耕莘健康管理專科學校

資訊安全暨緊急應變管理規範

中華民國 103 年 10 月 13 日資訊安全推動小組會議通過
中華民國 104 年 04 月 27 日行政會議通過
中華民國 105 年 05 月 23 日行政會議修正通過
中華民國 106 年 9 月 25 日資訊安全推動小組會議通過
中華民國 106 年 10 月 23 日行政會議通過
中華民國 107 年 4 月 30 日資訊安全推動小組會議通過
中華民國 107 年 5 月 28 日行政會議通過

目　錄

壹、總　則

一、依據

政府機關（構）資通安全責任等級分級作業規定及教育體系資通安全暨個人資料管理規範和本校資訊安全管理辦法辦理。

二、目的

耕莘健康管理專科學校（以下簡稱本校）為明確本校各單位資訊安全作業權責及通報與應變作業，以維護網路資訊系統的正常運作、確保網路資訊傳輸安全，並保障本校電腦處理資料之可用性、機密性與完整性，特訂定本規範。

三、目標

（一） 建立安全資訊作業環境，執行全天候服務。資訊組應有永續服務的能力，不宜有作業停頓、蠕蟲攻擊、駭客攻擊毀損及監測資訊外洩等事件發生，故積極推動建置資訊安全管理制度(Information Security Management System, ISMS)，確保本校資訊安全。

（二） 強化本校資訊網路安全防護機制。

（三） 提供本校資訊安全專業諮詢與通報機制。

（四） 落實本校資圖中心資訊安全管理與防護措施的執行。

（五） 宣導資訊安全與推動資安機制，並定期或不定期檢測資安執行狀況，進行改善措施。

四、訂定參考

（一） 中央標準檢驗局 CNS17799、CNS17800 規範。

（二） ISO/IEC 17799:2000、BS7799-2:2002、27001:2005 國際標準。

（三） 行政院及所屬各機關資安事件通報應變作業規範

（四） 各政府機關(構)落實資安事件危機處理具體執行方案。

（五） 政府機關（構）資通安全責任等級分級作業規定。

（六） 行政院所屬各機關(構)資訊安全管理規範。

（七） 行政院所屬各機關(構)資訊安全管理要點。

（八） 教育體系資通安全暨個人資料管理規範。

（九） 個人資料保護法。

（十） 電子簽章法。

五、適用對象

本校師、生、員工、臨時約聘/雇人員及接受本校委辦案派駐本校之人員。

六、適用範圍

（一） 資訊安全政策制定及評估。
（二） 資訊安全組織及權責。
（三） 人員安全管理及教育訓練。
（四） 電腦系統安全管理。
（五） 網路安全管理。
（六） 系統存取控制。
（七） 密碼學(加密控制)。
（八） 供應者關係。
（九） 系統發展及維護之安全管理。
（十） 資訊資產之安全管理。
（十一） 實體及環境安全管理。
（十二） 業務永續運作計畫之規劃及管理。

貳、組織與權責

一、資訊安全推動小組

為統籌本校資訊安全政策擬定、推行及稽核、管理事宜，成立本校「資訊安全推動小組」(以下簡稱本小組)，由副校長擔任召集人，資訊組及本校各單位一級主管及師生代表組成。其中資訊系統安全控制技術事宜由資訊組負責辦理，資料及資訊系統之安全使用及保護與稽核事宜由各業務單位負責辦理。必要時，本小組得委請校內、外學者專家，提供資訊安全顧問諮詢服務及技術支援協助，校內學者專家為無給職，校外學者專家得支領車馬費。

二、資訊安全相關人員安全權責

（一）資訊安全長

1. 由副校長擔任。
2. 督導本作業計畫作業執行狀況及成效。
3. 核定資安事件通報及應變處理事宜。
4. 監督通報作業、應變計畫與資安演練之實施。

（二）資安聯絡人

1. 由資訊暨圖書中心資訊組網路系統管理人員至少二人擔任，並於「國家資通安全通報應變網站」登錄聯絡資料。
2. 負責對內、對外之資通安全聯繫事宜。
3. 隨時掌握國家資通安全會報或相關單位提供之資通安全危害通告資訊，發布資安訊息給校內各單位及系統使用者。

4. 與系統管理人員保持連繫，協同鑑定資通安全事件，並依程序進行通報作業。

（三）資訊設備使用人員

1. 泛指運用本校資訊及網路系統，進行電子化作業之各單位及使用者。
2. 使用人員應妥善保管個人電腦及其週邊設備，每日下班前應關閉電腦及電源。
3. 使用人員應設使用權限，進入系統不得任意更改使用權限，以確保系統安全，適時防範操作時之疏失。
4. 使用人員對通行密碼應妥慎保管，不得洩漏或借給他人使用。設有特殊權限之應用系統，使用人員如需代理人，則需另行申請使用權限及通行密碼。
5. 使用人員應定期自行進行系統線上更新。
6. 使用人員負有對系統服務及功能異常反應，及配合協助資安事件通報應變作業之責任。
7. 使用人員有參加資訊安全教育訓練之義務(依教育部規定之訓練時數)。

（四）網路系統管理人員

1. 定時統計本校網路使用情形並評估網路設備現況，以提高網路速率，提供擴充設備之憑據。
2. 建立及維護本校網路系統使用者帳號。
3. 記錄網路系統異常狀況及維護相關資料。

（五）應用系統維護人員

1. 負責使用者代碼管理、權限管理、病毒防制、稽核作業程序等，以落實應用系統安全策略之要求。
2. 維護人員進出系統皆須留存維護紀錄，應用系統本身須提供安全控管功能，以滿足作業時之認證、授權與稽核之安全管理需求，確保資訊安全。

（六）機房管理人員

1. 負責機房進出人員之管理、機房工作日誌之督導查核及機房異常狀況之管理。
2. 建立及更新機房配備圖，標明每一設備名稱及位置。
3. 建立機房電源操作手冊，以因應特殊狀況緊急開關電源之操作程序及相關耗材清理更換。

（七）委外業務之管理人員

1. 訂定受委託管理資訊系統存取控制規定，界定存取控制之需求，並以書面或其他電子方式記錄之。
2. 應將受委託管理資訊系統之存取控制需求，明確告知委外業務之服務人員，以利其執行及維持有效的存取控制機制。

3. 資訊系統存取控制規定之研擬，應考量事項如下：
   (1)個別業務應用系統之安全需求。
   (2)資訊傳佈及資料應用之名義與授權規定。
   (3)相關法規或契約對資料保護及資料存取之規定。
   (4)契約終止時，應確保本校資訊及資產安全回收或是銷毀的措施。

（八）委外業務之服務人員

1. 委外網管人員
   (1)建立及維護本校網路系統使用者帳號。
   (2)定期記錄網路系統異常狀況及維護相關書面資料。
   (3)建立及維持一份有權存取系統的委外人員名單。
2. 委外系統維護人員
   (1)應善盡軟硬體系統建置及維護的責任。
   (2)應尊重智慧財權及資訊公開的限制。
   (3)系統維護人員進出系統皆需留存維護紀錄，委外應用系統本身須提供安全控管功能，以滿足作業時之認證、授權與稽核之管理需求，確保資訊安全。

（九）資訊安全稽核人員

1. 由內部控制稽核小組具資訊背景成員，每年實施一次資訊安全作業流程內部稽核。
2. 由資圖中心同仁每半年實施電腦、網路及系統安全設定進行自我稽核。
3. 依據資安檢核表，提出改善建議事項。
4. 協助資安事件之偵防作業。
5. 依據本計畫及配合教育部所辦理之外部稽核，以及校內內部稽核作業，核定本校稽核計畫，對相關單位及人員進行資訊系統及技術應用之安全評估，以確保其遵循本校之資訊安全政策及管理規範。
6. 資訊系統擁有者應不定期執行資訊安全評估，檢討相關人員是否遵守相關資訊安全政策及規範。
7. 因應突發性、專案性及特殊性之資訊安全稽核，需不定期檢討評估各項軟、硬體設備的安全性；評估內容應包括作業系統的評估，以確保系統軟體及硬體的安全控制措施正確地執行。
8. 安全風險評估應由具有專業知識及豐富經驗的系統工程人員或委請外界學者專家協助，在權責主管人員的監督下，以人工或是自動化的軟體工具執行安全檢查，產生技術評估報告，以利日後解讀分析。
9. 依據奉核之稽核計畫，進行資訊安全稽核工作，必要時得不定期視需要進行專案稽核工作。本校及所屬單位資訊安全稽核由資訊暨圖書中心資訊組會同秘書室內部稽核小組主辦；本校暨所屬各單位均應配合資訊安全稽核工作之進行。

參、規範內容

一、資訊安全政策的制定及評估

（一）資訊安全政策之制定

1. 資訊安全政策的目的為防禦一切有計畫的、意外的、來自內部的或外部的威脅，以保護本校資訊資產的安全。為表達本校對資訊安全推動之支持與決心，制定資訊安全政策。
2. 制定之資訊安全政策應宣達至各階層之同仁，一體遵循。

（二）資訊安全政策與管理規範之評估

資訊安全計劃、政策、管理規範及相關管理辦法應每年進行獨立及客觀的評估，以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，確保資訊安全實務作業之可行性及有效性。

二、資訊人員安全管理與訓練

（一）人員安全管理

1. 本校進用人員之安全評估由人事室負責，如其工作職責須使用處理敏感性、機密性資訊的科技設施，或須處理機密性及敏感性資訊者，應經適當的安全評估程序。
2. 本校新進人員於報到時，需依照本校人事室規定填寫到職單，並簽署「保密切結書」。保密切結書涵蓋期間包括從業期間與離職後，均有保密之責任，任何因未遵守本校資訊安全計劃規範所導致之資訊安全意外事件將嚴格懲處，本校並保有法律追訴權。
3. 本校各委外開發維護之廠商人員，必須簽署「保密切結書」，遵守本資訊安全管理相關規範。
4. 系統使用、管理與維護人員應將系統相關帳號及密碼彌封交由單位主管保存、建立代理人帳號，並進行權限設定與移轉，以利主管稽核及職務代理人進行緊急應變作業。
5. 本校同仁離職、留職停薪與休職人員，應依不同業務性質於期限內取消使用校內各項資訊資源之所有權限，並列入人員離職、留職停薪與休職必要手續。
6. 使用者如因職務異動而成為非授權使用者時，相關單位主管應於一週內主動通知資訊組變更其權限。

（二）人員教育訓練

1. 本校新進人員應施以適當的系統操作訓練，避免使用者不當之操作。
2. 新系統上線時，應對其作業人員、維護人員及網路管理人員施以適當的教育訓練。

3. 每年度應對校內同仁辦理資訊安全管理研習課程或訓練，提升其危機意識與資訊安全觀念。課程中必須給予完整之軟體著作權與版權觀念，嚴禁非法使用軟體，而自由軟體(freeware)與共享軟體(shareware)之安裝使用，亦必須詳細了解其版權宣告並遵守。
4. 每年度應針對校內資訊人員進行資訊安全管理訓練，以及危機處理防護演練。
5. 參與本校資訊系統開發維護之委外廠商人員，應避免開發之軟體帶有易受攻擊之程式碼，**並列入合約規範**。
6. 應隨時注意資訊安全最新訊息，參與資訊安全相關訓練，並利用內部網站及電子郵件公告同仁知悉。

三、電腦系統安全管理

（一）電腦系統作業程序及責任

1. 各電腦系統負責人，應訂定電腦系統作業手冊，並以書面、電子或其他方式載明之，以確保同仁正確及安全地操作及使用電腦，並以其作為系統發展、維護及測試作業的依據。
2. 電腦系統作業手冊應載明執行每一項電腦作業的詳細規定：
   (1)如何正確地處理資料檔案。
   (2)電腦系統作業時程的需求，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。
   (3)系統當機或發生錯誤之處理規定及回復正常作業之程序及作業之限制。
   (4)遭遇非預期的電腦系統作業技術問題時，與支援人員聯繫之方式。
   (5)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，輸出資訊之安全處理規定等。
   (6)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；電腦系統作業手冊應視為正式文件，作業程序的更改須經**單位一級主管**及**內控小組**核定。
3. 電腦稽核軌跡及相關的證據，應以適當的方法保護，作為問題研析及判斷是否違反契約或資訊安全管理規範的證據與協商補償之依據。
4. 為降低因人為疏忽或故意，導致資料或系統遭不法或不當之使用，在人力資源許可條件下，應儘可能將人員依業務及功能之不同區分角色，如：網路管理、系統行政、系統發展維護、變更管理、安全管理、安全稽核及作業人員。

（二）電腦病毒及惡意軟體之防範

1. 病毒防護軟體由資訊組統一進行，定期(每年)規劃評估與建置安裝。

2. 本校同仁應使用具合法版權軟體，避免上網下載來路不明之軟體。
3. 與外部交換資料時，使用資料前應啟動病毒防護軟體偵測。
4. 同仁應隨時更新病毒碼並下載修補系統漏洞。
5. 同仁操作電腦系統如發現病毒時應立即清除，並通報資訊組病毒或惡意程式名稱，無法自行清除病毒時通知資訊組派員協助處理。
6. 資訊暨圖書中心資訊組應定期（每年）依「校園公用電腦安全查核表」檢視校園內公用電腦（包括專案電腦、電腦教室電腦、教學用電腦及行政用電腦）之相關防護措施（包括防火牆、防毒軟體設定與不法軟體之安裝情形等）。

（三）作業權限與帳號管理

1. 核發使用者帳號、密碼前，應查核使用者是否已取得使用資訊系統之正式授權，及其授權之程度是否與業務目的相對稱。在未完成正式授權前，不得對該使用者提供存取服務。
2. 網路系統管理人員及應用系統維護人員應定期（每個月）檢查及撤銷閒置不用的帳號，並不得將其重新配給其他的使用者。
3. 應完善保管應用系統使用人員之註冊資料及授權紀錄，以備日後查考。
4. 使用者帳號名稱不應帶有足以辨識使用者權限的資訊。
5. 應嚴格管控應用系統之特別權限，視個別執行業務之需求，逐項考量賦予使用者系統特別權限之存取。
6. 應用系統設計使用者帳號、密碼時應遵循以下之原則：
   (1) 應要求使用者必須使用密碼（至少 6 碼，包含英數字或特殊符號，中等安全等級以上），以釐清使用責任。
   (2) 應設計於使用者第一次登入時，強制更改臨時性密碼之功能，並要求使用者定期修改密碼。
   (3) 應用系統登入程序中，不應顯示使用者密碼資料。
   (4) 存放機密性及敏感性資料之大型主機或伺服主機(如：人事系統、會計系統主機等)，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。

（四）軟體複製之控制

使用有智慧財產權的軟體，應遵守相關法令及契約規定。

（五）個人隱私之保護

1. 資訊系統處理個人隱私資料時，應依據「個人資料保護法」及本校「個人資料安全維護計畫」與「個人資料保護管理規範」等相關規定，審慎處理個人資料，非公務用途嚴禁調閱使用。
2. 提供公眾服務的資訊系統，如有存放申請或註冊之私人資訊，應將資訊獨立於系統之外，另行存放於防火牆內部之主機以妥善保管，避免有心人士竊取，侵犯隱私。

3. 個人資料依有關法令為特定目的外之利用時，應由該資料檔案承辦單位填具「個人資料調閱申請書」，簽奉核准後行之。

（六）系統登入安全管理

1. 系統登入程序應於使用者完成所有登入資料輸入後，始開始查驗登入資訊的正確性，登入失敗時，系統不應提供訊息告知使用者錯誤之資料項目。
2. 系統登入失敗次數以三次為限，並紀錄此登入失敗事件後中斷連線，強制該終端個人電腦必須間隔一段時間後才能再嘗試登入。

（七）日常作業之安全管理

1. 網路系統管理人員未經權責主管人員許可，不得閱覽、增加、刪除或修改其他網路使用者之私人檔案。如發現有可疑之網路安全情事（如病毒或特洛依木馬等），得經資圖中心主任核可後，使用適當的工具追蹤檢查相關檔案，採取必要處理措施，事後再行知會該檔案擁有者。如確定為感染病毒，為避免病毒擴散，得經主管同意後，逕行掃毒或隔離檔案再行知會該檔案擁有者。
2. 網路系統管理人員登入主機系統時，應保留所有登出入系統紀錄，不得新增、刪除或修改稽核資料檔案，避免於安全事件發生後造成追蹤查詢之困擾。
3. 各主機如有異常狀況應由該應用系統維護人員儘速排除。職務代理時除將系統相關帳號及密碼彌封交由單位主管保存、建立代理帳號或進行權限移轉設定，應將維護手冊移交給職務代理人員，由職務代理人員待命，以確保各主機之正常運作。
4. 各應用系統維護人員應提交各應用系統所需磁碟機容量、各項軟體名稱、系統操作及備份程序等，交予網路系統管理人員彙整管理。
5. 應用系統維護人員應每日注意觀察系統資源使用狀況及應用系統使用情形，有異常狀況應即時反應。
6. 機房管理人員應執行電腦機房環境監測，每日應填寫機房日誌，定期紀錄溫溼度，上下班需注意照明等相關電器設備之開關，並特別注意冷氣及除濕機運轉狀況，於必要時應進行相關耗材清理更換，機房日誌每週由資訊組組長簽核後，每月呈資圖中心主任核定。

（八）資料及媒體交換安全管理

1. 公文電子資料交換依行政院頒訂之「機關公文電子交換作業辦法」及相關規定辦理。
2. 本校及所屬機關公文電子資料交換，收文後需標明電子公文，並依本校收文處理作業程序辦理。
3. 本校與行政院公文電子資料交換，須採用認證與加解密之安全管制措施，始可進行公文收發。

4. 校外機關如因業務需求，必須透過網路與本校交換資料，經簽會資訊組，奉核定後，採以下方式擇一辦理：
   (1)透過網際網路(Internet)與本校連線作業者，依申請之連線項目，由資訊組事先於防火牆設定存取規則，以過濾網路之傳輸作業。
   (2)透過獨立之網路路由與本校特定主機連線作業者，為網路安全考量，此主機應盡量避免與校內網路連線。
   (3)使用磁帶、磁碟或光碟片等媒體進行資料交換時，應有妥善之包裝與安全措施，以防止運作過程中受到損害、破壞或未經授權之取用。
5. 進行媒體資料交換時，應透過安全評估，慎選安全可信賴之廠商或人員，並報請各單位主管同意。
6. 機密性之資料若需使用公眾電話設備傳送時，公眾電話設備必須有保護之措施，避免明文資料外洩。

（九）系統稽核

1. 應用系統維護人員對系統進行查核之自我稽核作業，應經權責單位主管同意始得為之，並避免影響業務正常運作。
2. 應用系統維護人員應定期（每半年）執行自我稽核作業，稽核作業時的所有系統存取應予監督並留下記錄，以備日後查考。
3. 資訊暨圖書中心主任及資訊組組長、圖書組組長應於自我稽核後，執行複稽作業。
4. 系統稽核應考量事項如下：
   (1)稽核需求及查核範圍，應經權責單位主管核定。
   (2)應限定以唯讀方式存取軟體及資料。
   (3)不能以唯讀方式進行系統存取時，應獨立複製另外一份系統檔案供稽核作業之用，且應於稽核作業完成後，立即消除檔案。
   (4)執行查核所需的技術資源，應於事前明確界定，並準備妥當。
   (5)執行特別及例外的查核，應於事前明確界定需求及範圍。
5. 系統稽核紀錄應包括下列事項：
   (1)使用者帳號控管狀況。
   (2)檢查系統登入的模式，確定使用者帳號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)系統所需硬碟空間需求及使用情形。
   (5)系統存取失敗情形。
   (6)追蹤特定的系統交易處理事項。
   (7)敏感性資源的使用情形。
   (8)例外事件及資訊安全事項的稽核記錄。

6. 應保護系統稽核工具（例如軟體及資料檔案）以防止誤用或被破解，並應與發展中或是實作的系統分隔，且應存放在安全的地點。

四、網路安全管理

（一）網路安全規劃與管理

1. 為維持本校網路能正常持續地運作，主要網路設備應考慮 Full Redundant 或準備備援設備即時替換。
2. 本校個人電腦及伺服器 IP 位址均由資訊組統一規劃發派，並由資訊組網管人員製作重要網路節點之流量統計表，及每日使用量最高之 30 台主機，公布於資訊組網頁。
3. 資訊組網管人員應針對本校所有電腦及伺服器進行流量之區隔與管控，為保持網路暢通，對傳輸量使用過大主機，依本校「校園網路侵權行為之停權建議」進行停權處置。
4. 資訊組得視業務需求，指派合格且適任之人員擔任各單位（含宿舍）網路安全管理人員，並與以適當之教育訓練。
5. 本校內部網路、DMZ 網段與外部網路之連線存取，均需透過防火牆之安全管控，防火牆之運作維護由資訊組指派專人負責。
6. 聯外網路應安裝入侵偵測防禦系統，網路安全管理人員須隨時監控非法入侵之犯罪行為，並收集入侵證據以作為法律控訴之證物。
7. 如需新增或遷移資訊系統主機時，應用系統維護人員應審度該系統之使用者性質、作業特性、作業公開程度及資料更新機制等因素，並會簽資訊組後，會同資訊組人員安裝至適當網段。資訊系統廢止時，亦應知會資訊組註銷紀錄。
8. 本校及附屬單位同仁如因業務特殊需求，需於防火牆對外開放特殊服務（如遠端登入 Telnet 或檔案傳輸 FTP 等），在不影響本校網路安全條件下（如採用 VPN tunnel 技術），經會簽資訊組並經資圖中心主任核可後，由資訊組設定開放權限。
9. 本校同仁利用微軟視窗作業系統之檔案分享功能提供他人存取檔案時，應僅針對必要對象開放使用權限，避免將權限完全開放。

（二）電子郵件安全管理

1. 本校之網路使用者禁止以電子郵件騷擾他人、發送匿名郵件、偽造他人名義發送郵件或惡意發送大量不當郵件，如有違反之情事，由本校人事室或學務處查處，必要時由資訊組提供技術支援。
2. 機密之公文及資料，不得以電子郵件傳遞；敏感性資料如有透過網路傳送之必要，應經加密處理後傳送。
3. 為防範假冒機關員工名義發送電子郵件，以電子郵件發送重要訊息時，應以電子簽章簽發，以達到身分辨識及不可否認的目的。

（三）聯外網路安全管理

1. 透過公眾網路傳傳送涉及全校師生權益、機密等敏感性或機密性資訊，必須規劃採用 PKI 或 SSL 之認證與加密機制，以保護資料的完整性及機密性，並保障連線之安全性。
2. 除開放公眾瀏覽與下載之系統外，本校提供外部連結之系統均需建立個別之安全機制（至少需具備基本的使用者登入認證機制），以保障網路的安全性。
3. 本校外部網路（含 DMZ 區）的電腦系統與網路設備，需與內部網路連線作業時，應檢附該外部設備之相關文件（如網路協定、提供服務項目及特殊需求等），會簽資訊組並經資圖中心主任核可後，始得進行連線作業，連線作業時應遵守本校之網路安全規定及連線作業程序。
4. 校外網路欲與本校 DMZ 區或內部網路連線時，需由業務承辦單位申請，經單位主管核可後，會簽資訊組承辦，於申請時段內開放防火牆連結設定。

（四）網路安全稽核

1. 資訊組網路系統管理人員需每日不定時檢視系統登錄紀錄。如發現異常狀況應立即通報單位主管，情節重大時應專案簽報並知會人事室或相關單位。
2. 網路系統管理人員應定期（每半年）執行自我稽核作業，稽核作業時的所有系統存取應予監督並留下記錄，以備日後查考。進行自我稽核作業時，應經權責單位主管同意，並避免影響資訊服務之正常運作。
3. 資訊暨圖書中心主任及資訊組組長、圖書組組長應於自我稽核後，執行複稽作業。
4. 資訊組應對校內網路建立警示系統，於特定網路安全事件發生時，能立即產生警示訊號通知網路系統管理人員，俾採取有效的防護措施，降低安全事件所產生的危害。

五、系統存取控制

（一）機密性／敏感性系統之作業管控

1. 對機密或敏感性的系統，宜建置獨立的或專屬的電腦作業環境。
2. 應用系統是否屬於機密或敏感性應由系統負責單位決定。
3. 機密或敏感性的應用系統須分享相關資源時，應經系統負責單位主管核可。

（二）使用者存取管理

1. 本校新進人員及委外服務人員由資訊組核發帳號後，啟用電腦系統。帳號及密碼嚴格禁止交付他人，職務代理時應將系統相關帳號及密碼彌封交由單位主管保存、建立代理帳號或進行權限移轉設定，並避免於電話或電子郵件中告知系統維護人員。

2. 所有網路使用者僅核發一個使用者帳號，如有特殊情形（如系統測試、免費軟體下載等用途），經會簽資訊組並奉核定後，始得核發匿名或多人共享的帳號。
3. 應用系統維護人員應定期（每半年）檢討及評估相關使用者之存取權限。
4. 為防止有人未經正式的授權程序取得特別權限，應定期（每半年）檢討系統存取特別權限之核發情形。
5. 資訊組應就應用系統維護人員所提之存取權限檢討與評估，提出具體改善建議。

（三）系統存取之責任

1. 人員因故離開座位中斷作業時，必須簽退系統或使用畫面鎖定保護，防止帳號被盜用或資料被竊取。下班或公出離開辦公室前，必須關閉電腦設備並將桌面收拾乾淨，避免有心人士竊取機密資料或侵入系統。
2. 同仁應保持高度之警戒心，防範不法人士以社交工程方法(Social Engineering)獲取帳號及通行碼入侵。並應具備高度之危機意識，如有發現疑似系統安全危機時，應迅速通知本校資訊組資訊安全處理人員。
3. 應用系統維護人員之責任：
   (1)使用者應善盡保護個人密碼之責任；如屬於群組軟體之使用者，應確保工作群組的密碼，僅限群組成員使用。
   (2)為維持密碼的機密性，應強迫使用者於首次使用時立即更改密碼。
   (3)密碼之交付應由系統維護人員親自或以安全之文書方式交付給使用者，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，並應確認使用者是否收到密碼。
   (4)自動化登入系統之密碼，不宜存放在巨集或是功能鍵中。
4. 應用系統使用人員之責任：
   (1)個人應負責維持密碼的機密性。
   (2)應避免將密碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。
   (3)當有跡象足以顯示系統及使用者密碼可能遭破解時，應立即更改密碼。
   (4)儘量避免以時間、個人資訊、單位識別代碼、電話號碼或使用者帳號等做為密碼。
   (5)應定期（每 6 個月）更換密碼，避免重複或循環使用舊的密碼。

（四）網路系統之存取控制

網路使用者應遵守本校校園網路使用規範，於授權範圍內存取網路資源，不得以任何方式竊取他人之登入帳號、密碼，不得使用任何軟體、設備竊聽網路上之通訊，不得使用任何手段干擾或妨害網路之正常運作，不得嘗試入侵防火牆主機，亦不得於本校網路上儲存、建置或傳播色情文字、圖片、影像、聲音等資訊。如有違反以上情事，依相關法規查處。

（五）電腦系統之存取控制

系統公用程式需進行安全管控，其機制如下：

1. 應嚴格限制及控制電腦公用程式之使用。
2. 設定使用者密碼以保護系統公用程式。
3. 將系統公用程式與應用系統分離。
4. 將有權使用系統公用程式的人數限制到最小的數目。
5. 應移除非必要的公用程式及系統軟體。

（六）應用系統之存取控制

1. 應依資訊存取規定，配賦應用系統使用人員與業務需求相稱的資料存取及應用系統使用權限。
2. 資訊存取的控制機制如下：
   (1)控制使用者僅能使用系統的部分功能。
   (2)限制使用者僅能獲知或取得授權範圍內的資料。
   (3)控制使用者存取系統的能力（例如限定使用者僅能執行唯讀、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。

（七）系統存取之應用與監督

1. 應用系統維護人員應建立及製作例外事件與資訊安全事項的稽核記錄，以作為日後調查及監督之用。
2. 應定期校正電腦系統作業時間，以維持系統稽核紀錄的正確性及可信度，俾作為事後法律上或是紀律處理上的重要依據。
3. 應建立系統使用情形之監督程序，確保使用者只能執行該授權範圍內的事項。
4. 應用系統於正式上線後，應由該應用系統發展單位（委外者則為原委託單位）進行系統存取安全的風險評估，並由資訊組協助提供相關意見。
5. 系統使用之監督作業，由應用系統維護人員依風險評估結果，建立監督紀錄作為日後稽核之用。

（八）校外人員存取資訊之安全管理

1. 對校外提供資料查詢或檔案傳輸服務，須辦理風險評估，並簽訂正式的契約或協定以規範連線單位應遵守之規定及限定作業範圍與服務內容後，始得提供服務。

2. 對於校外存取之第三者風險評估，應充分考量下列事項：

(1)第三者需要存取的資訊類型及資訊的價值等。

(2)第三者採行的資訊安全措施及安全保護水準。

(3)第三者之存取對本校資訊架構可能產生的安全風險及影響。

六、密碼學(加密控制)

（一）密碼學的目的

為保護資料在處理、使用及傳輸時的機密性與完整性及不可否認性並可對傳輸者進行身份驗證，應藉由加密控制措施，確保適當及有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。

(1)確保資訊的私密性（Confidentiality）

(2)提供驗證識別（Authentication）

(3)偵測資料是否被不當的竄改（Integrity）

(4)提供資訊傳送來源、接收目的或交易的證明(Non-repudiation）

（二）密碼式控制措施

1. 對高機密性或敏感性的資訊，在傳輸或儲存過程中以加密方法保護。
2. 使用加密方法，需進行風險評估，以決定採取何種等級的安全保護措施。

七、供應者關係

為確保對供應者可存取本校資產的保護，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，設立本校與供應者之管理措施。

（一）供應者關係之資訊安全

與供應者議定合約並文件化，降低與供應者存取本校資產關聯之風險的資訊安全要求事項。各單位在合約中載明及規定特別處理供應者存取本校資訊之資訊安全控制措施。控制措施宜列出本校將實作之過程及程序，以及本校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。

（二）於供應者合約中闡明安全性

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。面對外部人員存取本校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控制措施，宜包含:

(1)評估存取風險，了解存取的資訊類型、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。

（三）資訊及通訊技術供應鏈

與供應者之合約，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、設備零件廠商等整個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要求以外，界定適用於資訊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。

（四）供應者服務之監視及審查

本校應定期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定期(每半年)安排行程會議。

(3)各單位提供資訊安全事件的資訊，由廠商和資訊組審查這些資訊。

(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。

（五）管理供應者服務之變更

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.現有的服務的加強。

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。

八、系統發展及維護之安全管理

（一）委外廠商安全管理

1. 資訊服務委外時必須慎選口碑良好與高品質之廠商，訂定符合效能需求及系統安全規範之合約書，並制定違約罰責。
2. 應用系統委外維護運作合約，必須訂定合約期間所有工作內容與產出之著作權歸屬。
3. 廠商承包各單位委外設計操作之資訊系統時，凡涉及系統規劃、設計、執行、操作等相關作業之委外服務人員，應要求廠商之相關人員簽署保密協定，並將遵守本校資訊安全政策與相關規範納入合約中。
4. 各單位委外計畫若涉及資訊系統設計操作及資訊硬體設備者，於簽核時應知會資訊組；資訊組得就作業需求，提出可行性與適用性之資訊專業技術建議。
5. 各單位委外設計操作之資訊系統計畫中，凡屬與公文機密、個人及事業單位權益相關之資料，應留在機關內部處理，其它資料若需由承商攜回公司內部處理者，應簽奉資訊安全長核可。
6. 各單位委外設計操作資訊系統時，應會同資訊組檢討評估委外計畫中各項軟、硬設備及各項作業執行之安全性，以確保其符合本校的安全標準。
7. 承商如發現有違反資訊安全事件，應立即處理並同時通報本校。承商應將違反資訊系統安全事件之處理結果完整紀錄，於限期內提交資訊組。資訊組據此依本校「資訊安全事件標準處理程序（附件一）」進行查核評估，必要時可實地了解或實施專案稽核，並做成查核報告，簽會總務處及資訊組後陳核。

（二）系統發展及維護安全管理

1. 系統開發、維護及測試環境必須使用另行建置之專用伺服器，不可與實際運作中之伺服器共用。開發維護伺服器只允許系統開發維護人員登入使用，並須謹慎維護內存程式碼與資料之安全性。
2. 系統開發、維護及測試環境之系統登入方式應與實際運作之作業系統登入方式有所區別。
3. 資訊系統測試時，應使用虛擬資料建置測試用資料庫，嚴禁使用真實資料進行測試。若因業務需求必須使用真實資料，則須做好資料機密性之保護。

4. 新系統上線作業前，應進行功能測試，並經使用單位確認作業效能、系統容量及功能後，始得正式上線運作。
5. 新系統開發或增修維護既有系統時，應避免採用特殊技術，避免衍生危及整體資訊安全之顧慮。
6. 開發以 Web 網頁型態使用瀏覽器提供服務之作業時，應儘可能使用 PKI 或 SSL 之認證與加密機制傳輸資料。
7. 全球資訊網(WWW)網頁資料之更新，應由權責單位指定專人負責，上傳資料時應先執行掃毒，避免造成病毒之擴散。
8. 應用系統之原始程式碼，由應用系統維護人員負責版本的更新、維護及複製管理，並負責核發提供程式設計人員修訂。
9. 應用系統之各項系統文件，應用系統維護人員應確實建置完備並妥善保管，同時存放乙份於資訊組備查。
10. 應用系統軟體之版本必須嚴格管控，如需更新版本時，應用系統維護人員應妥善保管各版本之系統文件，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，資訊組得視需要，就各應用系統之更新狀況，提出具體評估建議。

（三）需求變更管理

資訊組每年視人力及業務狀況辦理資訊系統之更新作業，如屬業務緊急重大需求，應經資圖中心主任評估核可後，由資訊組專案辦理。

因應臨時業務需求，需求單位應填具「校務行政 E 化系統資訊服務需求申請單」，由該單位主管核可後向資訊組申請，資訊組得視人力、技術及成本考量，提出可行性方案及意見（或辦理情形）回覆原需求單位。

九、資訊資產之安全管理

（一）資訊設備安全管理

1. 本校各項資訊資產應依其機密性、完整性及可用性，區分不同等級，。
2. 本校各項資訊設備除依照相關審計法規財產管理外，各單位應自行負責設備之安全，移出本校時應經權責單位主管核定始得放行。
3. 本校各項資訊設備報廢時，除依相關財產減損規定辦理外，應經本校保管組會同相關單位，檢定其堪用狀況後，始得辦理報廢。
4. 本校同仁如發現有不明人士，未經許可擅接網路之情事，應立即通知資訊組處理，以掌握本校整體資訊設備之安全。
5. 重要之資訊資產必須上鎖，且保存於合於「八、實體及環境安全管理」中規範之電腦機房安全空間。

（二）機密或敏感資訊之安全管理

機密性或敏感性的資料，不得存放於對外開放的資訊系統中。

十、實體及環境安全管理

（一）電腦機房安全管理

1. 校級電腦機房由資訊組負責管理，各科電腦機房由各科自行負責管理，每月排定機房管理人員輪值表，呈單位主任核定後實施。
2. 校級電腦機房應以門禁系統進行控管，門禁卡片之發放由資訊組管制，並指定專人造冊列管。卡片不得轉借他人使用；其他人員臨時進出得申請臨時卡，於登記時間內使用，使用後繳回。
3. 本校委外服務廠商人員需經常進出機房工作者，得專案報備並由當事人簽署保密切結書，領取機房門禁卡片，專案執行完成時應歸還門禁卡始得辦理結案。
4. 機房管理人員應執行機房環境監測，每日填寫機房日誌，並注意機房溫溼度、空調及照明設備等之運轉狀況。
5. 電腦機房嚴禁煙火，並不得攜帶飲料、食物進入，如需進行清潔保養等工作應考量不得危害機房正常運作或需關閉部分系統主機始得為之，以避免人為疏失導致災害發生。
6. 電腦機房應裝設適用於電子設備之消防設施（如 FM200），並每年度定期檢驗。

（二）實體設備之採購、租借與維護安全管理

1. 本校正式之網域名稱為 ctcn.edu.tw，新購置、升級或新安裝建置之平台系統均應加入此網域，以便監控整體網路安全。
2. 新建置或安裝之軟體，安裝完成後應立即更新廠商預設之密碼。

（三）實體設備及環境之安全管理

1. 電腦主機系統及其相關儲存與網路連結設備必須以電源自動切換開關(ATS)連接發電機備用電源，並使用穩壓與不斷電(Uninterruptible Power Supply, UPS)系統供應電力，以避免電壓不穩定或瞬間斷電造成損害。
2. 所有網路連結設備必須嚴格之管控，交換器等網路設備之各插孔須清楚標示編號，網路接線兩端亦清楚須標示「來源-目的」位置，並繪製網路佈線圖。
3. 設備之搬遷必須嚴格管控與授權，並紀錄存檔。被授權之搬遷人員必須負責遷移設備之使用安全與內存系統資料安全。

（四）媒體、文件安全管理

1. 涉及機密性或敏感性之相關媒體、文件由業務單位指定專人設置保管箱列冊保管，媒體須以牛皮紙袋密封加蓋騎縫章，其傳遞與與使用均須獲得單位主管授權始得使用。
2. 系統文件應妥善保管，使用時於管理紀錄本登錄。如係委外操作之系統，應於合約規範於契約解除時歸還本校。
3. 每年應定期檢討機密性／敏感性資料，並專案簽報銷毀，並指定專人監督辦理。報廢之設備執行儲存媒體重新格式化(format)，移除相關

作業軟體、資料及具有版權之系統軟體；報廢之磁帶、磁碟或光碟片等媒體進行實體銷毀；含有機密性資料之書面文件，使用碎紙機予以銷毀。

十一、業務永續運作計畫之規劃及管理

（一）備援／備份作業之規劃與演練

1. 各單位自行或委外開發之資訊系統於上線運作後，應對該系統之原始程式碼進行備份 2 份，1 份自行保管，另 1 份繳交資訊組統一進行異地儲存保管。
2. 資訊系統設備故障或損壞時，應即時確實執行系統備援回復作業，維持業務之持續運作，並紀錄存檔。
3. 每日下班時段後，備份系統自動執行本校各重要共用電腦系統之資料差異備份(Differential Backup)，每半年自動執行各共用電腦系統之資料全量備份(Full Backup)。
4. 資訊系統作業紀錄每半年由各應用系統維護人員備份、清理。
5. 個人電腦中之重要資料備份應由同仁自行進行備份。
6. 每半年應進行備援設備、回復作業程式及機制之測試演練。

（二）業務永續運作規劃

1. 每年進行資訊安全風險評估，並據以修正本校「資訊安全暨緊急應變管理規範」。
2. 應使用弱點掃瞄、滲透測試及源碼(Source Code)檢測之系統安全檢測軟體，於資訊資產購入驗收及自我稽核時，進行系統安全檢核工作，以減少非法人士入侵之機會，並製作系統安全檢查報告(SMSR Reports)。
3. 應制定資訊系統「緊急應變與處理程序」及「災難復原程序」，以應付危機處理之需求，並演練以保障其有效可行性。

（三）突發事件應變辦法

任何突發之安全事件或造成運作中斷之事件，本校同仁不得隨意接受新聞媒體採訪發言，須經校內分析整理後，由校方代表統一發言。

肆、緊急應變與處理程序

本校資訊及網路系統管理人員發現系統服務及功能異常，或經通知疑遭破壞或不當使用，或其他災害影響系統正常運作時，即啟用事件通報應變處理程序。

一、事件通報應變處理

（一） 事件鑑定與確認：

1. 系統管理人員或使用者發現資訊或網路系統服務及功能異常反

應，應立即通知資安聯絡人進行鑑定。

2. 資安聯絡人協同系統管理人員分析資安徵兆或校外通知，確認為資安事件後，依據事件類別及對業務影響程度，區分資安全事件等級，並依本校「資訊安全事件處理程序（附件一）」處理，填具「資訊安全事件處理單（附件二）」。
3. 必要時系統管理人員得採取緊急應變措施，防止事件影響擴大。
4. 系統管理人員應記錄事件狀況、應變措施等相關資訊，交由資安聯絡人進行通報。
5. 資安事件等級如下：
   - A 級：影響公共安全、社會秩序、人民生命財產。
   - B 級：系統停頓，業務無法運作。
   - C 級：系統短暫停頓，業務中斷，短時間可修復。
   - D 級：系統效能降低，業務遲滯，可立即修復。
   - E 級：違反校園網路使用規範或其他公約。

（二） 事件通報：

1. 資安聯絡人立即依循內部行政程序，將事件狀況、應變措施等相關資訊向資訊安全長報告。
2. 屬『A』、『B』、『C』、『D』級之資安事件，資安聯絡人應於確認資安事件 1 小時內至「國家資通安全通報應變網站」登錄事件通報。如因網路中斷無法上網登錄，則應填具「資訊安全事件通報單」，傳真至國家資通安全會報通報應變組，俟網路恢復後上網登錄補報。
3. 屬『A』或『B』級之資安事件，資安聯絡人應於確認資安事件 2 小時內向教育部資安聯絡人通報，並提供事件細節內容。

（三） 事件處理：

1. 系統管理人員進行損害評估，並分析系統復原所需資源。
   1. 資安聯絡人協調資通安全處理小組成員進行應變處理作業。
   2. 資通安全處理小組依組織、人力、應變措施與所需資源，判定是否自行處理或需請求上級支援。
   3. 若判定需請求上級支援，經資訊安全長核定後，應於確認資安事件 12 小時內向教育部提出申請支援。
   4. 系統管理人員進行資安事件處理前，應先儲存或備份系統記錄與稽核軌跡等相關資訊，保全事件證據。
   5. 系統管理人員應記錄事件處理過程，以供後續稽核改善之參考。

（四） 事件回覆與結案：

1. 資通安全事件處理完成經資訊安全長核定後，資安聯絡人依下

列規定時間內回報。

(1) 屬『A』或『B』級之資安事件，須於確認資安事件 **36 小時**內至「國家資通安全通報應變網站」完成通報結案，並向教育部回報處理結果。若系統無法完成恢復應完成損害管制，並尋求業務運作替代方案。

(2) 屬『C』或『D』級之資安事件，須於確認資安事件 **72 小時**內至「國家資通安全通報應變網站」登錄通報事件結案。

(3) 屬『E』級之資安事件，如為教育部通知疑是侵犯智慧財產權事件，須依教育部規定 **7 天之內**回報處理結果。

二、入侵處理

（一）發現網路或系統入侵之處理步驟

網路使用者發現網路或系統入侵之情事時，應立即通知資訊組，資訊組接獲通知後，應依本校「資訊安全事件處理程序（附件一）」處理，填具「資訊安全事件處理單（附件二）」，並採取下述任一適當措施以防止災害繼續擴大：

1. 當確定本校網路安全被突破時，被入侵之應用系統應切斷入侵者的網路連接，並即設定為「拒絕任何存取」，如無法切斷網路連接則必須關閉網路防火牆。
2. 如入侵者已被資訊組嚴密監控，在不危害內部網路安全的前題下，得適度有條件地允許入侵者存取動作，以利追查入侵者。一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的連接。

（二）網路或系統入侵之追蹤調查

1. 檢視記錄檔中是否有不尋常的來源位置或不尋常的操作動作。檢查登入時間、程序的執行記錄以及系統日誌所做的記錄等，以防止入侵者修改記錄檔來隱藏行蹤。
2. 對入侵者的追查，除利用稽核檔案提供的資料外，得使用系統指令執行反向查詢，並聯合相關單位(如 Hinet、區網中心等)追蹤入侵者。
3. 當檢查機器是否被入侵時，必須檢查所有區域網路上的機器。如一台機器被入侵，同一網段的其它機器也有可能已被入侵；或是入侵者利用其它機器為窗口來入侵本校網路。

（三）網路或系統入侵的事後處理

1. 入侵者之行為若觸犯法律規定，構成犯罪事實，由人事室或學務處查處，並立即告知檢調單位，請其處理入侵者之犯罪事實調查。
2. 資訊組應全面檢討網路安全措施及修正防火牆的設定，尋求適當之解決辦法，以防禦類似的入侵與攻擊。
3. 保留所有記錄供資訊安全稽核。

三、安全稽核流程與獎懲措施

（一）稽核計畫

1. 本校應配合教育部所辦理之外部稽核，以及校內內部稽核作業，以落實執行資訊安全稽核工作，以反映教育部資訊安全管理政策、法令、技術及相關業務之最新狀況，並確保本校資訊安全實務作業的可行性及有效性。
2. 稽核計畫之重點內至少應包括本校公用電腦（專案電腦、電腦教室電腦、教學用電腦及行政用電腦）之相關防護措施（包括防火牆、防毒軟體設定與不法軟體之安裝情形等）、機房安全管理維護、網路安全管理維護、本校三個單位以上共同使用之應用系統安全管理維護、利用網際網路開放外界連線作業之資訊系統安全管理維護、本校委外服務之各項資訊系統安全管理維護、同一年度內休離職人員管理之各項資訊系統或資料庫、同一年度內新開發之資訊系統安全管理維護及上年度專案稽核計畫結果列入待改進之項目。稽核內容則視本規範各相關項目內容及精神，查核是否均按規定辦理並完整記錄及保留應填寫之各項紀錄表。
3. 資訊安全稽核結果，除特殊原因得簽奉核可不公開外，應彙整相關單位之優缺點及綜合改進建議，簽奉核可後提供相關單位改進，本校各單位及人員不得將相關資訊安全稽核結果資料洩漏給不相關之第三者。
4. 為求資訊安全稽核工作之客觀性及有效性，必要時得運用可行之工具程式等輔助進行稽核，或委請校外專家學者，協助本校進行資訊安全稽核工作。

（二）獎懲措施

1. 稽核之結果，由資圖中心會同人事室或學務處進行檢討，對於執行資訊安全作業工作績優者或有缺失部分，由本校「資訊安全推動小組」擬議，予以獎勵或懲處。
2. 本校教職員生違反本計畫之作業規定，情節重大者，依相關法規及相關獎懲標準辦理懲處。
3. 委外管理人員及委外服務人員違反本規範之作業規定，應通知受委託承商更換相關人員，並視情節依合約規定要求承商賠償本校之損失。

伍、災難復原程序

（一） 人員的生命安全為第一，緊急危機之應變處置，係以維護、救助員的生命安全為最優先考慮。

（二） 備份資料及設備為最珍貴財物，當情況必須保護、搶救財物時，應以各電腦系統及備份資料為優先搶救之標的物。

（三） 損失大小先於機率高低，遭遇危急事件，於行動上必須有所抉擇時，應優先處理可能造成重大損失的事項，至於其發生機率之高低，則列為次要考慮。例如停電時，不應急於關機（此時電腦當機的機率可能頗高），而應先找出停電的原因（因火災引發停電的可能性或許不是最高，但是損失卻會相當大）。

（四） 危急事件處理程序

1. 危急事件：指危及人員生命安全、資訊網路設施、財物、甚至名譽等突發事件。如：火警、停電、停水、地震、颱風、水災、竊盜、暴力脅迫、空調系統故障、電力設施故障、資訊設備故障受損、網路中斷、系統安全（含資料安全）等事件；但不僅限於此。
2. 危急事件通報：依據發生事件之不同，通報給主責單位，並視情況發展進行適當的應變處置。
3. 處理人員會合：接獲電話通知後，相關資訊作業人員應立即會合，迅速評估及研討處理模式，並擬定緊急處置之行動計畫。
4. 搶救備份資料：發生火警時，置放於機房內、外儲存備份資料之媒體、記錄文件及重要系統設備，應屬最優先搶救之財物。必要時，得先行搶救，再執行危急事件通報。
5. 通知有關部門：依事件狀況性質，陳報其他相關主管部門。
6. 進行緊急處置：根據擬定之行動計畫，立即展開必要的緊急處置，以期避免或減少災害損失。另應儘可能維持現場證據（如執行電腦系統備份）以利後續調查事件發生原因。
7. 詳細記錄處理情形，並適時彙報處理進度，紀錄應保存一年以上。
8. 展開復原工作：在確定無安全之虞的情形下，展開復原工作，並陸續開放服務。
9. 調查與檢討：調查事件發生之原因、責任，並檢討改善相關作業程序。
10. 呈報事件經過：向單位主管呈報整個事件之發生原因、處理經過及改善措施。

（五） 現場復原

1. 緊急應變分組應協調相關人員清理災害現場。
2. 資訊機房災害復原作業應依最近一次風險評鑑結果，將資訊系統及作業依據其重要性循序復原。
3. 進行復原作業時，資訊機房復原順序處理原則如下：
   (1) 資訊機房之實體設備相關回復順序：
      A. 電力與空調相關之設備為優先。
      B. 網路連接相關設備次之。
      C. 備援設備回復、資料回復、文件傳送/接收中繼設備等。

(2) 資訊機房之各相關網路實體設備、資料庫、資料之災難回復順序：

A. 相關網路實體設備為優先。

B. 應用系統程式次之。

C. 資料庫。

D. 資料回復。

4. 資訊系統復原完成後，應由使用單位確認資料之正確性，始得宣告可正常作業。

（六） 系統回復

進行系統回復處理時，須於主要備援設備及相關資訊系統設備可運作後，依下列相關處理方式：

1. 單純應用程式（或檔案）損害：由災害緊急應變任務分工名單之應用系統回復負責人會同各應用系統管理權責單位，備妥回復所需媒體，協調應用系統維護廠商進行應用系統之應用程式（或檔案）回復作業事宜。
2. 資料庫損害：由災害緊急應變任務分工名單之資料庫系統回復負責人會同各應用系統管理權責單位，備妥回復所需媒體，邀集資料庫之管理單位或系統維護廠商進行資料庫回復作業事宜。
3. 主機或機關網路嚴重損害：由災害緊急應變任務分工名單之主機系統回復及網路系統復原負責人，協調主機或網路設備相關廠商進行故障修護（或由廠商提供相當的替代設備），將作業系統平台回復至可正常運作狀態，再備妥回復應用系統所需的媒體後，由各系統回復負責人處理後續應用程式、檔案及資料庫回復作業事宜（如前述）。
4. 資訊機房嚴重損害：當機房毀損時，須於事前選定之臨時機房替代地點，重新架設設備及網路環境後，按前述處理方式辦理。

（七）資訊機房火警處置須知

1. 火警發生時，若自動滅火系統、偵煙或偵溫感測器皆已感應，並發出火警警報音響及啟動自動噴灑設定，應立即離開機房並緊閉門窗，以免遭受到濃煙或其它化學物質之傷害。若自動滅火系統感應火警，但並未自動啟動，或火勢已經不容等待時，應立刻採取人工作業，以迫使滅火系統啟動噴灑裝置。
2. 若火警警報未響起，且自動滅火系統亦未感應啟動，應立即持滅火器，進入機房尋找火源。找到火源後，距火源適當處，將滅火器噴嘴對準火燄底部，來回噴灑。
3. 離開機房，並立即撥消防電話。若自動滅火系統仍未啟動，應盡可能以人力強制啟動滅火系統，並設法關閉 UPS 總電源。
4. 在消防隊到達之前，若火勢確定已被滅火系統撲滅，仍應立即關閉 UPS 總電源開關，以策安全。
5. 通知相關單位人員及主管。

6. 於消防隊未到達之前。在人員安全為第一的原則下，繼續依狀況進行可能的應變處置，如：搶救備份資料儲存媒體、文件及協助人員緊急逃生等。

（八） 停電處置須知

1. 造成電力中斷的因素有許多，如電力公司預期或不預期的斷電、室內電力超載之跳電、電線短路、UPS 故障、電源插座鬆脫，或其它天災、人禍等因素。若遇電力中斷，應先判斷造成停電的原因。若屬一般性斷電，應至機房實地檢查 UPS、電力設施及機房中各項設備之安全；若各項設備經檢查後均安全無恙時，仍應密切注意機房內溫度及 UPS 警示燈號。
2. 若 UPS 或空調系統有異常狀況，或有網路設備、電腦系統異常故障時，應即時通知有關的維護管理同仁，請求協助。

（九） 強烈地震處理須知

1. 發生強烈地震時，應盡量遠離機房、電力設施、玻璃門窗，並尋找較安全的掩護物躲避，待地震歇止時，再行處置。
2. 當建築物結構受損時，宜速離開建築物，再因應處理各種可能發生之情況。
3. 倘自身不幸受傷，或有其他人員受傷，而必須送醫急救時，宜先以電話通知 119，之後再通知相關單位主管，以請求協助。
4. 地震過後，應先檢查機房內是否有火警發生，若機房發生火警，應配合所屬人員，協助處理。
5. 若因地震導致停電時，在人員安全無虞下，即依停電處置須知程序進行處置。
6. 地震後，通常陸續會有餘震發生。因此，在視情況許可下，應即檢查機房及辦公室各項設施，如：高架地板是否變形、牆壁地板是否有龜裂、輕鋼架天花板是否變形鬆落、配電箱是否受損、以及機房內各項設備是否正常等。
7. 若發現機房或辦公室其他設施有受損之情形，應即告知相關單位人員及主管，以便因應處置。
8. 檢查後，若未發現有任何損失，仍應將各項置於高處易墜落之物品，挪至地面，或暫時加以固定。

（十） 強烈颱風及豪雨處置須知

1. 預先完成防颱準備
   (1) 部署建立指揮聯絡體系，調整資訊機房值班人員表。
   (2) 手電筒預備電池。
   (3) 檢查並緊閉資訊機房及辦公室等門窗。
   (4) 檢查電源設施及消防滅火系統。
   (5) 關閉不必要的電源。

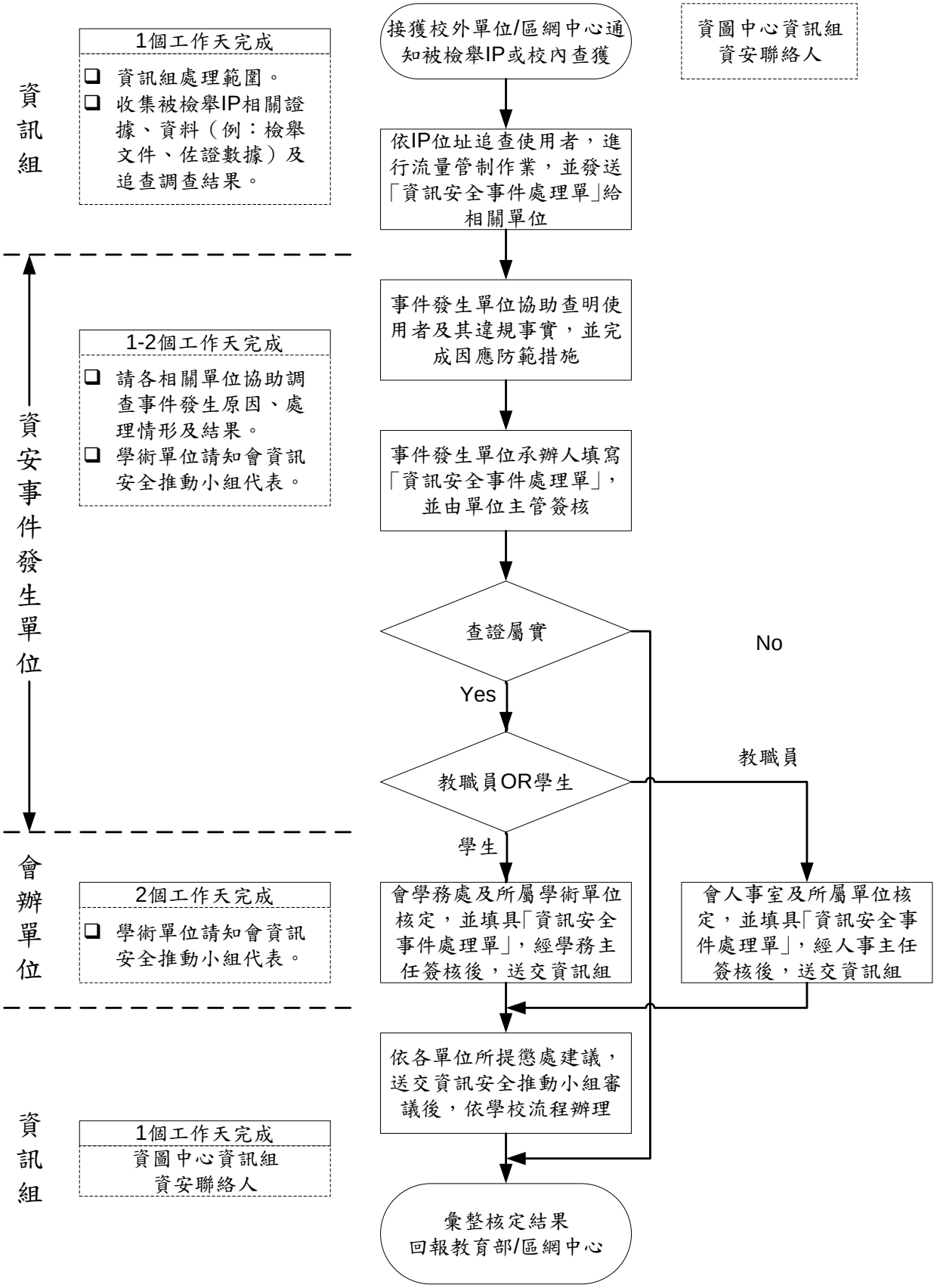
2. 強烈颱風登陸後，機房輪值視情況暫停，輪值同仁應格外注意自身安全，並隨時注意颱風的動態。
   (1) 對外通信設施失效：颱風期間應經常檢查電話線路，發現對外電話不通時，立即使用行動電話通知資通安全處理任務編組召集人，並通知相關負責同仁或廠商協助檢修。
   (2) 機房建築設施受損：應即通知資通安全處理任務編組召集人，並視情況需要，配合相關單位人員進行處置。
   (3) 人員病痛、受傷：值班人員因故發生病痛，難以有效執行任務時，可通知單位主管，並請求支援。倘因故受傷時，可先行通知辦公室內其他同仁，以請求協助。

陸、附則

一、本校附屬機構未定訂資訊安全管理規範者得適用本規範。

二、本計畫經資訊安全推動小組討論，提請行政會議通過，簽請 校長核定後實施，修正時亦同。

資訊安全事件標準處理程序



委外管理人員及委外服務人員違反本規範之作業規定，應通知受委託承商更換相關人員，並視情節依合約規定要求承商賠償本校之損失。

耕莘健康管理專科學校 資訊安全事件處理單

1.資安事件簡述(資圖中心資訊組填寫) 檢附：□ 通知書 □ 網路流量記錄 □ 其他_____

發生日期：____年____月____日 時間：(GMT+0800)_____

IP：_____（所屬單位：_____） 網路卡號：_____

發現方式：□ 校內偵測 □ 校外單位通知 □ 區網中心通知

事件類別：□ 針對特定傳輸埠大量掃描，埠號(port number)為_____

□ DoS 攻擊，攻擊目標 IP 為_____

□ 垃圾郵件攻擊(SPAM) □ 外部攻擊(Attack) □ 設備故障：_____

□ 侵犯智慧財產權，名稱為_____

□ 其他_____

事件說明：_____

影響等級：□ A(影響公共安全、社會秩序、人民生命財產) □ B(系統停頓，業務無法運作)

□ C(系統短暫停頓，業務中斷，短時間可修復) □ D(系統效能降低，業務遲滯，可立即修復)

□ E(違反校園網路使用規範或其他公約)

應變措施：□ 送學務處依校規處理 □ 停用網路 □ 停用帳號 □ 其他_____

※欲申請復權者，請 mail 至 cc@ctcn.edu.tw，資訊組將於收單三日後回覆

承辦人：_____ 資訊組組長：_____資圖中心主任：_____

2.事件調查(所屬單位處理) 所屬單位：_____

請說明該事件發生之原因和處理情形，以及防範補強措施。

該 IP 使用者：_____ 學號/員工編號：_____聯絡電話：_____

※ 請查明上述 IP 之使用者，並確認是否為本人所為，若涉及侵犯智慧財產權或情節重大者請會會辦單位依相關規定處理。

承辦人或導師：_____ □ 處理完畢，不需會辦 單位主管：_____

※ 為配合教育部訂定回報資訊安全處理結果之___天期限，**處理單位請於___月___日前完成**，以利作業

3.核定(會辦單位處理) 會辦單位：□ 學務處 □ 人事室 □ 總務處 □ 其他_____

處理意見：

承辦人：_____ 單位主管：_____

※為配合教育部訂定回報資訊安全處理結果之___天期限，**會辦單位請於___月___日前完成**，以利作業

資訊安全長：_____