105學年度資訊安全推動小組第1次會議記錄

時　　間： 105 年 9 月 30 日（星期五）15:00

地　　點：新店校區耕莘樓 3 樓 C308 會議室、宜蘭校區行政樓 2 樓 A-203 會議室

主　　席：林校長淑玟

記　　錄：彭麒修

出 席 者：林淑玟委員、劉蕙蓉委員、葉國良委員、林志弘委員、何昭中委員
李書芬委員、葉泓源委員、王美業主任、李瑞美委員、吳怡萍委員
陳佩彥委員、何金城委員、陳佩彥委員、曾惓慈委員、何宜倩委員
彭麒修委員、姜元媛委員、林冠伶委員、江悅慈委員、呂美煥委員
薛來銘委員、車成緯委員
黃美綺委員(妝 531-新店校區學生會代表）
黃嘉榆委員(N534 宜蘭校區學生自治會代表）

一、主席致詞：

上次會議決議事項執行情形報告

項次	上次會議決議事項	執行情形
1	104 年度統合視導統合視導報告及改善措施與工作	依104學年度資訊安全推動小組第2次會議通過後,依會議決議進行改善措施及工作。
2	105 年度資訊安全危機處理防護演練計畫執行結果及檢討	依104學年度資訊安全推動小組第2次會議通過後，請相關單位列入年度工作計畫，並作為內控程序增修依據，「業務流程衝擊分析表」與「演練暨處理執行表」及「矯正與預防處理單」一併同會議記錄陳請資訊安全長覆核。
3	105-1 學期資圖中心資安(含個資)教育訓練規劃	依104學年度資訊安全推動小組第2次會議通過後，依規劃場次進行資安教育練。
4	修正「資訊安全暨緊急應變管理規範」	依104學年度資訊安全推動小組第2次會議通過後，依修訂條文內容進行「資訊安全暨緊急應變管理規範」修正。
5	廢除「校園網路及電腦使用者規範」	依104學年度資訊安全推動小組第2次會議通過後，廢除「校園網路及電腦使用者規範」。
6	建立中華電信無線網路熱點	中華電信因成本考量暫不於本校建置熱點。

7	105 學年度資訊暨圖書中心學校經費編列執行內容	依104學年度資訊安全推動小組第2次會議通過後，依決議執行。

二、工作報告：

完成事項

1. 宜蘭校區網路架構重整工程。
2. 辦理資訊安全講座及教育訓練。
3. 校園資安事件報告。
4. 教育部 105 年度學術機構分組資通安全通報演練計畫。
5. 伺服器、網路及系統安全自我稽核檢查。
6. 完成 104 學年度全校各單位個資盤點及文件查核工作。
7. 完成 104 學年度全校各單位個資風險評鑑報告，並已呈繳校內稽核小組。
8. 目前全校各教學及行政單位正進行個資現場查核工作。
9. 105 學年度各單位個資保護窗口，已調查並公佈於本校個資宣導網站。

待辦事項

1.ad認証Web Service服務建立。

2.105提升資訊設備與建置(全人系統_提案單位: 全人、教務-第一年整合式數位學習平台建置、第二年學習分析診斷系統建置_提案單位: 教務處）。

3.配合交通大學校園共享版moodleset 3.0數位教學共同平台開發。

4.預計106年3月修訂個人資料保護相關程序書、作業說明書，本文件擬由資圖中心依據法規先行修正，經相關會議通過後，請各單位配合遵守。

三、提案討論：

提案 1：106 年度資訊安全危機處理防護演練計畫，提請討論。

說　明：

1. 依據本校「資訊安全暨緊急應變管理規範」，每年需進行一次 106 年度資訊安全危機處理防護演練。
2. 擬自 3/6 至 4/30 進行「106 年度資訊安全危機處理防護演練」，，演練計畫詳附件 1。
3. 演練分兩階段進行，第一階段自 3/6 至 3/31，由全校各單位就既有資訊系統業務流程進行衝擊分析，釐清重要程度。第二階段針對衝擊分析結果為「高」的項目，進行危機處理防護之緊急應變演練，針對資料庫與系統備份還原，以及資訊系統停止提供服務時之人工應變作業進行。

決　議：照案通過，並加強與各系統負責同仁溝通，推行演練前教育訓練。

提案 2：105 學年度資訊暨圖書中心資訊素養教育訓練，提請討論。

說　明：

1. 為提升教職同仁教學及行政業務處理的專業能力，使具備良好的資訊素養內涵及資訊能力，強化教學品質與行政業務處理效能。特規劃辦理此一系列之相關活動，請詳參附件 2。
2. 課程內容除以評鑑表冊、計畫書及日常行政所需統計圖表與剪報等需求外，更融入 BAP（Business Application Professionals）國際認證技能指標進行案例導向規劃，並於課程結束後之寒假期間，配合國際認證場次安排輔導及考照。

決　議：照案通過，依照會議決議公告實施。

提案 3：依據教育部「教育體系資通安全暨個人資料管理規範 2016 版」檢視本校資安及個資相關法規，進行必要之修正，提請討論。

說明：教育部為配合資通訊環境之變遷，針對「教育體系資通安全暨個人資料管理規範」進行必要之重新檢視與調整，為符合「教育體系資通安全暨個人資料管理規範 2016 版」資訊組針對差異部分進行學校資安規範及相關內控程序修訂，請詳參附件 3。

決　議：照案通過，依照會議決議公告實施。

提案 4：104 學年度個資風險評鑑報告，提請討論。

說　明：

1. 依據本校「個人資料安全維護計畫」辦理。
2. 本校行政及教學單位合計有 17 單位進行個資盤點，各單位已於 105 年 7 月完成 104 學年度個資盤點清冊。
3. 各單位盤點之個人資料共盤點出有 580 項，其中風險值在(中 M)以上者有 9 項，佔總個人資料約 1.5%。
4. 詳細個資風險評鑑報告詳參附件 4。

決　議：照案通過，依照會議決議呈報稽核工作小組。

提案 5：修正本校個人資料安全維護計畫，提請討論。

說　明：1.個資法 2015 年 12 月 31 日修正之個資法第 6 條規定，有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，原則上不得蒐集、處理或利用，僅在例外情形下得以為之。2015 年 12 月 31 日修正時，追加了兩項例外情形：為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內；經當事人書面同意。

2.配合個資法修正，修正本校個人資料安全維護計畫(四)界定個人資料範圍，加註底線文字：

「特種個人資料」之蒐集、處理與利用：本校依照「學校衛生法」規定，學校應建立學生健康管理制度；健康檢查及疾病檢查結果，應載入學籍資料。依「勞工安全衛生法」規定：可蒐集、處理與利用「員工」之「健康檢查」及「醫療」相關資訊。特種個人資料得經當事人書面同意蒐集、處理或利用。

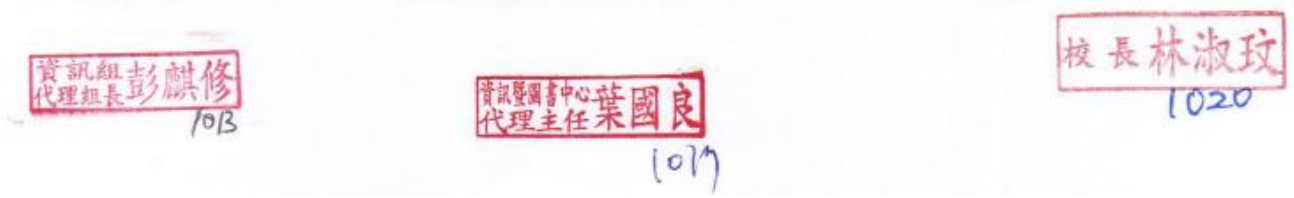
決　議：照案通過，依照會議決議公告實施。

四、臨時動議：

五、散　　會(15:30)。

陳 105 學年度第 1 學期第 1 次資訊安全推動小組委員會會議紀錄

資訊組組長　　資訊暨圖書中心主任　　校長



校園資安事件:

單位	發佈時間	結案時間	事件主旨	處理狀況	後續追蹤
資圖中心 資訊組	105.06.14	105.06.18	日期:20160614 地點:T2-208 學號:100515080 姓名:洪晨祐 違反學術網路使用 netcut 切斷電腦教室其他人網路，學生下載近 10GB 檔案，造成電腦教室網路不穩定，嚴重影響教學網路。	1. 檢查校內對外網路是否正常。 2. 檢查個別網段是否正常。 3. 測試電腦教室網段，確認為 T2-208 媒數科專業電腦教室網路異常。 4. 檢測所有電腦發現某一電腦有私自安裝的 netcut 軟體並大量下載檔案。 5. 詢問之前在該教室上課學生使用此電腦的為洪晨祐同學。 6. T2-208 媒數科專業電腦教室裝有還原卡，電腦進行重新開機即移除 netcut 軟體，T2-208 媒數科專業電腦教室網路回復正常。	填寫資安事件處理單，因該生為數媒科學生，需由所屬單位數媒科說明該事件發生之後續處理情形，以及防範補強措施。
資圖中心 資訊組	15.09.23		加退選課期間學生帳號(102512135-妝543-鄔羽宣)被	資訊組查詢校務系統資料庫，提供教務處該生被退選及加選的時間	教務處協助該生退選被惡意加選的課程。資圖中心探討可能造成本案的原

			盜，課程被惡意退選及加選。	及 IP 地址做為相關證據。	因，並作為爾後建立新的教務行政系統的參考。

附件 1--資訊安全危機處理防護演練計畫

耕莘健康管理專科學校 106 年度
資訊安全危機處理防護演練計畫

壹、 依據:

一、 行政院國家資通安全會報函頒「國家資通安全通報應變作業綱要」。
二、 教育部函頒「教育部資通安全處理小組作業說明」。
三、 耕莘健康管理管理專科學校「資訊安全暨緊急應變管理規範」。
四、 耕莘健康管理管理專科學校內部作業控制程序。

貳、 目的:

一、 為確保本校資訊業務永續運作，並降低關鍵業務流程受重大故障或災害之影響。
二、 各單位資訊系統業務流程衝擊分析。
三、 測試各單位於發現資安事件時，是否可正確、快速執行通報作業。
四、 測試資安聯絡人聯絡管道是否暢通。
五、 測試電子郵件、電話等各種通訊聯絡管道暢通與存活率。
六、 測試使用者在系統故障狀況下之緊急應變，如何正常的進行相關業務處理作業。
七、 測試系統管理者在系統故障的狀況下緊急應變，如何於資安事件容忍時間（最大可容忍中斷時間）內，緊急回復系統運作及資料庫備份及還原與測試。

參、 辦理單位:

一、 主辦單位：資訊安全推動小組。
二、 規劃單位: 資圖中心。
三、 演練單位：依資訊資產盤點後進行業務流程衝擊分析，衝擊分析重要分級為「高」者。
四、 稽核單位:內稽小組。

肆、 演練期程:

一、 各單位資訊系統業務流程衝擊分析重要分級為「高」者：106 年 3 月 6 日至 106 年 3 月 31 日止。

伍、 演練執行情境：

一、 準備作業：各單位資訊系統業務流程衝擊分析，填具「業務流程衝擊分析表」。
二、 負責明細：校際網路資訊安全危機處理防護演練規劃、運作及維護。
三、 情境說明：模擬因「木馬病毒入侵」後，造成系統主機無法正常運作，導致系統服務中斷，且暫時無法提供服務。
四、 標準作業流程：依據資訊安全暨緊急應變管理規範，以及「緊急應變與處理」、「災難復原程序」與「安全事件管理」內控程序辦理，包含下列項目：
1. 目的：病毒入侵發生時，以最短時間恢復校園內部網路及連線單位連線。

2. 中斷狀況：因病毒入侵後，造成系統主機無法正常運作，導致系統服務中斷。
3. 預防措施：
   (1) 於系統主機上加裝防毒軟體。
   (2) 定期進行系統、資料庫之叢集、備援、恢復機制等預防或減災的日常維護措施。
   (3) 業務單位人工作業流程控管及熟稔。
4. 事件通報：通報單位主管、資訊安全小組(資訊暨圖書中心)及各連線單位目前現況。
5. 應變處理：
   (1) 進行資訊安全事件管理程序，依據事件現況評估影響範圍及對組織運作之衝擊。
   (2) 依據事件評估結果，建請資訊安全長決議是否宣布災變及啟動資訊安全危機處理計畫，以維業務持續運作。
   (3) 視需要負責災害現場證據收集，俾利未來可能之訴訟與損害求償事宜。
   (4) 進行緊急應變與處理程序。
   (5) 使用單位改採人工作業因應。
6. 回復作業：進行災難復原程序，回復中毒系統主機正常運作。

陸、 演練執行程序：

一、 資訊系統業務流程衝擊分析。
二、 收到各單位通報或主動式偵測。
三、 進行通報資訊安全小組(資訊暨圖書中心)及單位主管。
四、 檢查網路通訊設備是否運作正常。
五、 檢查網路回應狀態並確認影響範圍。
六、 機房實體線路及電源供應檢查。
七、 檢查系統是否有錯誤訊息。
八、 檢查系統是否有與資料庫正常連線。
九、 檢查系統伺服器是否運作正常。
十、 檢查資料庫伺服器是否運作正常。
十一、依據資安組織內外部聯絡人清單，通知設備及線路、系統廠商處理維修事宜。
十二、使用者在系統未回復前依業務流程及內控作業程序，緊急改用紙本表單進行人工作業。
十三、系統管理人員上線測試完成後，通知各使用單位已恢復並確認系統運作正常。
十四、通知資訊安全小組(資訊暨圖書中心)及單位主管處理完畢。
十五、內稽人員、資訊組人員偕同業務單位資訊系統負責人將演練過程與結果登錄於「演練暨處理執行表」後，陳請資訊安全長簽核。

柒、 其他注意事項：

一、 全程參與研習人員每場核發研習時數 3 小時。
依教育部資安規定，各業務性質同仁每年度所應接受訓練時數如下：一般主管（3 小

時)、資訊人員（6 小時)、資安及稽核人員（12 小時)、一般使用者（3 小時)。

二、 本次演練結果檢討後，於一個月內擬定改善計畫填具「矯正與預防處理單」，由資圖中心資訊組彙整，提交資訊安全推動小組專案報告，陳請資訊安全長簽核後，作為擬定「業務持續運作管理」內控程序之依據。

業務流程衝擊分析表

紀錄編號：　　填表日期：　　年　　月　　日

業務流程	單位名稱	負責人	系統復原時間目標（RTO）	資料復原時間目標（RPO）	重要分級	備註
					□高□中□低	
					□高□中□低	
					□高□中□低	
					□高□中□低	
					□高□中□低	
					□高□中□低	
					□高□中□低	
					□高□中□低	

說明事項：

1. 資圖中心資訊組應協同各單位針對單位資訊系統業務服務，檢視其流程。依業務之重要性、資訊資產價值及風險評鑑結果，鑑別出關鍵業務。
2. 進行業務衝擊分析，應判斷各項資訊資產與業務流程中斷時，對於本校各單位業務流程之影響及衝擊程度，據以判斷最大可容忍中斷時間（本校為 24 小時）、系統復原時間目標（Recovery Time Objective, RTO），以及資料復原時間目標（Recovery Point Objective, RPO）等，分別給予「高」、「中」或「低」之重要分級，並將業務衝擊分析之結果登錄於「業務流程衝擊分析表」，並呈資訊安全推動小組審查。重要分級為「高」之業務流程，即為本校之關鍵業務流程。
   (1) 系統復原時間目標（Recovery Time Objective, RTO）：於基礎設施正常供應下，關鍵業務從事件發生到復原的目標時間，以小時為基本單位。
   (2) 資料復原時間目標（Recovery Point Objective, RPO）：於基礎設施正常供應下，關鍵業務從事件發生到復原期間，資料所能回復之時點，以小時為基本單位。此將影響系統與資料庫備份頻率設定。

業務單位承辦人	業務單位主管	資訊組承辦人	資訊組組長	資圖中心主任	資訊安全長

演練暨處理執行表

承辦人：
協辦單位：
演練日期：

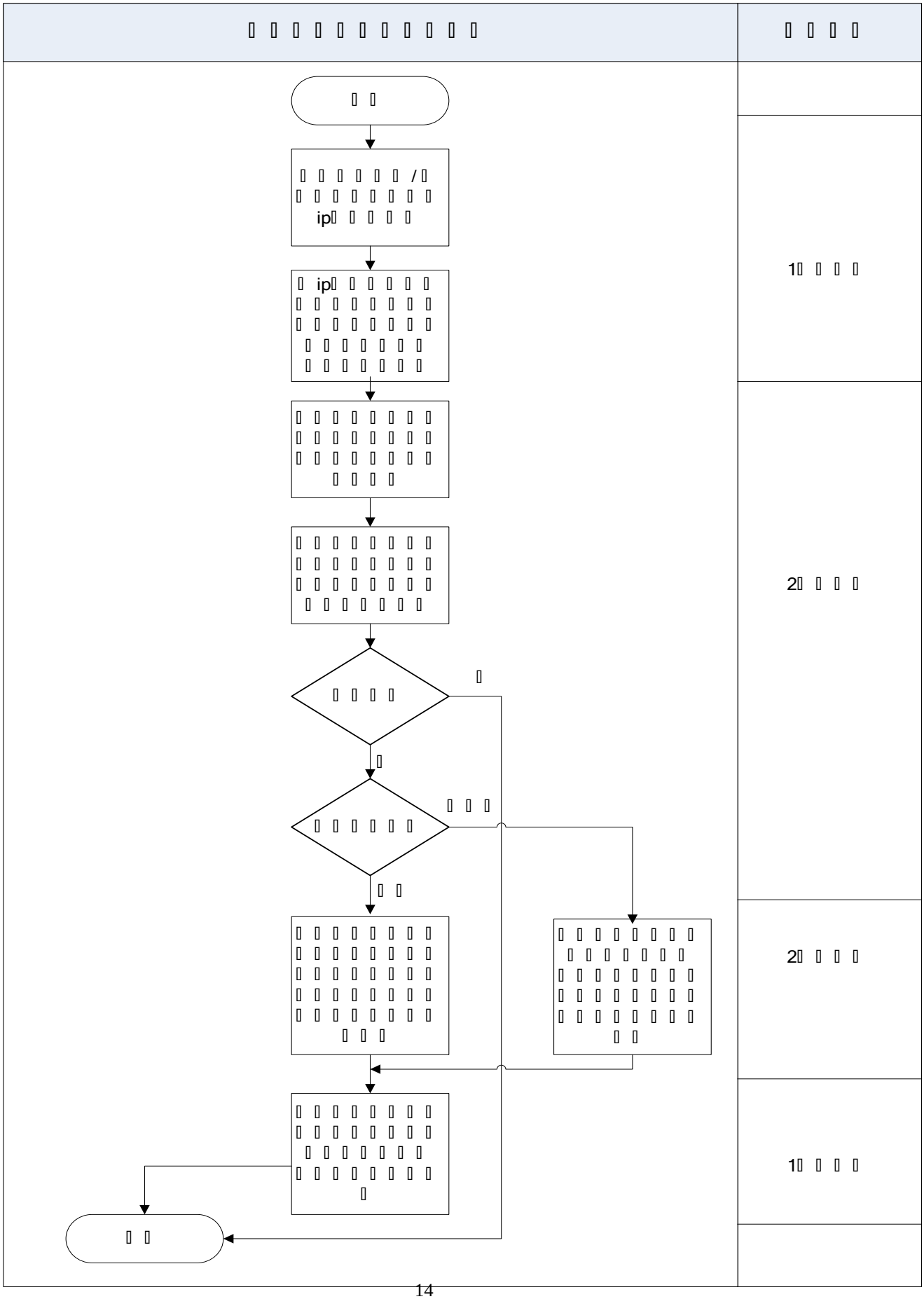
計畫開始時間		計畫需要時間	
計畫結束時間		實際作業時間	

演練執行項目 （下列項目僅為範例參考）		執行程序 （實際演練過程之執行紀錄）	負責人 簽章	執行結果
1	進行通報流程			
2	確認網路是否暢通			
3	檢查網路回應狀態			
4	網路通訊設備是否正常運作			
5	實體線路檢查			
6	進行通報流程			
7	使用者（或承辦人）上線測試			
8				
9				
10				
11				
12				
13				
14				
15				
16				

17				
18				
初步檢討：				

內稽人員	業務單位主管	資訊組承辦人	資訊組組長	資圖中心主任	資訊安全長

安全事件管理作業程序



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_____

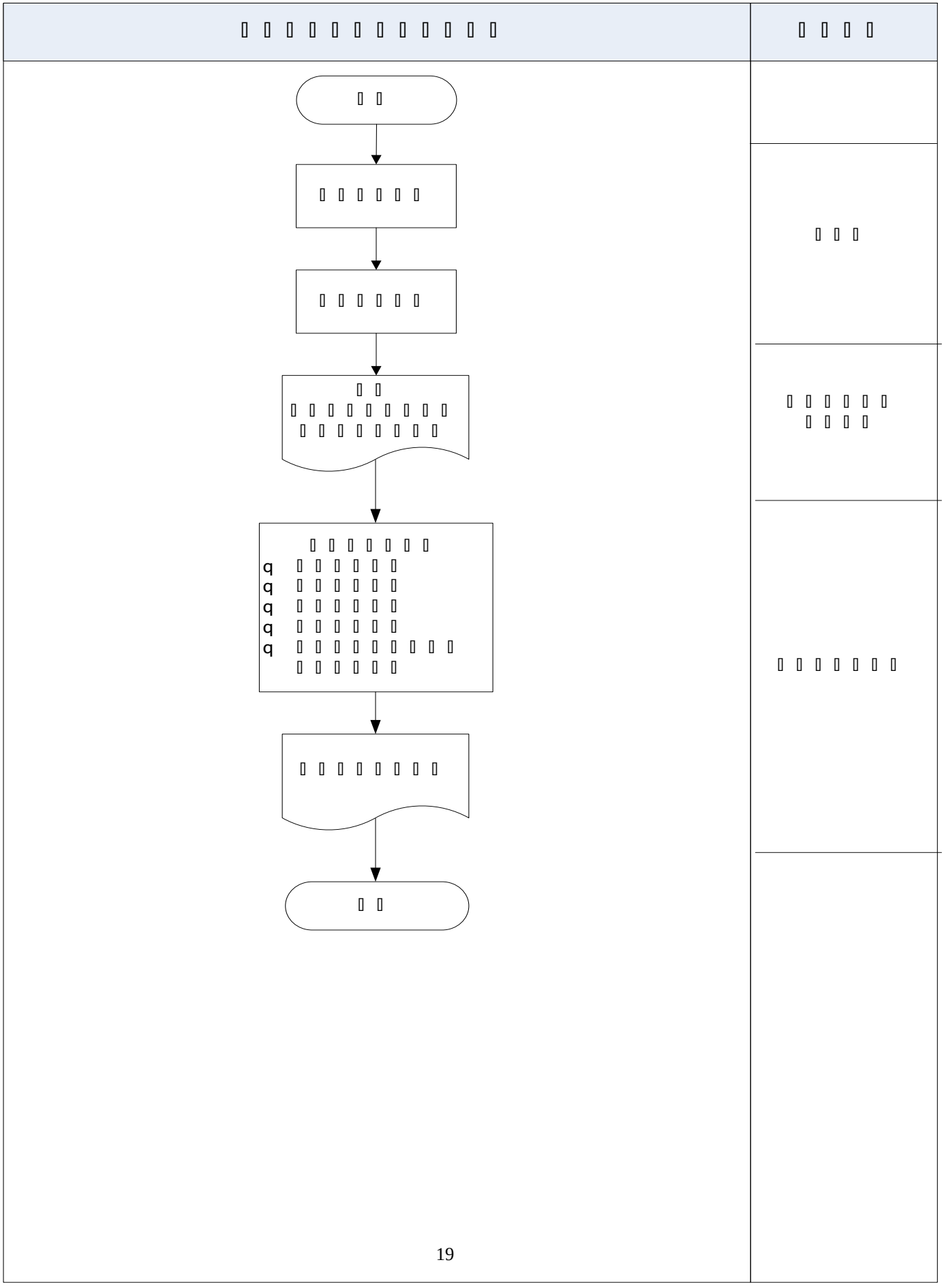
處理意見：

承辦人：_____ 單位主管：_____

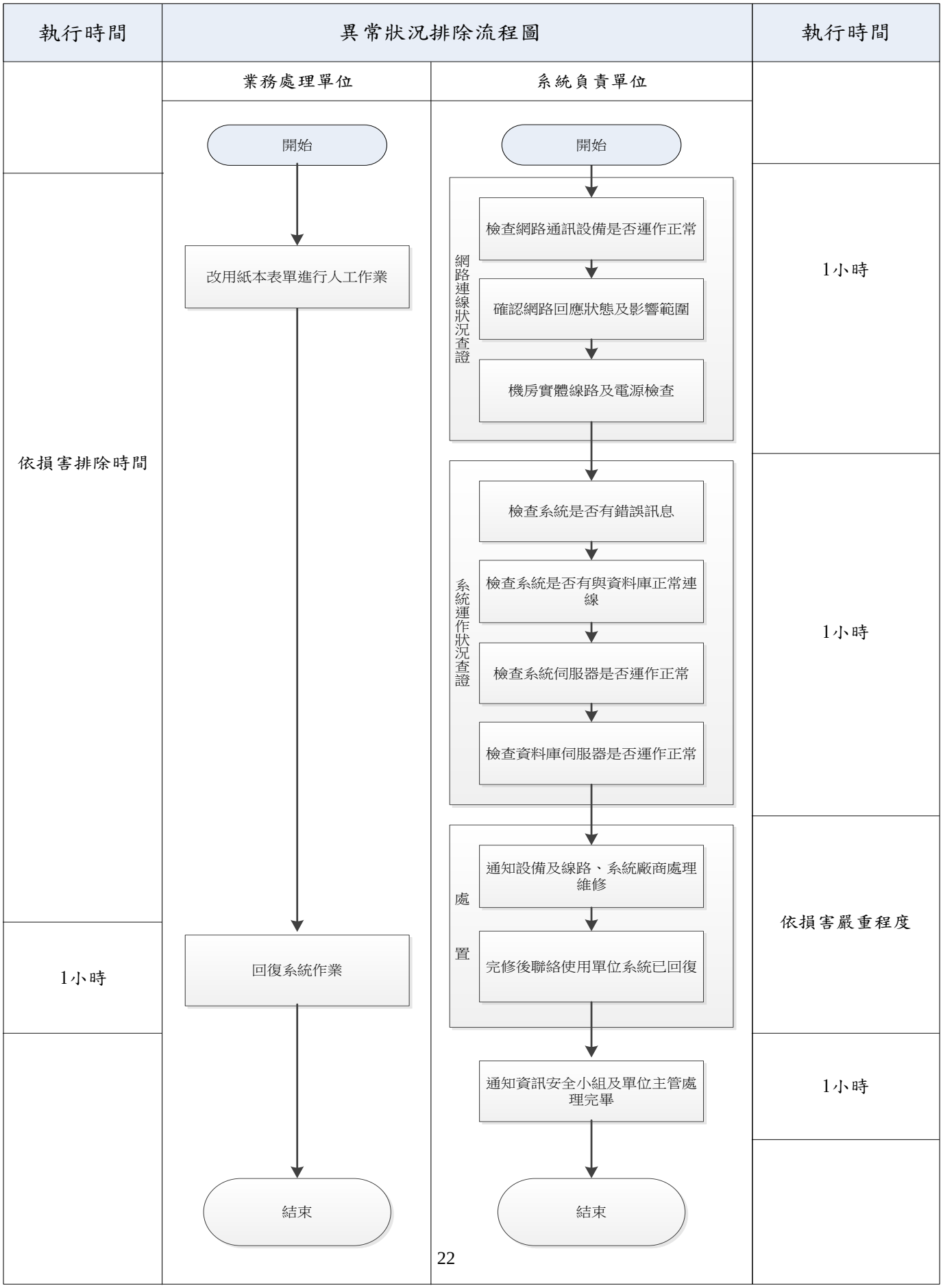
※為配合教育部訂定回報資訊安全處理結果之___天期限，**會辦單位請於___月___日前完成**，以利作業

資訊安全長：_____

緊急應變與處理流程圖



異常狀況處理流程圖


執行時間
異常狀況排除流程圖
執行時間
業務處理單位
系統負責單位
開始
開始
檢查網路通訊設備是否運作正常
確認網路回應狀態及影響範圍
機房實體線路及電源檢查
網路連線狀況查證
1小時
改用紙本表單進行人工作業
檢查系統是否有錯誤訊息
檢查系統是否有與資料庫正常連線
檢查系統伺服器是否運作正常
檢查資料庫伺服器是否運作正常
系統運作狀況查證
1小時
依損害排除時間
通知設備及線路、系統廠商處理維修
完修後聯絡使用單位系統已回復
處置
依損害嚴重程度
1小時
回復系統作業
通知資訊安全小組及單位主管處理完畢
1小時
結束
結束

矯正與預防處理單

紀錄編號：_____　　填表日期：　　年　　月　　日

<table>
<tr><td>提出單位</td><td>OOO</td><td>提出人員</td><td>OOO (稽核組長或稽核人員姓名)</td><td>提出日期</td><td>稽核報告最後簽核日</td></tr>
<tr><td>處理單位</td><td>OOO</td><td>處理人員</td><td>OOO</td><td></td><td></td></tr>
<tr><td>事件分類</td><td colspan="2">□主要不符合事項　□觀察事項
□次要不符合事項　□建議事項</td><td>事件來源</td><td colspan="2">☑內部稽核　　□外部稽核
□資訊安全事件 □自行提出
□其他_____</td></tr>
<tr><td>問題或不符合事項說明</td><td colspan="5">玖、七 經檢視多項表單紀錄
（如：「資訊資產清單」），發現記錄編號、製表日期等欄位尚未填寫。</td></tr>
<tr><td>原因分析</td><td colspan="5">因 ISMS 制度導入期間較為緊湊，故造成部份表單未填上記錄編號及製表日期欄位。</td></tr>
<tr><td rowspan="4">矯正與預防措施評估</td><td colspan="5">暫時性對策：（控制不符合事項的擴大或消除單一事件的影響）
因本處理單無暫時性對策，故不需填入
(原則：若無法立即根治、需等待經費或預算才得以改善之缺失，應列出暫時性之控管措施對策。若永久性對策可以立即進行改善則可不填暫時性對策)</td></tr>
<tr><td>預訂完成日期</td><td></td><td>追 蹤 人</td><td colspan="2"></td></tr>
<tr><td>追蹤日期</td><td></td><td>確認結果</td><td colspan="2"></td></tr>
<tr><td colspan="5">長期性對策：（消除不符合事項或潛在風險的根本原因，防止類似事件發生）
1. 將目前已產生之 ISMS 制度表單記錄，全部重新檢閱後，把遺漏之記錄編號及製表日期填上。
2. 原發佈表單未有記錄編號及製表日期欄位，將編制入該等表單中後重新發佈。
3. 用 E-mail 向同仁宣導「加強注意填寫表單之記錄編號及製表日期」。</td></tr>
<tr><td>預訂完成日期</td><td>建議：預訂完成日期最長為『提出日期』後一年內，若本處理單無暫時性對策，建議預訂完成日期應盡量控制在一季內)</td><td>追 蹤 人</td><td colspan="2"></td></tr>
</table>

	追蹤日期		確認結果	

注意事項

1. 說明

1.1 矯正措施：為防止不符合資訊安全管理制度(ISMS)實施、操作及使用之事項重複發生，所採取之措施。

1.2 預防措施：為預防不符合資訊安全管理制度(ISMS)實施、操作及使用之事項發生，所採取消除未來不符合事項發生原因之措施。

1.3 缺失：不符合資訊安全管理制度(ISMS)實施及操作事項者。依影響程度分為：

1.3.1 主要缺失：未執行資訊安全管理制度(ISMS)之要求，或多個次要缺失集中於同一控制措施者。

1.3.2 次要缺失：未能完全遵循資訊安全管理制度(ISMS)之要求，但為單一事件者。

1.3.3 觀察：發現可能對資訊安全管理制度(ISMS)造成影響的事實及事件，但未有足夠證據顯示會影響資訊安全政策及目標的達成，卻因未來可能成為缺失而需要再覆核。

1.3.4 建議：發現可能對資訊安全管理制度(ISMS)造成影響的潛在問題，可提出建議之改善措施，以預防未來發生之可能性。

1.4 潛在風險：尚未發生但未來有可能發生之不確定事件。

1.5 暫時性對策：能控制缺失的擴大或消除單一事件的影響之措施。

1.6 長期性對策：能消除缺失或潛在風險的根本原因之措施。

1.7 缺失權責單位：矯正及預防措施之實際執行單位。

2. 原因分析

防制缺失權責單位應分析問題發生之原因及影響程度，決定優先順序與處理時限。

2.1 矯正與預防措施評估

2.1.1 缺失權責單位提出矯正與預防措施時，得區分為暫時性對策及永久性對策，防止類似事件發生。

2.1.2 評估措施時須考慮成本效益及可行性。

2.2 追蹤執行狀況

2.2.1 矯正與預防措施之執行狀況，應由缺失權責單位依據「矯正與預防處理單」確實執行。

2.2.2 有關執行狀況之追蹤，由內部稽核組員、組長或相關權責人員負責。

2.2.3 請依「矯正與預防處理單」上的項目，進行改善，並於一個月內提供改善佐證文件，副本一份繳交至資圖中心資訊組追蹤存查。

內外部系統聯絡人清單

	系統名稱	單位名稱	姓名	職稱	聯絡電話	聯絡電子信箱
內部連絡人	校務行政系統	資訊組	彭麒修	代理組長	02-22191131-5524	Kirin@ctcn.edu.tw
	數位學習網	資訊組	彭麒修	代理組長	02-22191131-5524	Kirin@ctcn.edu.tw
外部連絡人	電子公文系統	漢龍科技股份有限公司	張素綾	專員	02-27893389	suling.cs@gmail.com
	會計系統	先傑電腦股有限公司	戴小姐	經理	05-2398001	at3063@alltop.com.tw
	門禁管理系統	威博系統科技公司	葉仕杰	經理	02-22620020	yeh2055@gmail.com
	產學合作計畫案管理系統	康眾科技股份有限公司	陳昇沅	專案經理	02-27005298	Ryo@kzt.com.tw

附件 2

105 學年度資訊暨圖書中心資訊素養教育訓練

一、主　　旨：教職同仁除應具有教學及業務處理的專業能力外，更應具備良好的資訊素養內涵及資訊能力以提昇教學品質與業務處理效果。而為提升教職同仁資訊素養及能力，而籌辦一系列之相關活動。

二、主辦單位：資圖中心資訊組。

三、辦理對象：全校教職員。

四、實施日期：105 年 9 月 12 日至 106 年 1 月 14 日。

五、活動項目：

場次	日期	時間	地點	課程主題
1	105 年 10 月 5 日(三)	13:30~17:20 (4 小時)	新店:T604 宜蘭:T1-201	基礎 word 應用
2	105 年 10 月 19 日(三)	13:30~17:20 (4 小時)	新店:T604 宜蘭:T1-201	進階 word 應用
3	105 年 11 月 2 日(三)	13:30~17:20 (4 小時)	新店:T604 宜蘭:T1-201	基礎 excel 應用
4	105 年 11 月 16 日(三)	13:30~17:20 (4 小時)	新店:T604 宜蘭:T1-201	進階 excel 應用
5	105 年 12 月 7 日(三)	13:30~17:20 (4 小時)	新店:T604 宜蘭:T1-201	基礎 powerpoint 應用
6	105 年 12 月 21 日(三)	13:30~17:20 (4 小時)	新店:T604 宜蘭:T1-201	進階 powerpoint 應用

附件 3

檢視本校資安及個資相關法規待修正對照表

教育體系資通安全暨個人資料管理規範要點	對應校內政策範圍	二者差異說明
A.5 資訊安全政策訂定與評估	資訊安全政策制定及評估	符合要點
A.6 資訊安全組織	資訊安全組織	符合要點
A.7 人力資源安全	人員安全管理及教育訓練	符合要點
A.8 資產管理	資訊資產分類與管制	符合要點
A.9 存取控制	存取控制安全	符合要點
A.10 密碼學(加密控制)	無	待增加
A.11 實體及環境安全	實體及環境安全	符合要點
A.12 運作安全	通訊與作業安全管理	符合要點
A.13 通訊安全	通訊與作業安全管理	符合要點
A.14 系統獲取、開發及維護	系統開發與維護之安全	符合要點
A.15 供應者關係	無	待增加
A.16 資訊安全事故管理	資訊安全事件之反應及處理	符合要點
A.17 營運持續管理之資訊安全層面	業務永續運作管理	符合要點
A.18 遵循性	相關法規與施行單位政策之符合性	符合要點
B.1 個人資料管理政策	無	待增加
B.2 個人資料管理組織	無	待增加
B.3 人員認知與訓練	無	待增加
B.4 個人資料之識別與風險管理	無	待增加
B.5 公正與合法的處理	無	待增加
B.6 個人資料特定目的處理	無	待增加
B.7 適當相關與正確性	無	待增加
B.8 保存與處置	無	待增加
B.9 當事人權利	無	待增加
B.10 資料安全議題	無	待增加
B.11 國際傳輸	無	待增加
B.12 委外管理	無	待增加

「資訊安全政策」修正條文對照表

修正條文	現行條文	說明
(九)資訊安全稽核人員 …以符合「我國行政院教育部所規範C級專科學校資安等級需求」、本校「資訊安全管理辦法」及相關法令、法規之要求…	目的 …以符合「我國行政院教育部所規範 C 級資安等級的需求」、本校「資訊安全管理辦法」及相關法令、法規之要求…	增加「專科學校」。
適用範圍 3.1 本政策適用範圍為本校之內部人員(專兼任教職員生)、委外服務廠商及其所屬專案人員與訪客等。	適用範圍 3.1 本政策適用範圍為本校之內部人員(專兼任教職員生)、委外服務廠商與訪客等。	增加「及其所屬專案人員」。
目標 4.1.… 4.2. 保護本校業務服務之安全，避免未經授權的修改，以確保其可用性與完整性。	目標 4.1.… 4.2. 保護本校業務服務之安全，避免未經授權的修改，以確保其~~正確性~~與完整性。	將「正確性」修正為「可用性」。
責任 5.1.… 5.2.… 5.3 本校全體人員、委外服務廠商及其所屬專案人員與訪客等皆應遵守本政策。	責任 5.1.… 5.2.… 5.3 本校全體人員、委外服務廠商與訪客等皆應遵守本政策。	增加「及其所屬專案人員」。

備註：請於修正處畫底線標示，俾便對照。

耕莘健康管理專科學校

資訊安全政策

1　目的

為確保耕莘健康管理專科學校（以下簡稱「本校」）所屬之資訊資產的機密性、完整性及可用性，以符合「我國行政院教育部所規範C級資安等級的需求」、本校「資訊安全管理辦法」及相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本校之業務需求，訂定本政策。

2　聲明

資安觀念眾知曉，機密資料保護好，完整正確不可少，安全服務為首要。

3　適用範圍

3.1 本政策適用範圍為本校之內部人員(專兼任教職員生)、委外服務廠商與訪客等。

3.2 場所：本校新店、宜蘭二校區。

3.3 設備：

本校二校區主機代管設備、資訊機房設備、教學用設備、行政用設備、教職員生個人資訊設備。

3.4 資訊安全管理範疇涵蓋11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：

3.4.1　資訊安全政策訂定與評估。

3.4.2　資訊安全組織。

3.4.3　資訊資產分類與管制。

3.4.4　人員安全管理與教育訓練。

3.4.5　實體與環境安全。

3.4.6　通訊與作業安全管理。

3.4.7　存取控制安全。

3.4.8　系統開發與維護之安全。

3.4.9　資訊安全事件之反應及處理。

3.4.10　業務永續運作管理。

3.4.11　相關法規與施行單位政策之符合性。

4　目標

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

4.1 保護本校業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。

4.2 保護本校業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

4.3 建立本校業務永續運作計畫，以確保本校業務服務之持續運作。

4.4 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。

5 責任

5.1 本校應成立資訊安全推動小組統籌資訊安全事項推動。

5.2 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。

5.3 本校全體人員、委外服務廠商與訪客等皆應遵守本政策。

5.4 本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。

5.5 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。

6 審查

本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，並確保本校業務永續運作之能力。

7 實施

本政策經資訊安全推動小組通過，提請行政會議審議，陳請校長核定後，公布實施，修訂時亦同。

附件 4

耕莘健康管理專科學校

「個人資料檔案」
風險評鑑報告書

機密等級：限閱

版本編號：1.0

修訂日期：105.07.31

一、 目的

耕莘健康管理專科學校(以下簡稱本校)為依據「個人資料保護法」、「個人資料保護法施行細則」(以下簡稱細則)與相關法規規範，提供本校擁有個資資產之相關單位，共同遵行之風險評鑑標準，以協助有效執行風險控管，預防個資外洩事件之威脅。

二、適用範圍

適用於本校各單位，本校所屬機關準用之。

三、 名詞定義(詳見個人資料保護法第二條)

(一) 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

(二) 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

(三) 蒐集：指以任何方式取得個人資料。

(四) 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

(五) 利用：指將蒐集之個人資料為處理以外之使用。

(六) 國際傳輸：指將個人資料作跨國（境）之處理或利用。

(七) 公務機關：指依法行使公權力之中央或地方機關或行政法人。

(八) 非公務機關：指前款以外之自然人、法人或其他團體。

(九) 當事人：指個人資料之本人。

(十) 威脅：可能對系統或組織造成傷害之意外事件。

(十一) 弱點：因個資資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

(十二) 風險：可能對團體或組織的資產發生損失或傷害的潛在威脅，通常用產生之影響及發

生機率來衡量。

四、 權責說明

(一)本校各單位（以下簡稱各單位）應指定專人辦理下列事項：

1. 當事人依個人資料保護法第十條及第十一條第一項至第四項所定請求事項之考核。
2. 個人資料保護法第十一條第五項及第十二條所定通知事項之考核。
3. 個人資料保護法第十七條所定事項之公開或查閱。
4. 個人資料保護法第二十七條所定個人資料檔案安全維護。
5. 個人資料保護法令之諮詢。
6. 個人資料保護事項之協調聯繫。
7. 單位內個人資料損害預防及危機處理應變之通報。
8. 本校個人資料保護規範及各資安全維護計畫之執行、單位內個人資料保護之自行查核。
9. 其他單位內個人資料保護管理之規劃及執行。

(二)、本校應設置個人資料保護聯絡窗口，辦理下列事項：

1. 個人資料保護業務之協調聯繫及緊急應變通報。
2. 重大個人資料外洩事件聯繫窗口。
3. 各單位依前點指定專人之名冊製作及更新。
4. 各單位依前點指定之專人與職員工教育訓練名單及紀錄之彙整。

五、風險評鑑程序說明

(一) 為評估個人資料檔案之風險，本校應規劃個人資料風險評鑑與管理作業，風險評鑑作業應包括下列項目：

1. 評估個人資料風險

(1) 建立風險評鑑的標準(如下表所示)，包括：風險發生之機率與影響/衝擊之程度。個人資料檔案之風險評鑑應依據實際狀況，對照「影響及衝擊等級表」(如下表1)及「風險發生可能性等級表」(如下表)之內容，並於「風險評鑑表」(參考個資表單2-310-016)中進行之風險分析。

表1：影響及衝擊等級表

衝擊項目	衝擊程度	標準說明
個人資料可識別程度	□低度衝擊 □中度衝擊 □高度衝擊	低度—無法識別或查詢困難之個資為低度；需耗時始可辨識者為中度；容易識別者為高度
個資數量	□低度衝擊 □中度衝擊 □高度衝擊	低-20 筆以下（團體訴訟不成立） 一般中-個資 21~10,000 筆 高-特種個資 21~1,000 筆
個人資料敏感程度	□低度衝擊 □中度衝擊 □高度衝擊	是否可以識別到特定人員為判斷標準(否即為低度)
個人資料所屬單位	□低度衝擊 □中度衝擊 □高度衝擊	是否為組織內部個人資料(是即為低度)
是否符合特定目的	□低度衝擊 □中度衝擊 □高度衝擊	是否為特定目的範圍內(是即為低度)
個人資料蒐集處理與利用符合條件	□低度衝擊 □中度衝擊 □高度衝擊	是否符合法定職務範圍、或是符合法定義務範圍(是即為低度)
利用範圍	□低度衝擊 □中度衝擊 □高度衝擊	是否為組織內部所利用(是即為低度)
國際傳輸	□低度衝擊 □中度衝擊 □高度衝擊	是否有國際傳輸行為(否即為低度)
個人資料檔案儲存位置	□低度衝擊 □中度衝擊 □高度衝擊	是否個人資料檔案有受保護的之地點(是即為低度)
個人資料檔案保護機制	□低度衝擊 □中度衝擊 □高度衝擊	是否需要耗費行政工續或相關流程方可取得(是即為低度)

表2：風險發生可能性等級表

風險等級	評估標準
可能性低(1) L	1.很少發生或無發生可能性。 2.0-3年期間沒有發生過。
可能性中(2) M	1.可能發生或偶爾發生。 2.0-3年期間發生次數小於3次。
可能性高(3) H	1.經常發生。 2.1年內發生2次以上。

(2)各單位須針對各項個人資料之使用及控管狀況，依據「影響及衝擊等級表」之各個評估項目，識別其組織面臨內部弱點及外在威脅所產生之影響與衝擊程度，並將影響及衝擊程度記錄於「風險評鑑表」。

(3)識別風險發生之可能性及影響/衝擊程度，將此2項評分進行相乘，即求出該個人資料檔案之風險值。風險值=風險發生可能性等級x影響及衝擊等級表。

(4)將經由風險值計算公式所得之風險值，對應至「風險分布矩陣圖」(如下圖)以判斷風險值之分布情況。

影響程度	風險分布(風險值)		
非常嚴重(3)	3 高度	6 高度	9 極度
嚴重(2)	2 中度	4 高度	6 高度
輕微(1)	1 低度	2 中度	3 高度
	極少可能(1)	有可能(2)	極有可能(3)
	發生機率(等級)		

2. 處理個人資料風險

各單位依照單位內部個資盤點表及各資項目彙整表所列之個資檔案，定期進行風險評估，並填入「個人資料檔案風險評鑑表」。並依風險評鑑結果，對於風險值為高度之個人資料檔案進行風險處理，擬定改善措施，並納入本校內部控制風險評估作業手冊。

(二) 覆核

1. 持續改善

為保持本風險評鑑方法之有效性與適用性，本校各單位應定期檢討「風險評鑑表」之項目，以期確保本校個資資產均處於最佳保護之下。

2. 風險重新評鑑

(1) 每年應至少執行1次風險評鑑。

(2)當範圍內有以下的狀況發生之時，則實施不定期的複核，以更新及確保個資資產風險評鑑的正確性及完整性：

(A) 有新增、變更或移除個資資產。

(B) 組織業務調整。

(C) 個資外洩發生。

六、風險評鑑結果分析

(一)期程

本校自民國105年6月到7月間，執行個資風險評鑑作業之結果，分述如下。

經過個人資料辨識與價值評估結果，此次風險評鑑階段，於相關業務單位辨識出 580 項個人資料檔案。請參考檔冊：「風險評鑑表」。

個資風險評估結果統計			
風險等級(低L)	風險等級(中M)	風險等級(高H)	合計
571	9	0	580

(二)可接受風險值

本校個人資料檔案目前尚未導入個資管理系統，各單位人力作業考量，本次作業之可接受風險值，建議值為風險等級(中M)。可接受風險值之判斷與建議係考量各個人資料價值、威脅利用弱點造成個人及學校權益損害及營運中斷之可能性對應所產出之風險分布來判斷。資訊資產最終風險值為高於(中M)者，將於風險改善計畫表中提出處理建議方案，經風險評鑑結果確認本校今年度無超過可接受風險之個資資產，因此無風險改善計畫。