馬偕學校財團法人馬偕醫護管理專科學校

110 學年度第 1 學期資訊安全暨個人資料保護推行委員會第 1 次會議紀錄

壹、時間：110 年 10 月 26 日星期二 09:00

貳、地點：關渡校區第二會議室(603 室)

參、出席人員：校長(陳裕仁)、教務主任(黃瑞吉)、秘書室主任(張讚昌)、學生事務主任(顏政通)、總務主任(李靜慧)、技術合作處主任(李信成)、圖書資訊處主任兼人工智慧暨醫療應用科主任(陳秀玲)、育成中心主任(李晢晃)、人事室主任(詹婉卿)、會計主任(黃惠瑩)、校牧室主任(湯玉芳)、軍訓室主任(陳春梅)、跨領育教育中心主任(呂漢軍)、餐飲管理科主任(楊啟良)、應用外語科主任(林美瑩)、化妝品應用與管理科主任(張靜雯)、視光學科主任(劉祥瑞)、資安專長諮詢委員(陳秀玲)

列席人員：

主席：陳裕仁資安長　　紀錄：陳永瑞

請假：校牧室主任(湯玉芳)、護理科主任(邱文璽)、餐飲管理科主任(楊啟良)、幼兒保育科主任(周佩諭)、生命關懷事業科主任(林龍溢)

肆、開會祈禱：

伍、確認上次會議紀錄：請參閱附件資料。

陸、議案追蹤或追蹤事項：

柒、報告事項：

一、「110 年度資訊安全暨個人資料保護教育研習營」，已於 110 年 06 月 11 日下午 13:00-16:00 辦理一般人員講習，110 年 07 月 12 日下午 13:00-16:00 辦理各級主管場次。

二、教育部 110 年度學術與部屬機關(構)分組資通安全通報演練已於 110 年 9 月 6 日 10 點 14 分接到通知，10 點 23 分填報完成。

三、有效性量測表與績效回饋統計表，如附件一。

四、110 年 09 月 2 日~110 年 09 月 3 日執行資訊安全內部擴大稽核，共開出 5 個不符合事項及 10 個觀察事項，報告如附件二。

五、依自我評鑑風險評鑑結果評估電算中心目前可接受風險水平值為 63，查看風險改善計畫軟體類 4 件、資料類 4 件，共計 8 件，已完成風險改善計 5 件，餘 3 件將於 111 年 07 月 31 日改善完成，如附件三。

六、自 109 年 11 月 24 日~110 年 10 月 25 日共計發生 7 起資安事件，如附件四。

七、ISMS 程序書及表單修改審定，詳請參閱附件五至附件十一。

修訂對照表:

現行條文	修正條文	說明
附件五 ISMS-P-232-002 存取通信與作業管理程序書 (1) 5.5.4.2　防火牆設定異動時，應填寫「防火牆進出規則申請表」，經主管簽准後，交由網路管理人員設定。	**附件五 ISMS-P-232-002 存取通信與作業管理程序書** (1) 5.5.4.2　防火牆設定異動時，應填寫「防火牆進出規則申請表」或電算中心服務申請單，經主管簽准後，交由網路管理	(1)防火牆異動設定填寫表單

現行條文	修正條文	說明
(2) **5.7.7** 系統負責人應於每日上班時依「系統與網路檢查紀錄表」所列項目，檢查各主機狀況，以確保系統正常運作。	人員設定。 (2) 5.7.7 系統負責人應於每週工作日選擇兩天上班時依「系統與網路檢查紀錄表」所列項目，檢查各主機狀況，以確保系統正常運作。	(2)系統巡查週期
附件六 **ISMS-P-232-037** **系統與網路檢查紀錄表**	附件六 **ISMS-P-232-037** **系統與網路檢查紀錄表** 系統與網路檢查紀錄表，增列核心系統項目，移除路由器(ROUTER)項目	變更檢查項目
附件七 **ISMS-P-232-038** **防火牆進出規則申請表**	附件七 **ISMS-P-232-038** **防火牆進出規則申請表** 更改有效期限為兩年	更改有效期限
附件八 **ISMS-W-232-003** **系統開發與維護程序書** **5.4.2 變更作業之控制流程：** 5.4.2.1 在實際執行變更作業前，申請者應先填具「系統開發需求申請單」或「電算中心服務申請單」或「系統功能修改申請單」提出變更需求，並經權責主管人員核准確認。 5.4.2.2 變更作業如有需要，應會辦相關人員配合。 5.4.2.3 上線前應先進行測試，必要時請相關人員配合建置測試環境。 5.4.2.4 除非事先經由權責主管人員核准外，測試不應在線上營運系統執行。 5.4.2.5 測試完成後，申請者應擬定「系統上線及緊急復原計畫表」，決定上線日期，經權責主管人員確認後始得上線。 5.4.2.6 上線後應立即於線上營運系統再行測試，以確認系統運作正常。測試人員不宜與程式開發者為同一人，以減少錯誤機會發生。 5.4.2.7 上線後測試如發現狀況，應嘗試可否立即排除，如無法立即排除，應依「系統	附件八 **ISMS-W-232-003** **系統開發與維護程序書** **5.4.2 變更作業之控制流程：** 5.4.2.1 在實際執行變更作業前，申請者應先填具「系統開發需求申請單」、「電算中心服務申請單」、「系統功能修改申請單」或其他申請紀錄，提出變更需求，並經權責主管人員核准確認。 5.4.2.2 變更作業如有需要，應會辦相關人員配合。 5.4.2.3 上線前應視資源進行測試，必要時請相關人員配合建置測試環境。 5.4.2.4 除非事先經由權責主管人員核准外，測試不應在線上營運系統執行。 5.4.2.5 測試完成後，申請者應視情形擬定「系統上線及緊急復原計畫表」或有相關緊急復原程序，經權責主管人員確認後始得上線。 5.4.2.6 上線後應立即於線上營運系統再行測試，以確認系統運作正常。測試人員不宜與程式開發者為同一人，以減少錯誤機會發生。 5.4.2.7 上線後測試如發現	調整開發及維護程序

現行條文	修正條文	說明
上線及緊急復原計畫表」，回復上線前原狀。 5.4.2.8　變更作業完成後應修改相關系統設計與功能規格書。	狀況，應嘗試可否立即排除，如無法立即排除，應依「系統上線及緊急復原計畫表」，回復上線前原狀。 5.4.2.8　變更作業完成後應修改相關系統設計與功能規格書。	
附件九 **ISMS-F-232-026** **業務流程衝擊分析表**	附件九 **ISMS-F-232-026** **業務流程衝擊分析表** 依擴大導入與驗證範圍修改業務衝擊營運分析表	配合擴大導入與驗證範圍，修改業務內容
附件十 **ISMS-F-232-028** **資訊安全管理制度內部稽核計畫** 本中心施作範圍內之相關資訊業務。 (本校 ISO/IEC 27001 驗證範圍涵蓋：電子計算機中心機房與辦公室等場域實體環境管理作業。)	附件十 **ISMS-F-232-028** **資訊安全管理制度內部稽核計畫** 本中心 ISMS 導入與施作範圍內之相關資訊業務。 (本校 ISO/IEC 27001 驗證範圍涵蓋：電子計算機中心機房與辦公室等場域實體環境管理及 5 個核心系統：教學務系統、人總會系統、TronClass 系統、單一入口驗證網(SSO)及 AD 主機之開發、維運或維護變更流程暨支援其之網路服務。)	配合擴大導入與驗證範圍，修改稽核範圍
附件十一 **ISMS-W-232-004** **資訊安全適用性聲明書**	附件十一 **ISMS-W-232-004** **資訊安全適用性聲明書** 擴大導入與驗證範圍修改範圍，及 A.9.4.5、A.12.1.4、A.14.2.1 ～ 9 、 A.14.3.1 、A.18.1.5 適用性更改為適用	配合擴大導入與驗證範圍，修改範圍及適用聲明

八、今年外部事件：

(1). 國發基金系統遭中國駭客入侵，通報為三級資安事件

(2). 宏碁印度分公司遭駭數日，駭客宣稱竊得臺灣總部的員工資料。

(3). 網路釣魚攻擊威脅增加，透過應用程式騙取用戶大型網站帳號的存取權限

九、109 年 11 月 24 日至 110 年 10 月 25 日，本校「當事人個人資料申請表」，申請案件為 0 件。

十、資訊安全管理制度內外部議題之改變：

(1). 內部議題：配合政治大學區域網路中心管理會第 84 次會議報告事項一各級學校網站應導入 HTTPS，本校已導入中華電信萬用憑證進行官網、教學務系統及人總會系統等網站 HTTPS 加密，並於 110 年 7 月完成憑證之更新。

(2). 外部議題：依據 110/09/08 教育部來函，鑒於學校使用雲端資通服務(如：Google 表單等) 蒐集個人資料時，可能因設定不當而增加個資外洩及資安

風險，請各校使用資通系統或雲端資通服務蒐集教職員、學生及家長個人資料者，應注意蒐集及使用個人資料之「最小化」為原則以降低風險，並請各單位主管加強宣導並督導。

十一、 關注方之回饋：業務永續運作計畫演練已於 109 年 12 月 19 日、110 年 08 月 03 日完成演練，並依資安顧問建議，配合擴大 ISMS 導入與驗證範圍，加入教學務系統統 WEB 虛擬機還原演練，如附件十二、附件十三。

十二、 持續改善之機會：配合教育部「110 學年度第 1 次臺灣學術網路防範惡意電子郵件社交工程演練」，於 110 年 4 月 9 日提供本校教職員生 Email 相關資訊予教育部資訊及科技教育司；並依 110 年 8 月 25 日教育部提供之演練結果函至有關單位進行改善與宣導(創稿文號：1101294912)附件十四。

十三、 ISO/IEC 27001 續審暨擴大範圍驗證預訂於 110 年 10 月 27、28 日舉行，共計 2.5 人天外部稽核。

捌、議案討論：由資安長宣達配合填寫防火牆政策相關申請表單

說明：配合 ISO 27001 資安規範，需由資安長於資安相關會議上宣達。

決議：資安長已於會議中宣達。

玖、臨時動議：紙本個資銷毀，可考量三芝校區方便處理。

說明：每年暑假一次，可增加次數或校區以方便銷毀。

決議：需再討論連絡廠商和尋找合適場地配合。

拾、閉會祈禱：

拾壹、散會

紀錄：　　執行秘書：

校長：