. 應避免使用非本校防護範圍內(本校各辦公室)之網路及電腦設施辦理公務，若確有其必要使用外部(如住家、公共場所)資訊環境，請確認資訊使用環境是否具備下列防護措施:
    (1) 儲存於攜帶式儲存媒體(如行動碟)之公務相關電子檔案應予加密。
    (2) 使用之連網電腦設備應安裝防毒軟體(含最新版之病毒碼更新)及防火牆，並應保持啟動運作狀態。
    (3) 處理公務之電腦設備以不連上網路為原則(使用本校網路應用系統除外)，同時於處理完畢後應將公務相關電子檔案移除，且避免存放於主機。
20. 應隨時清理個人電腦的資源回收筒，確保已經刪除的重要資料不會因遺留在資源回收筒未清理，而遭未經授權之使用。
21. 微軟公司自本(103)年 4 月 8 日起終止 XP 作業系統之支援服務,為避免滋生資安漏洞，請依「因應微軟公司 Windows XP 作業系統終止支援服務之防護措施建議」（表單編號：YUNTECH-ISPI-D-022），預為規劃並管制落實相關防護措施。

(二)、密碼設定原則：

1. 電腦設備應設定帳號密碼並定期檢查，密碼建議每 6 個月更新一次。
2. 密碼設定原則密碼建議長度至少 8 個字元，且包含文數字等。建議可採用包含大寫及小寫字母、數字、標點符號、特殊字元之組合以增加複雜度。
3. 密碼之設定不得與帳號相同。
3. 妥善保管帳號及密碼，不隨意透漏或提供給他人使用；勿將密碼記載在他人垂手可得之地方，如：貼在螢幕上。
4. 懷疑密碼外洩，立即變更密碼。

(三)、軟體使用安全：

1. 請勿下載、安裝或使用來路不明、未經授權或影響電腦網路環境安全之電腦軟體。
2. 進行下載、複製、使用軟體或不明來源檔案前，應先完成掃描檢查是否具有惡意軟體，確認檔案安全無虞，嚴禁任意移除或關閉防毒軟體。
3. 移除電腦設備中非法或未經受授權軟體、音樂、影片檔等。
4. 公務用電腦設備安裝軟體時，注意下列事項：
    (1) 安裝全校授權軟體時，請先參閱資訊中心授權軟體清單（http://tcx.yuntech.edu.tw/index.php?option=com_content&task=view&id=822），並確認其授權版本，避免使用無授權及非法軟體，以落實使用合法軟體。
    (2)安裝自購軟體，請注意其授權數量、範圍、使用期限，與取得合法授權證明或相關佐證(授權序號或授權資料網頁)，以確認所使用軟體之合法性。

(四)、個人電腦安全相關設定，請參閱「個人電腦安全操作作業說明書」。

(五)、每年定期執行上述個人電腦安全設定後，請填寫「個人電腦資訊安全自我檢

查表」（表單編號：YUNTECH-ISPI-D-001），檢查結果為”否”之項目，請再依「個人電腦安全操作作業說明書」落實安全設定。使用者確實設定完成於檢查表簽章後，逕送單位資安與個資聯絡人彙整留存。

二、伺服器資訊安全管理

（一）、各行政及教學單位對外開放網際網路服務之伺服器，應符合「國立雲林科技大學伺服器管理辦法」之規定。

（二）、設定防火牆以控管外界與單位內網路間之資料傳輸與資源存取，應符合「國立雲林科技大學防火牆系統管理規範」，並關閉不使用的通訊埠，以避免病毒感染及駭客攻擊。

（三）、開放外界連線作業之伺服器主機，應避免外界直接進入資訊系統或資料庫存取資料。

（四）、伺服器主機管理之安全性，應視需要之使用情況，加密通道（如 VPN、SSH）等各種安全控管技術。

（五）、各單位開發之系統及網站(含委外開發)，應於完成後，先執行弱點掃描與完成修補風險弱點始可上線；運作中網站亦請定期進行必要的系統及網站弱點掃瞄，相關檢測事項請依「網站應用程式弱點檢測管理要點」辦理。

（六）、每次掃描完成後應產出弱點掃描報告與進行相關漏洞修補，並填寫「弱點處理報告單」(表單編號：YUNTECH-ISPI-D-002)，修補後應進行複掃，確保弱點均已處理無遺漏。弱點若因故無法修補，應於「弱點處理報告單」說明無法修補之原因與防禦因應方法。

（七）、伺服器管理者應於每工作日時依「系統與網路巡查紀錄表」(表單編號：YUNTECH-ISPI-D-003)所列項目檢查重要系統主機狀況，以確保系統正常運作。

（八）、重要系統設定檔、網頁資料、伺服器檔案、資料庫及機敏性檔案資料均應訂定備份週期，並依據週期執行系統排程或手動備份。備份宜以加密方式保護，備份狀況記錄於「備份狀況紀錄表」(表單編號:YUNTECH-ISPI-D-004)。

（九）、伺服器結束遠端系統維護作業後，應關閉應用系統及網路連線，並清除螢幕上的資訊，將作業系統登出。

（十）、檢視各設備中系統之時間是否一致，並進行校正及同步作業。

三、資產(個資)盤點及業務流程

(一)、各單位應鑑別所管轄設備，含已申請報廢仍繼續使用之資訊資產，並建立「資訊資產清單」（表單編號：YUNTECH-ISPI-D-005）（以下所稱之資訊資產清單內含「單位內部保有及管理個人資料之項目清查表」）。

(二)、每年至少進行乙次資產盤點與資訊資產清單覆核，以更新及確保資訊資產清單的正確性及完整性。

(三)、資訊資產分類規則：

1. 資訊資產依其性質不同，分為三類：軟體、硬體、個人資料。

(1)軟體（Software / SW）：作業系統、應用系統程式、套裝軟體等。

(2)硬體（Hardware / HW）：主機設備等相關硬體設施，如個人電腦、共用之公共電腦、可攜式電腦、伺服器等。

(3)個人資料(Personal Information)：儲存於硬碟、磁帶、光碟等儲存媒介或以紙本形式存在之文書資料、報表等紙本文件，含直接或間接蒐集之可直接或間接方式識別個人之資料。

(四)、資訊資產編號及標示規則：

1. 軟硬體資訊資產編碼方式，第1~3碼為單位別，第4~5碼為資產類別，第6~8碼為資訊資產流水編號。例：XXX-XX-XXX。
2. 個人資料特定目的包括法律、法規命令、行政規則及行政計畫等在內。個人資料類別請參照法務部85年8月7日法令字第19745號，請詳填該特定目的項目之名稱及代碼。

(五)、資訊資產盤點說明

1. 軟、硬體

清查辦公室、實驗室之全部電腦設備(含桌上型電腦、共用之公共電腦、可攜式電腦、伺服器等)及軟體，逐一編碼記錄於資訊資產清單，另將該電腦設備之IP位址及安裝軟體名稱(含作業系統、應用系統程式、套裝軟體)一併列入清單中。

2. 個人資料

清查直接或間接蒐集之可直接或間接識別該個人資料的所有紙本文件及電子檔。

(六)、以直接或間接方式蒐集之個人資料後，遵循個人資料保護法第十七條規定，填寫「個人資料新增報告書」（表單編號：YUNTECH-ISPI-D-006）於簽章後連同電子檔，逕送資訊中心網路組彙整留存並公告於「資安與個資保護」網站上供大眾閱覽。

(七)、每年執行乙次個人資料清查，完成後請填寫於「單位內部保有及管理個人資料之項目清查表」（表單編號：YUNTECH-ISPI-D-007），並在紙本上用印後，將紙本連同電子檔逕送資訊中心個資聯絡窗口人員彙整。

(八)、每年執行乙次資訊系統分級分類，填報「資訊系統安全等級評估表」（表單編號：YUNTECH-ISPI-D-008），鑑別資訊系統安全等級，針對掌握保護重要標的，採行安全防護措施。鑑別內容包含：識別資訊類別、設定影響構面等級、識別業務屬性並檢視安全等級、設定資訊系統安全等級。

(九)、資訊資產之報廢（或銷毀）應依「實體與環境安全控管」之相關規定，採取適當之方式進行銷毀。

四、個人資料保護管理規範

(一)、個人資料使用管理：

1. 蒐集個人資料時，明確告知當事人機關名稱、蒐集目的、個人資料之類別、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。
2. 蒐集個人資料應符合特定之目的，並確保資料之正確性、完整性和時效性。
3. 當事人可以行使之權利及方式，例如當事人可請求查詢、閱覽、製給複製本、補充、更正、刪除、停止蒐集、處理或利用（表單編號：YUNTECH-ISPI-D-023）。
4. 向當事人說明可自行判斷是否提供個人資料，若為本校提供服務時所必須之資訊，因而造成無法提供該服務情形時，當讓當事人瞭解對其個人權益之影響。
5. 蒐集個人資料時，需經適當之授權與監督並僅就所需之必要欄位進行收集。經授權同意交換個人資料時，電子類文件需對資料檔案加密或透過加密通道傳送、紙本類文件以彌封或其他安全方式進行傳遞交換工作。傳遞接收個資之承辦人需將列印、轉交等行為登載於「個人資料簽收紀錄」(表單編號：YUNTECH-ISPI-D-009)。
6. 校內各單位因公務作業所需人事資料時，請填寫「人事資料需求表」(表單編號：YUNTECH-ISPI-D-020)，逕向人事室提出申請，經授權同意後，依「個人資料保護法」規定辦理。
7. 當個人資料蒐集範圍逾法律、法規命令、行政規則及行政計畫(教育主管機關法令規範、學則等規定)，或係依作用法、組織法所定執行法定職務者之特定目的外，應依個資法規定取得當事人之書面同意。書面同意範本請參閱「個人資料蒐集、處理、國際傳遞及利用同意書」（表單編號：YUNTECH-ISPI-D-010），範本內容可依單位需求修改。
8. 個人資料若非經資料當事人之書面同意或經法令規定許可，不得任意揭露、販售或用於蒐集時的特定目的以外之用途。
9. 非由當事人提供之個人資料，得於處理或利用前向當事人補行告知義務，告知方式得以書面、電話、傳真、電子文件或其他適當方式為之。
10. 個人資料之處理行為需經單位主管核准，宜釐定使用範圍及調閱或存取權限。個資存取時應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，並留存可識別之發送紀錄需及個資使用者身分以供事後稽查。
11. 使用者經正式授權存取個人資料檔案時，其帳號必須為唯一，避免共用帳號。
12. 以電腦處理個人資料時，需核對個人資料之輸入、輸出、編輯或更正是否與原件相符。個人資料提供利用時，對資料相符與否如有疑義，應調閱原始檔案查核。
13. 針對有備份必要之個人資料，除有必要時採取加密機制，存放重要機敏資料之備份媒體亦應以適當方式保管，且定期執行資料回復測試，以確認備份資料之可用性。

14. 禁止使用即時通訊軟體、外部信箱（如奇摩信箱、Gmail、Hotmail等）傳輸及存取個人資料檔案，利用校內信箱（webmail）傳輸個人資料時請加密保護與留存追查紀錄。

15. 各單位管理之網站或網頁內容，於確有必要公布個人資料時，需經單位主管核准，且依相關法律及規範處理，始得公布。

(二)、本校個人資料保護聯絡窗口

個資保護聯絡窗口:

資訊中心網路組陳珮芸行政助理

聯絡電話:05-5342601分機2653

電子郵件：pdp@yuntech.edu.tw

辦理事項如下：

1. 本校與公務機關間個人資料保護業務之協調聯繫及個資安全事件通報。
2. 本校發生重大個人資料外洩事件聯繫窗口。
3. 本校各單位之其他重大個人資料保護管理事項聯繫處理。
4. 公告本校保有個資項目於「資安與個資保護」網站上供大眾閱覽。

(三)、學術研究個資之處理方式：

1. 所需研究資料若涉及個人資料範圍時，請注意下列事項：
   (1)資訊中心並非個人資料的擁有者，僅是代管者，如未經適當合法程序，不宜擅自散布資料。
   (2)未涉及個人資料者，請以專簽會資訊中心辦理，資訊中心將依「去識別化」之工作負荷提出會簽意見，待校長核可後，再依資訊安全管理制度之規定填具資料需求表(如提供研究使用,要另行加註明及需另填保密合約切結書)。
   (3)涉及個人資料者，主管機關會依據個人資料保護法內容，針對學術研究資料進行詳細規範，供遵循辦理。

(四)、個資處理人員管理：

1. 處理接觸機敏資料人員，應簽署「保密切結書」（表單編號：YUNTECH-ISPI-D-011），克盡保密之責，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。
2. 禁止人員在社群網站、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。

(五)、個人資料外洩(竊取、洩露、竄改或其他侵害事件)處理流程：

1. 立即通知本校個人資料保護聯絡窗口。
2. 個資外洩單位以最速件級別專簽會資訊中心辦理。
3. 發生個資外洩事件，即時以書面、電話、傳真、電子文件或其他足以使當事人知悉或可得知悉的方式，通知個人資料受侵害項目、產生之影響及已採取之因應措施。
4. 事件發生 36 小時內復原或完成損害管制，並填報「資訊安全事件通報單」回覆資訊中心。（表單編號：YUNTECH-ISPI-D-018）

（六）、蒐集、利用及處理個人資料時，請務必遵守「個人資料保護法」，確實妥善保管所取得之個人敏感性資料。個人資料管理人若違反個人資料保護法規定者，將受法律制裁；其他未盡事宜，悉依個人資料保護法之規定辦理。

（七）、每半年各單位資安與個資聯絡人請填寫「個人資料保護檢核表」（表單編號：YUNTECH-ISPI-D-012），確保單位內部個人資料受到保護，作業程序依規範辦理執行。

五、文件管理

（一）、資安與個資聯絡人協助管制、保管、維護、建檔稽核計畫內相關文件，將其鎖在安全的儲櫃或其他安全場所，並建立「資訊安全管理文件列表」（表單編號：YUNTECH-ISPI-D-013）列管。文件發送對象應以最低必要的人員為限。

（二）、文件須分類歸檔，並依使用者職權賦予適當之文件存取權限，對於具機密性資料及文件，於文件、表單上載明為「限閱文件」，應特別控管以避免資料外洩。

（三）、表單或紀錄至少需保留一年，且考慮單位或法律上資料保存期限之要求。

（四）、單位承辦人保有之個人資料之紙本文件，不需使用時應置放於上鎖之安全儲櫃或其他安全場所內，避免有心人士或非授權人員拿取。

（五）、使用影印機、印表機、傳真機、掃描機或多功能事務機後，應立即將紙本資料取走。

（六）、含個人資料之紀錄紙本文件請依相關法令規定或契約保存年限保管，不再使用時請銷毀或依相關法令規定妥善處理，個資文件保留以最小化為原則。

（七）、文件之報廢（或銷毀）應依「實體與環境安全控管」之相關規定，採取適當之方式進行銷毀。

六、通訊與作業管理

(一)、儲存管理：

1. 電腦儲存設備、可攜式資訊媒體若需連接資訊媒體設備或網路時，應先進行電腦病毒掃瞄，確認無問題後始可使用。
2. 電腦儲存設備、可攜式資訊媒體如為單位內共同使用，使用者切記在使用完畢後將所有的資料文件移除，以免資料遭他人誤用。
3. 機敏性資料若儲存於電腦儲存設備、可攜式資訊媒體，應考量使用加密技術或其他技術加強安全控管。
4. 重要之儲存媒體(含機敏性資料之電腦儲存設備)、可攜式資訊媒體，不使用時應置放於實體安全區域及環境（如：門禁控管辦公區域內之上鎖之防潮箱、書櫃）或由專人管理，僅經授權或簽署保密協議後方可使用。
5. 非公務需求不得將載有機敏性資料之可攜式資訊媒體攜出辦公場所。
6. 電腦儲存設備、可攜式資訊媒體所使用之密碼或編碼技術不應透露予與業務無關之人員。
7. 電腦儲存設備、可攜式資訊媒體遞送前應加以妥善包裝保護，避免發生實體損壞。
8. 外部團體或個人更新或維修電腦設備時，應指派專人在場，確保個人資料之安全及防止個人資料外洩。

(二)、存取管理：

1. 使用者職務異動或離職時，應即時通知相關單位調整或終止使用者之存取權限。並將其所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。
2. 依執行業務需透過校務行政系統存取相關資料時，請依學校規定提出申請。
3. 應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制。例如新增、刪除或執行等。
4. 特殊權限之授權管理，必須依執行業務系統別需求，例如作業系統、資料庫管理系統、網路服務系統、監控管理系統等賦予系統存取特殊權限的授權，且以執行業務及職務所必要的最低資源存取授權為限。
5. 使用者經正式授權存取業務相關之系統資料時，其識別資料與帳號必須為唯一，禁止借用他人之帳號或共用帳號。
6. 重要資訊系統及特殊權限之存取帳號之密碼變更期間應較一般權限之帳號頻繁。
7. 使用者或委外廠商之人員如因作業需求，需對系統進行存取，請填寫「資訊服務申請表」提出申請，經主管授權或允許執行存取作業。「資訊服務申請表」（表單編號：YUNTECH-ISPI-D-015）中應載明作業需求內容、所需權限、帳

號有效時間，由系統管理者依照所需權限及帳號有效時間，建立必要之帳號供使用。

七、實體與環境安全控管

(一)、安全管理：

1. 無人時或下班最後一人離開時，需將辦公室關門上鎖。
2. 為確保相關設施之安全，非單位指定之人員不得擅自進入機房或使用相關資訊設備。
3. 於單位安全區域與辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並儘速通知相關單位進行處理。
4. 若外部人員或單位內部未具機房或管制場所進出權限之人員，因執行業務需求進入該場所時，應指派人員隨行並填寫「人員進出機房登記表」(表單編號：YUNTECH-ISPI-D-016)後方可進出。

(二)、報廢管理：

1. 報廢後移作他用之電腦設備，請移除所有軟體(含作業系統與應用軟體等)並清除儲存之資料內容。
2. 儲存機敏性資料檔案之電腦或相關設備，於報廢或移轉他用時，應利用資料清除軟體工具，清除儲存之內容，確認所儲存之資料已清除且無法還原閱讀其內容。
3. 軟、硬體資訊資產報廢時，應更新修改「資訊資產清單」，經單位主管審核並確認資料、軟體清除後，方可進行資訊資產報廢程序。
4. 機敏性文件廢止時，請依相關法令規定妥善處理。個資文件之廢止須填寫「個人資料銷毀申請表」(表單編號:YUNTECH-ISPI-D-014)，經單位主管核可銷毀後，逕行通知資訊中心網路組。
5. 機敏紙本文件不再使用時，嚴禁挪為廢紙回收再使用，應以碎裂方式進行破壞使其無法閱讀識別，並刪除電子檔。

八、委外廠商管理

(一)、委外、租賃或購買套裝應用資訊系統時，請依「國立雲林科技大學委外、租賃或購買套裝應用資訊系統注意事項」辦理。(表單編號：YUNTECH-ISPI-D-017)

(二)、委外廠商於支援執行業務時，處理之個人資料或獲知敏感等級(含)以上資訊，應遵守「個人資料保護法」及本校之相關規定，不得對外透露、任意複製或攜出機密性之業務資料，為確保前述事項之落實，要求廠商及其人員簽署「保密切結書」(表單編號：YUNTECH-ISPI-D-011)，更換廠商或人員時亦同。

(三)、 針對涉及個資的委外作業，委外廠商視同委託機關，屬個資法適用範圍內。應重新審閱委外合約，於委外合約中載明所處理之個人資料保密義務委外廠商有相當的要求與管控資訊安全相關責任及違反之罰則。

(四)、於專案期間，本校可透過稽核等方式監督委外廠商之個人資料管理作法，如個資蒐集、處理、利用、傳輸與銷毀之管理情形。

(五)、與委外廠商所簽訂正式書面協議或契約中，應明確陳述契約終止時，相關個人資料的銷毀或交還程序。

(六)、自行開發或委外處理個人資料檔案之資訊系統，避免以真實個人資料進行測試，如需使用，完成測試作業後立即移除，或將可辨識之個人資料修改為無法辨識之模糊資訊。

(七)、宜避免允許維護人員或系統服務廠商以遠端登入方式進行牽涉機敏性資料的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密通道進行（如：HTTPS、SSH等），及權限控管及留存稽核紀錄。

(八)、委外廠商履行合約應提供其使用之軟體，且均須為合法軟體，並不得違反智慧財產權之規定，如有違反事情發生，委外廠商須承擔所有法律責任。

(九)、委外廠商所使用之工具軟體、處理作業之執行紀錄及異常處理記錄應留存，本校有權進行稽核，廠商不得異議。

(十)、委外廠商人員對於系統帳號應善盡保管之責，系統帳號不得任意交由非作業相關人員使用。

(十一)、委外廠商相關系統之開發或負責人員離職時，應繳回其所借用之設備、軟體及終止作業權限。

(十二)、委外廠商人員，於進行開發或維護軟硬體作業時，需視處理程序中之可能風險，採取適當的安全控制措施，並條列安全規定於正式合約中。

(十三)、委外廠商需針對交付之系統，應保證系統內不含後門程式、隱密通道及特洛伊木馬程式。

九、資訊安全事件

網路異常事件處理（含智財權侵權處理）

(一)、接獲教育部、區網中心或經其他單位檢舉通知資訊安全事件通知後，資訊中心將立即管制異常的主機之網路連線。

(二)、依據「國家資通安全會報通報與應變作業流程」規範，事件影響等級處理時程如下：

1. 4、3級事件：發現事件後36小時內復原或完成損害管制
2. 2、1級事件：發現事件後72小時內復原或完成損害管制

（資訊安全事件等級說明請參閱「資訊安全事件通報單」表單）

(三)、各檢舉來源處理方式：

1. 被網路檢舉者，提供abuse資安網站(http://abuse.yuntech.edu.tw)讓被檢舉者回報處理情況。
2. 被電子郵件檢舉者，透過電子郵件方式回覆本校abuse 帳號處理。
3. 被書面檢舉者,請侵權主機使用單位協助了解並儘速處理。並依資訊中心 規定回覆填寫「資訊安全事件通報單」（表單編號：YUNTECH-ISPI-D-018）。

(四)、情節重大者，聯絡該IP 使用者通知該導師或指導教授輔導，給予正常的法律認知後。經使用單位回覆處理狀況，確認問題已經處理後，方能解除對違規主機之網路封鎖。

十、法規遵循性

校內相關法規

伺服器管理辦法	個人電腦及網路使用注意事項
委外、租賃或購買套裝應用資訊系統注意事項	電子郵件信箱使用規範
防火牆系統管理規範	校園網路使用規範
電腦教室管理辦法	

政府機關資訊安全相關法規

教育部「校園通用資安管理原則」	著作權法
教育部所屬機關及各級公私立學校資通安全工作事項	刑法第 36 章妨害電腦使用罪
教育體系資通安全管理規範	國家機密保護法
行政院及所屬各機關資訊安全管理要點	國家機密保護法施行細則
個人資料保護法	政府資訊公開法
個人資料保護法施行細則	單位業務所屬主管機關之相關法令規範