

馬偕學校財團法人馬偕醫護管理專科學校

109 學年度第 2 學期資訊安全暨個人資料保護推行委員會第 1 次會議議程

壹、時間：110 年 6 月 1 日星期二 10:00

貳、地點：關渡校區第二會議室(603 室)

參、出席人員：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(呂建陳)、圖書資訊處主任(呂漢軍)、育成中心主任(陳觀彬)、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)、通識教育中心主任(李信成)、護理科主任(邱文璽)、幼兒保育科主任(周佩諭)、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)、高齡服務事業科主任(施秋蘭)、視光學科主任(劉祥瑞)、生命關懷事業科主任(林龍溢)、資安專長諮詢委員(陳秀玲)

列席人員：電子計算機中心技佐(周建名)

主席：陳裕仁校長(資安長)

執行秘書：呂漢軍主任

紀錄：陳秀玲

主任

請假：

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、本校依教育部所屬機關(構)及學校資通安全責任等級分級作業規定，隸屬於 C 級機關，5 月行政會議已通過行政會議，委員會成員加入校長並修改本校資訊安全長為校長。

二、自 109 年 10 月 29 日-110 年 05 月 06 日，本校「當事人個人資料申請表」，申請案件為 0 件。

三、自 109 年 10 月 29 日-110 年 04 月 30 日共計發生 5 起資安事件，如下所示。

事件單編號	事件說明	事件處理結果	確認為資安事件時間	通報完成時間
188707	自行通報 學生個人網路硬碟遭到入侵造成 放置於技合處伺服器被攻擊	將可疑設備網路斷開並格式化重灌， 並關閉網路芳鄰	2020-12-21 09:43:57	2020-12-23 09:54:37
191156	教育部資安事件 通告-馬偕醫護管理專科學校 [210.71.79.107] 主機疑似進行挖礦程式連線	已中斷網路連線，待處理 完成後再上線	2021-04-06 09:50:06	2021-04-06 09:55:32
191578	教育部資安事件 通告-馬偕醫護管理專科學校	已將個人電腦斷網並施行 網路封鎖和	2021-04-19 11:00:49	2021-04-19 11:04:44

	[210.71.79.107] 主機疑似進行挖 礦程式連線	重灌		
事件單編號	事件說明	事件處理結果	確認為 資安事件時間	通報完成時間
191588	自行通報 電腦中殭屍病毒	停止該 ip 的 運作，並阻 斷目的 ip	2021-04-19 10:01:51	2021-04-19 10:01:51
191805	教育部資安通告- 馬偕醫護管理專 科學校 [210.71.79.107] 主機疑似進行挖 礦程式連線	斷該設備	2021-04-26 10:07:18	2021-04-26 10:10:19

- 四、教育部將於 110 年 4 月至 11 月期間進行防範惡意電子郵件社交工程演練計畫，請轉達提醒同仁勿使用校園電子郵件信箱開啟來路不明之電子郵件、連結及檔案。
- 五、本年度 ISO 27001 將校園核心系統納入資訊安全認證範圍，包含「人總會系統」、「教學務系統」、「SSO 單一入口驗證網」、「TronClass 系統」、「AD 系統」，如系統有簽定年度維護合約或系統增修合約時請承辦單位注意需加入「資訊安全責任條款」。(請參閱附件一)
- 六、因應項四，電算中心安排於暑假期間請中華電信資安團隊對「教學務系統」、「人總會系統」、「SSO 單一入口驗證網」進行滲透測試，將到校進行，進行的工作日數將視實際作業進行，如於上述期間系統有任何使用問題，請與電算中心聯絡。
- 七、「110 年度資訊安全暨個人資料保護教育研習營」，預計於 110 年 6 月 11 日(五)下午 13:00-16:00 辦理一般人員講習，將採 Team 線上研討會方式進行，110 年 07 月 12 日(一)下午 13:00-16:00 辦理各級主管場次(視疫情決定會議方式為實體或線上，將於一週前公告)。
- 八、本年度業務永續演練計畫擬訂於 110 年 08 月 15 日前完成演練，議題為「教學務系統虛擬機備份還原測試」。
- 九、本年度資訊安全內部稽核擬訂於 110 年 09 月 02、03 日舉行。
- 十、資安宣導：
1. 資安議題討論-內部議題：
 - (1)先傑報修系統，因應資訊安全需求，登入密碼將請先傑協助修改為強密碼。
 - (2)請各單位承辦人員注意報修時不得上傳相關個資資訊，及機敏性資料。
 - (3)請善用檔案加密功能傳輸。
 2. 資安議題討論-外部議題：

為降低機敏資料遭不當竊取之風險，致校職員生個人資料外洩，使用資通訊產品(含軟體、硬體及服務)時，應配合行政院「各機關對危害國家資通安全產品限制使用原則」辦理，並儘量避免使用大陸廠牌。

捌、議案討論

玖、臨時動議：

拾、閉會祈禱：

拾壹、散會

<附件一>

各單位如有簽辦或會辦**資通訊服務類**之專案，請檢視其契約是否含有下列「資訊安全責任」之相關內容載明或條款，若未包括者，請視專案需要，加入下列條文或需求：

X、資訊安全責任：

- (一) 廠商應遵守政府所頒訂之各項資訊安全規範及標準，並遵守本校各項資訊安全管理及保密等相關規定，且本校保有對廠商執行稽核之權利。
- (二) 廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。
- (三) 契約履約或終止後，廠商應刪除或銷毀執行服務所持有本校之相關資料，或依據本校之指示返還之，並保留執行紀錄。
- (四) 廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。
- (五) 廠商提供服務，如發生資安事件時，必須通報本校，提出緊急應變處置，並配合本校進行後續處理。
- (六) 廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合本校對系統品質及資訊安全的要求。
- (七) 履約期間廠商須配合行政院「各機關對危害國家資通安全產品限制使用原則」等資通安全管理相關規範，若本專案產品屬公告之禁用項目，則須無償更換為符合前述原則規定且滿足本校業務需求之軟體、系統及設備等，以避免潛在之資訊安全風險。
- (八) 廠商如違反前述規定，應就本校所受損害負賠償之責；如致他人權利受有損害時，廠商亦應負責。