耕莘健康管理專科學校

102學年度校園網路管理及資訊安全推動小組第2次會議紀錄

時間：103 年 04 月 15 日（星期二）上午 8：30

地點：耕莘樓 3 樓會議室、宜蘭校區行政 2 樓會議室

出、列席者：如簽名單

主席：蕭校長淑貞

記錄：鍾大定

一、主席致詞：（無）

資訊安全簡介：辜國隆博士，簡報檔請詳參附件 1。

二、工作報告：

近期校園資安事件報告，內容請詳參附件2

三、提案討論：

提案 1（提案單位：資訊暨圖書中心資訊組）：

案由：訂定耕莘健康管理專科學校資訊安全管理辦法，提請審議。

說明：1. 依據「教育部所屬機關及各公私立學校資通安全工作事項」，本校所屬「資訊安全責任等級分級」為「C級」，防禦機制強度等級為「2」，應執行工作要項如下：

- 各單位自行成立推動小組規劃資訊安全管理系統(Information Security Management System, ISMS）作業。
- 稽核方式為「自我檢視」。
- 主官,主管,技術,一般人員所應接受資安教育訓練，分別為每年2,6,12,4小時，技術人員應接受資安專業訓練。
- 每年進行一次檢測機關網站安全弱點。

2. 學校資訊安全政策為「符合我國行政院教育部所規範C級資安等級的需求」。
3. 學校訊安全聲明為「機密資料保護好，完整正確不可少，安全服務為首要，永永遠遠沒煩惱。」
4. 為強化校園資訊安全管理，建立安全及可信賴之電子化系統，確保資料、系統、設備與網路之安全，特依據「行政院及所屬各機關資訊安全管理要點」、「教育體系資通安全管理規範」及「教育部所屬機關及各公私立學校資通安全工作事項」，擬定「耕莘健康管理專科學校資訊安全管理辦法」，以作為學校「資訊安全政策」與「資訊安全管理規範」之原則，請詳參附件3。

擬辦：通過後，提請行政會議議決。

討論：林淑玟副校長：離職員工電子郵件帳號是否停用，並將其自通訊錄群組中刪除，以免資料外流。此外，先前評鑑時，教務組的委員曾建議建置異地備援系統，是否考量？重點時刻如選課需要加強備份。

辜國隆顧問：1. 異地備援考量是系統或資料，系統則耗費較大。

2. 備援是需要演練的，需考量對系統停止作業之忍受時間，並考量永續經營之問題，若沒有系統時的人工作業要可以進行，待系統恢復正常時再依紙本資料進行輸入，使工作不中斷。
3. 每個條文都是一個流程，且非資訊單位可以負責，建議校層級能夠主導。

葉國良代理主任：後續會訂定本校資訊安全規範，非重點時刻則以 24 小時為最大忍受時間，也請各位主管先行思考對於資安事件所造成資訊服務中斷的容忍程度。

對於異地備援或備份機制，將納入中長程計畫中考量。會後議會請資訊組同仁再行檢視離職員工帳號及通訊錄。

決議：照案通過，並請各單位將會議中討論與建議部分納入後續擬定資安政策及規範之執行面考量。

提案 2（提案單位：資訊暨圖書中心資訊組）：

案由：修訂校園網路管理及資訊安全推動小組設置要點，提請審議。

說明：1.本小組僅就個資及資安相關議題討論，故擬修訂本小組設置要點之名稱。

2.依據「耕莘健康管理專科學校資訊安全管理辦法」修訂本要點，請詳參附件 4。

擬辦：通過後，提請行政會議討論。

討論：無。

決議：照案通過。

提案 3（提案單位：秘書室）：

案由：擬定本校個人資料保護管理規範，提請審議。

說明：為強化本校個人資料保護及管理，係依據「個人資料保護法」、「個人資料保護法施行細則」及「教育體系資通安全管理規範」等相關規定為基礎訂定之，請詳參附件 5。

擬辦：通過後，於本校個資法宣導執行專區公告實施。

討論：林淑玟副校長：請取消表單編號之標註，以免每次修正編號時都要再提案修規範。

決議：依建議修正後通過。

四、臨時動議：（無）

五、主席結論：（無）

六、散　　會：（上午 09：30）

資訊組組長　　資訊暨圖書中心主任　　校長

附件 2

已通報教育機構資安通報平台之資安事件

事件單編號	單位	來源	等級	IP	發佈時間	結案時間
28547	耕莘健康管理專科學校	N-ASOC	1 級		2013-10-23 14:46:22	2013-10-23 14:48:28
28290	耕莘健康管理專科學校	N-ASOC	1 級	163.21.98.252	2013-10-21 08:57:42	2013-10-21 10:37:45
28195	耕莘健康管理專科學校	N-ASOC	1 級	163.21.98.226	2013-10-18 08:16:41	2013-10-19 22:26:25
27579	耕莘健康管理專科學校	N-ASOC	1 級	163.21.98.248	2013-10-01 13:56:05	2013-10-01 16:56:22
32916	耕莘健康管理專科學校(宜蘭校區)	N-ASOC	1 級	120.101.97.60	2014-01-23 10:37:40	2014-01-23 10:51:17
32631	耕莘健康管理專科學校(宜蘭校區)	N-ASOC	1 級	120.101.97.60	2014-01-14 15:38:51	2014-01-14 16:10:45
27837	耕莘健康管理專科學校(宜蘭校區)	N-ASOC	1 級	120.101.127.254	2013-10-11 08:36:50	2013-10-13 23:04:47
26818	耕莘健康管理專科學校(宜蘭校區)	N-ASOC	1 級	120.101.127.36	2013-09-10 11:17:27	2013-09-10 14:30:01

發生資安事件時，請盡速登入教育機構資安通報平台進行通報流程。

事件等級 3.4 級，需於 36 小時內登入教育機構資安通報平台完成所有通報應變流程。

事件等級 1.2 級，需於 72 小時內登入教育機構資安通報平台完成所有通報應變流程。

近期資安事件（102.07～102.09）：

時間	事件	原因	改進措施
102.03.26	電子郵件無法收發	教師使用預設密碼,被駭客轉寄大量電子郵件	1. 請教師修改密碼 2. 發信提醒教職員安全使用電子郵件應注意事項 3. 查出對方 IP 與 Email，加入黑名單 4. 於電子郵件系統中設定密碼等級中以上，並須於 180 日內更換密碼。

附件 3

耕莘健康管理專科學校資訊安全管理辦法（草案）

民國 103 年 04 月 15 日校園網路管理及資訊安全推動小組會議通過

民國 000 年 00 月 00 日行政會議通過

第一條　為強化資訊安全管理，建立安全及可信賴之電子化系統，確保資料、系統、設備與網路之安全，特依「行政院及所屬各機關資訊安全管理要點」及「教育體系資通安全管理規範」訂定本辦法。

第二條　有關資訊安全管理事務，依下列原則分工：

一、 資訊暨圖書中心負責研擬、建置及評估資訊安全政策、規範及相關實施計畫等事項。

二、 學校各業務單位依據資訊安全政策、規範及相關實施計畫，負責資料之使用管理及維護等事項。

第三條　資訊安全管理原則如下：

一、 各單位對可存取機密性或敏感性資訊或系統之人員，及因工作需要須配賦系統存取特別權限之人員，應簽署保密協議。

二、 負責重要資訊系統之管理、維護及操作之人員，應妥適依權責分工，並建立代理人制度。

三、 業務主管應負責督導所屬之資訊或資料作業安全，防範不法或不當行為。

四、 利用公眾網路或電子郵件等網路工具傳送資訊或進行交易處理，應注意可能發生之風險。

五、 利用網際網路與全球資訊網公布及流通資訊，應注意資料之安全性、機密性及敏感性，未經當事人同意之個人隱私資料及文件，不得上網公布。單位網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭違法竊取或不當使用。

六、 離（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（休）職必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

七、 辦理資訊業務委外作業時，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約中。廠商以遠端登入方式進行系統維護者，應加強安全控管。廠商建置及維護重要軟硬體設施時，應在本校相關人員監督及陪同下始得為之。

八、 各單位對於儲存各項機密資料或程式軟體之磁碟及光碟片等媒體，應設專人管理並定期備份，防止資料洩漏或損毀。並依資料之儲存方式不同，避免因環境因素造成對儲存媒體之損害。

九、 對於電腦設備之裝置地點，應考量使用及管理上之安全，並應指定專人負責，非經允許，不得進入及隨意操作設備，並採行必要之事前預防及保護措施，偵測及防制電腦病毒與其他惡意軟體，以確保系統正常運作。

十、 應擬定「資訊安全政策」與「資訊安全管理規範」，評估資安相關法令與各種資安事件對單位正常業務運作之影響，審查政策的可行性與有效性，並訂定相關緊急應變與回復作業程序及相關人員之權責，定期演練與調整更新計畫，以維業務永續運作。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，並經由資訊安全推動小組及行政會議審議通過後，以適當方式向所有員工公布與宣導，在必要時告知相關單位及合作廠商，以利共同遵守。

第四條　若發生資訊安全事件，應立即向資訊組人員通報，以利資訊組採取適當反應措施。若確定為資安事件，發生事件之單位應填寫資安事件通報表至資訊組。

第五條　應成立本校「資訊安全推動小組」，以統籌本校資訊安全政策擬定、推行及稽核、管理事宜。資訊安全推動小組設置要點另訂之。

第六條　本辦法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，修正時亦同。

檔　　號：
保存年限：

教育部　函

地址：臺北市中山南路5號
傳真：(02)2737-7043
聯絡人：塗正良
聯絡電話：(02)8732-9045

發文日期：中華民國96年12月19日
發文字號：台電字第0960196582號
速別：普通件
密等及解密條件或保密期限：普通
附件：教育部機關學校資通安全工作事項（196582.DOC，共1個電子檔案）

主旨：各機關、學校應編列經費落實資通安全工作事項，資訊安全長(副首長以上)應加強監督執行情形，請 查照。

說明：

一、檢送「教育部所屬機關及各公私立學校資通安全工作事項」。

二、各縣市政府教育局請轉知所屬國中小學，並協助監督考核執行情形。

正本：公私立大專院校、公私立高級中等學校、各縣市政府教育局、部屬機關、國立小學、附設醫院、農林場、臺灣學術網路區域網路中心、各縣市教育網路中心
副本：本部高教司、政風處、技職司、中教司、國教司、中部辦公室、體育司、教研會、電算中心(副本均含附件)

教育部所屬機關及各級公私立學校資通安全工作事項

壹、 資訊安全責任等級分級：

一、機關學校應參考「資訊安全責任等級分級」及本部相關規定，執行相關資訊安全管理工作，各縣(市)政府應協助所轄中小學執行資訊安全工作。

二、依據行政院於 94 年 7 月 21 日核定「政府機關（構）資訊安全責任等級分級作業施行計畫」，各資訊安全責任等級分級應執行工作項目如下：

作業 / 內容 / 等級	防禦機制強度	防護縱深	ISMS 推動作業	稽核方式	資安教育訓練(主官,主管,技術,一般)	專業證照
A 級	強度等級 4	NSOC/SOC、IDS、防火牆 防毒	96年通過第三者認証	每年至少執行二次內稽	(4,6,18,4 小時)/每年	96年資安專業鑑定證照二張
B級	強度等級 3	SOC(OP) IDS、防火牆 防毒	97年通過第三者認証	每年至少執行一次內稽	(4,6,18,4 小時)/每年	96年資安專業鑑定證照 一張
C級	強度等級 2	IDS, 防火牆 防毒	各單位自行成立推動小組規劃作業	自我檢視	(2,6,12,4 小時)/每年	資安專業訓練
D級	強度等級 1	防火牆 防毒	推動 ISMS 觀念宣導	自我檢視	(1,4,8,2 小時)/每年	資安專業訓練

資訊安全責任分級包含本部所屬機關及各公私立學校區分如下：

A 級：教育部、台大醫院、成大醫院

B 級：大學、區域網路中心、縣(市)教育網路中心

C 級：學院、專科學校、部屬館所

D 級：高中職、國中小學

貳、 資通安全通報應變：

一、需配合「國家資通安全緊急應變中心」建立緊急通報應變組織，各機關學校應建立資訊安全長(副首長以上)及 2 位資訊安全聯絡人，並列入行政業務交接項目。

二、2 位資訊安全聯絡人應於「國家資通安全應變網站」登入基本資料：

網址 https://www.ncert.nat.gov.tw 電話：(02)2733-9922

名稱	姓名	職稱	電話	傳真	行動電話	E-MAIL
第 1 聯絡人						
第 2 聯絡人						

三、機關學校發現資安事件或接獲「國家資通安全會報」、本部等相關主管機關通知發生資

安事件時，應於 1 小時內至「國家資通安全應變網站」進行資安事件通報，並於 36 小時內處理完成或完成損害控制後至進行結案通報。

四、 機關學校應配合「國家資通安全會報」及本部每年辦理資通安全攻防演練、通報演練、社交工程演練等相關演練作業。

參、 資訊安全防護：

一、 電腦網路使用安全注意事項：

（一）各機關學校應酌參「立法院審議 96 年度中央政府總預算—通案附帶決議事項」，並考量網路環境狀況訂定合適之「電腦網路使用安全注意事項」並確實執行，以有效規範行政人員、教師、學生電腦網路使用安全。

（二）應建立網路使用安全稽核機制，並適當進行內部稽核或自我檢視。

二、 網路安全管理：

（一）應設置防火牆並適當阻絕外部對內之網路連線及通訊埠。

（二）應訂定「網路安全管理作業規範」、建立網路對外服務申辦作業及安全檢查。

（三）網路安全建立檢核機制，並適當進行安全檢核。

三、 電腦系統安全管理：

（一）應訂定「電腦設備安全管理作業規範」，以規範伺服主機及個人電腦作業系統建置安全，系統上線使用前應建立申辦作業及安全檢查。

（二）電腦設備作業系統及相關伺服軟體應適時更新軟體及進行漏洞修補。

（三）電腦設備作業系統應安裝防毒軟體並適時更新病毒資料庫。

（四）作業系統進行遠端維護時，應於加密管道進行，並管制維護來源 IP。

（五）電腦系統應建立檢核機制，並適當進行安全檢核。

四、 應用軟體(網站)安全管理：

（一）應訂定「應用軟體安全管理作業規範」以規範應用軟體、資料庫、程式開發建置及使用安全，系統上線使用應建立申辦作業及安全檢查。

（二）應用程式所有輸入欄位應進行字元檢查，排除不必要特殊字元(如’ "!$%^&*_|-><;等)以防止資料庫隱碼攻擊(SQL-injection)。

（三）應用程式進行遠端維護時，應於加密管道進行，並管制維護來源 IP。

（四）應用軟體應建立檢核機制，並適當進行安全檢核。

肆、 相關文件說明：

一、 教育體系資訊安全管理制度(ISMS)規範：

（一）教育體系資訊安全管理制度規範網址：

http://www.edu.tw/EDU_WEB/EDU_MGT/MOECC/EDU0688001/tanet/fix.htm

（二）教育體系各機關適用對象如下：

1.「教育體系資通安全管理規範」第 1 群：適用教育部電算中心、部屬館所、縣(市)網中心及公私立大專院校。

2. 「教育體系資通安全管理規範」第 2 群：適用公私立高中職學校。

3. 「國中小學資通安全管理系統實施原則」：適用國中小學。

（三）教育體系資訊安全管理制度規範導入試作點範例—國立成功大學

http://www.edu.tw/EDU_WEB/EDU_MGT/MOECC/EDU0688001/tanet/fix.htm

附件 4

耕莘健康管理專科學校

「校園網路管理及資訊安全推動小組設置要點」修正條文對照表

修正條文	現行條文	說明
設置要點名稱 資訊安全推動小組設置要點	設置要點名稱 校園網路管理及資訊安全推動小組設置要點	修正設置要點名稱。
第　一　條 依據「耕莘健康管理專科學校資訊安全管理辦法」，特設立耕莘健康管理專科學校資訊安全推動小組(以下簡稱本小組)。	第　一　條 本校為校園網路管理及推動資訊安全體制，茲依據教育部 96 年 12 月 19 日台電字第 0960196582 號函及「行政院及所屬各機關資訊安全管理要點」，特設立耕莘健康管理專科學校校園網路管理及資訊安全推動小組(以下簡稱本小組)。	修正小組成立依據。

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

校園網路管理及資訊安全推動小組設置要點

民國98年4月27日行政會議通過

民國102年5月27日行政會議通過

第　一　條　本校為校園網路管理及推動資訊安全體制,茲依據教育部 96 年 12 月 19 日台電字第 0960196582 號函及「行政院及所屬各機關資訊安全管理要點」,特設立耕莘健康管理專科學校校園網路管理及資訊安全推動小組(以下簡稱本小組)。

第 二　條　本小組之職掌：

一、資通安全政策之研議。

二、跨部門資訊安全事項權責分工之協調。

三、資訊資產價值及風險評估之研議。

四、資訊安全事件之危機通報、緊急應變檢討與監督。

五、整體資訊安全措施之協調與研議。

六、應採用之資訊安全技術方法或程序之協調與研議。

七、資訊安全計畫之協調與研議。

八、辦理資訊安全相關教育訓練及稽核業務。

九、制訂校園網路及資訊設備各項使用規範。

十、個人資料保護與管理相關工作事項。

十一、其他重要資訊安全事項之協調與研議。

第　三　條　本小組設委員如下：

一、當然委員：校長、各一級主管、資訊暨圖書中心二級主管及學生代表（由學生自治會推派一人參加）。

二、選任委員：教師代表各科 1 人，由各科推派產生，任期為 1 年，連選得連任之。

第　四　條　本小組設置召集人一人，由校長兼任；副召集人一人，由秘書室主任兼任，負責推動及協調本校個人資料保護管理業務；執行秘書一人， 由資訊暨圖書中心主任兼任，負責綜理本小組相關業務。

第　五　條　本小組每學年至少召開會議 1 次，必要時得召開臨時會議，均由召集人擔任主席，召集人不能出席會議時，由召集人指定委員代理之。開會時應有全體委員二分之一（含）以上出席，決議事項應有出席委員三分之二（含）以上同意。

第　六　條　本小組召開會議時，得邀請本校有關單位人員列席。

第　七　條　本小組會議決議事項，由資訊暨圖書中心資訊組為任務執行督導單位。

第　八　條　本要點經行政會議通過，陳請校長核定後公布實施，修正時亦同。

附件 5

耕莘健康管理專科學校個人資料保護管理規範

民國 103 年 04 月 15 日校園網路管理及資訊安全推動小組會議通過

一、依據：

（一） 個人資料保護法。

（二） 個人資料保護法施行細則。

（三） 教育體系資通安全管理規範。

（四） 「教育部提升校園資訊安全服務計畫」。

二、目的：

耕莘健康管理專科學校(以下簡稱本校)為明確本校各單位個資安全作業權責及通報與應變作業，保障本校個人資料處理之機密性與完整性，特訂定本規範。

三、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。

四、規範內容：

(一)、個人資料使用管理：

1. 向當事人蒐集個人資料時，除法律明文規定外，需經當事人同意並明確告知蒐集目的、個人資料之類別、利用期間、地區、對象及方式。
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. 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蒐集。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」。
4. 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」，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。
5. 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、電腦處理、國際傳遞及利用同意書」，範本內容可依單位需求修改。
6. 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。
7. 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。
8. 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及個資使用者身分以供事後稽查。
9. 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。
10. 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。
11. 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。
12. 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: 資訊暨圖書中心圖書組

辦理事項如下：

1. 本校與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「個資法宣導執行專區」網頁供大眾閱覽。

(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)資圖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，請以專簽會資圖中心辦理，資圖中心將依「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」，克盡保密之責，並確認於異動、離職或合約終止時，變更、取消或停用其使用者識別帳號存取權限，必要時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圖中心辦理。
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」回覆資圖中心。

(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或機密性資料。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)、各單位資安與個資聯絡人每半年填寫「資安及個人資料保護檢核表」，進行自我檢核後，交付資圖中心圖書組備查，並由資圖中心於收件後兩週內進行覆核，以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、本規範經資訊安全推動小組通過，陳請校長核定後公布實施，修正時亦同。

個人資料簽收紀錄

單位	姓名	個人資料 檔案名稱	檔案類型	傳遞加密方式	簽收日期
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		
			□紙本 □電子檔		

人事資料需求表

日期：　年　月　日

機密等級

申請單位					
聯絡人		電話		E-mail	
相關單位	□教務處□學務處□總務處□研發處□資圖中心□會計室 □其他＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿				
需求資料內容					

資料需求概述：

一、用途：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

二、本項資料需求：□經常性　□偶發性 說明：＿＿＿＿＿＿＿＿＿＿

三、使用頻率（作業週期）：□每年一次 □每學期一次 □每月一次
□每週一次 □每日一次　□其他：＿＿＿＿＿＿

四、人工作業每次所需工時：＿＿＿＿＿＿＿＿＿＿＿＿

五、資料需求之格式：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

六、取得資料方式：□email：＿＿＿＿＿＿＿＿□其他：＿＿＿＿＿＿

註: 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。

七、資料需求之輕重緩急：□非常急迫　□急迫　□可依正常之先後次序

※ 申請人必須遵守「個人資料保護法」，妥善保管所取得之個人敏感性資料。

※ 涉個人資料之電子類文件需對資料檔案加密或透過加密通道傳遞。

意見說明	（由人事室填寫）

申請單位		會辦單位		承辦單位	
申請人	主管	承辦人	主管	承辦人員	主管

限閱文件

個人資料蒐集、電腦處理、國際傳遞及利用同意書　範本

紀錄編號：_____

立同意書人（以下稱本人）與本校約定，關於蒐集、電腦處理、國際傳遞及利用本人資料之相關事宜，本人同意下列各條款：

一、合於本校依「個人資料保護法」教育主管機關法令規範或學則等規定之特定目的、資料類別、資料範圍、資料保有期限、資料利用範圍及其他相關事項範圍內，本校得蒐集、電腦處理、國際傳遞及利用本人之個人資料及本人與教育主管機構間之全部資料。

二、本校得將前條資料提供於本校業務相關單位或經主管機關同意之機構，並由上述各機構蒐集、電腦處理、國際傳遞及利用該資料。

三、前條所列各單位依教育行政法規或章程所定業務需要等特定目的，得蒐集、電腦處理、國際傳遞及利用本人之個人資料及本人與教育主管機構間之全部資料，並得將該資料提供於本校、由本校蒐集、電腦處理、國際傳遞及利用該資料。

立同意書人：　　簽章

身分證統一編號：

地址：

此致

耕莘健康管理專科學校

中　　華　　民　　國　　年　　月　　日

限閱文件

保密切結書

紀錄編號：_____

身份別　　□本校教職員工（含專案助理）□委外廠商

具保密切結同意人，因業務之執行而知悉校方機密或任何不公開之文書、電子資料、圖畫、消息、物品或其他資訊，將恪遵保密規定。未經合法書面授權，絕不以任何形式利用或擅自洩漏、告知、交付、移轉、傳播職務上任何業務相關資料及所有須保密訊息資料予任何第三人；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，違者願負法律責任。

此致

耕莘健康管理專校

具切結書同意人：（簽章）

身分證字號/護照號碼（人員）：_____

代表人（委外廠商）：_____

統一編號：_____

電話：(　)_____

地址：_____

中　　華　　民　　國　　年　　月　　日

資訊安全事件通報單

日期：年　月　日

通報單位聯絡資料			
單位名稱		通報人	
電話		電子郵件	

資訊安全事件通報事項	
發生時間	年　月　日　時　分
設備資料	IP 位址（無；可免填）： Web 位址（無；可免填）： 設備廠牌、機型： 作業系統名稱、版本： 已裝置之安全機制：

資訊安全事件資料	
事件影響等級	□4 級□3 級□2 級□1 級
事件分類	□非法入侵□感染病毒□阻斷服務□個資外洩□其他
破壞程度	□系統當機□資料庫毀損□網頁遭篡改□隱私權侵害□其他
事件說明	
可能影響範圍及損失評估	
應變措施	
期望支援項目	
解決辦法	
解決時間	年_月_日_時_分

權責（事件）單位		會辦單位	資圖中心	
承辦人	單位主管		資安承辦人	主管

資安及個人資料保護檢核表

紀錄編號：_____　填表日期：　年　月　日

查核項目	檢查結果		
	是	否	不適用
個人資料保護與安全			
1.1 個人資料之處理行為是否經權責單位核准，釐定使用範圍及調閱、存取權限？	☐	☐	☐
1.2 個人資料之處理行為是否留存使用者身分與其行為紀錄以供事後稽查？	☐	☐	☐
1.3 含有個人資料之紙本報表，其處理及利用行為是否有適當之授權、監督，及記錄列印、轉交等行為？	☐	☐	☐
1.4 交換紙本個人資料時，是否採取彌封或其他具備保密機制之傳遞方式？	☐	☐	☐
1.5 交換個人資料時，是否記錄轉交或傳輸行為之流向？	☐	☐	☐
1.6 對於個人資料之調閱，是否有申請及核准程序？	☐	☐	☐
1.7 對於個人資料之調閱，是否記錄並保存調閱者身分及行為？	☐	☐	☐
1.8 若需於單位管理之網站或網頁公佈個人資料時，是否經所屬單位主管核准，並依相關法律及規範處理？	☐	☐	☐
1.9 處理個人資料檔案之個人電腦，是否設置使用者代碼及通行碼？	☐	☐	☐
1.10 是否與他人共用電腦系統帳號？			
1.11 處理個人資料是否採取權限區隔，非專責處理特定個人資料者不得具有存取或查閱個人資料之權限？	☐	☐	☐
1.12 個人資料檔案是否予以加密？	☐	☐	☐
1.13 是否至少每月備份電腦內個人資料檔案？	☐	☐	☐
1.14 個人資料檔案使用完畢後，是否立即退出應用程式？	☐	☐	☐
1.15 交換個人資料檔案時，是否對資料檔案加密，或是透過加密通道傳送？	☐	☐	☐
1.16 是否禁止使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案？	☐	☐	☐
1.17 是否將存放敏感性個人檔案資料的電腦與外部網路隔絕（如：防火牆）？	☐	☐	☐

查核項目	檢查結果		
	是	否	不適用
2 設備管理			
2.1 是否指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息？	☐	☐	☐
2.2 儲存個人資料之資訊設備是否置放於實體安全區域(如：門禁控管之辦公區域、機房）？	☐	☐	☐
2.3 儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，是否置於實體保護之環境？	☐	☐	☐
2.4 儲存個人資料檔案之媒體是否有攜出、拷貝或複製的管控機制，並留存紀錄？	☐	☐	☐
2.5 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用，是否刪除其所儲存之個人資料檔案？	☐	☐	☐
3 人員管理			
3.1 機關學校是否對處理個人資料檔案之人員施予資訊安全與個資隱私保護之教育訓練，並定期於單位內宣導個資隱私保護之重要性？	☐	☐	☐
3.2 處理個人資料檔案之人員職務異動時，是否依規定列冊移交相關儲存媒體及資料？	☐	☐	☐
3.3 處理個人資料檔案之人員職務異動時，接替人員是否於相關系統重置通行碼，並視需要更換使用者識別帳號？	☐	☐	☐
3.4 處理個人資料檔案之人員，是否簽訂保密切結書？	☐	☐	☐
3.5 處理個人資料檔案之人員離職或合約終止時時，是否依規定取消或停用其使用者識別帳號並收繳通行證件？	☐	☐	☐
4 系統開發及委外管理			
4.1 處理個人資料檔案之資訊系統，是否在將個人資料檔案的安全需求納入系統開發考量（如：邏輯測試）？	☐	☐	☐
4.2 處理個人資料檔案的資訊系統之維護、更新、上線、及版本異動等作業，是否有安全管控措施？	☐	☐	☐
4.3 維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作時，是否透過加密通道進行（如：**HTTPS**、**SSH**等）？	☐	☐	☐
4.4 處理個人資料檔案資訊系統之開發，是否避免以真實個人資料進行測試？如需使用，是否於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？	☐	☐	☐
4.5 委外建檔的個人資料檔案，是否於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則？	☐	☐	☐

單位：_____職稱：_____資安及個資聯絡人：_____(簽章)

個人資料銷毀申請表

日期： 年 月 日

申 請 單 位		申 請 人	
電子郵件			
個人資料檔案名稱			
個資內容／目的簡述			
銷毀原因			
銷毀範圍	□全部檔案 □部份檔案＿＿＿＿＿＿＿＿＿＿		
銷毀方式			
銷毀時間	年 月 日 時 分		
申請人	承辦人	單位主管	

個人資料新增報告書

日期

單　　位				填寫人			
電子郵件				分機號碼			
檔案名稱	保有依據	特定目的	個人資料類別	個人資料之範圍	有否特種資料？何種特種資料？	有無監督管理之非公務機關及其名稱	個資使用方式
							□直接蒐集 □間接蒐集 來源：_____ □處理 □利用 □國際傳輸
							□直接蒐集 □間接蒐集 來源：_____ □處理 □利用 □國際傳輸
							□直接蒐集 □間接蒐集 來源：_____ □處理 □利用 □國際傳輸

承辦人 _____　個資專責人員_____　單位主管_____