唯心聖教學院

113 學年度第一學期第 1 次資訊管理發展委員會會議紀錄

承辦單位：校務發展處圖書資訊組

日　　期：中華民國 113 年 11 月 22 日(五)

地　　點：唯心聖教學院教育行政大樓一樓會議室

唯心聖教學院

資訊管理發展委員會會議記錄

時　　間：民國 113 年 11 月 22 日(星期五)
地　　點：唯心聖教學院教育行政大樓一樓會議室
主　　席：石國慶處長
出席人員：李珍玫副校長（兼行政處長暨代理會計主任)、朱克剛教授、偉晟科技有限公司董事長林榮隆董事長、偉晟科技有限公司林瑋恩、校務發展處圖書資訊組組員顏鈺珊、校務發展處圖書資訊組助理蕭丞廷。
請　　假：唯心聖教應用易經研究所所長洪瑞良所長、陳佳伶律師
紀　　錄：顏鈺珊賢士

壹、 主席致詞

一、今天麻煩朱老師和林董事長審視本校網路硬體、軟體設備。
二、目前官網請廠商重新開發，近期準備上新官網，目前遇到資安相關問題，所以今天請兩位專家給予專業的建議，告知是否有不足或尚須加強部分。

貳、報告事項

參、討論事項

提 案 一：有關新舊官網資訊安全議題，請討論。
說　　明：
一、 舊官網網頁常發現故障。
二、 新官網網頁手機版網址被轉址。
三、 新官網負責廠商-春先生創意設計有限公司目前提供伺服器環境設定所需規格：
Ubuntu： 20.04 版本 或 22.04 版本
CPU：4 cores 以上
Memory：8G 以上
Disk：80 GB SSD 以上
apache 2.4 以上
php 8.1 以上
MySql 8.0 以上
附　　件：唯心聖教學院-網路與系統環境建議改善事項。
決　　議：

一、 有關今年 6 月官網遭轉址，主因為透過 Windows 上 XAMPP 的 php 進行漏洞攻擊，新官網的環境規格是 Ubuntu，可避免上述情事。

二、 本案請新官網廠商春先生於系統上線前完成弱點掃描，並交付掃描報告且完成程式更新與修補。

三、 本案未來應建立定期弱點掃描之資安評估報告，由校發處評估修補模式。

提 案 二：校外對內連線資安議題，請討論。

說　　明：目前學校師生與廠商由校外對內連線使用 anydesk。

決　　議：

有關校外對內連線之資安政策，可由校方建立使用規則，廠商須提出申請，始可開特定 ip 進行連線處理；此外，亦可參酌其他大學，使每個使用者皆採用固定 IP。

提 案 三：有關唯心聖教學院圖書館系統維護一案，請討論。

說　　明：

一、 該網頁常發生網頁故障之紅色頁面。

二、 113 年 10 月 1 日，第四屆多位新生借書，發現查無此人，經與承辦人確認之前已為第四屆新生建立系統帳號，後經查看僅剩一位新生資料在系統上。

決　　議：

有關圖書管理資訊系統維護事項

一、 請原購置廠商－寶慶文化科技股份有限公司確認系統 log 記錄。

二、 考慮圖書管理資訊系統重新開機之排程，以利網頁正常運行。

三、 可重新評估圖書管理資訊系統之系統學年度維護合約，以利系統正常維運。

提 案 四：有關本校 VPN 使用常異常事件，請討論。

說　　明：學校 VPN 使用常發生師生設定完後，隔一段時間無法正常使用，需再次重新設定。

決　　議：

有關本校 VPN 使用異常事件，解決方案：

一、 可購置等級較優之 VPN Server。

二、 可評估購置 Forti 防火牆含 VPN 功能，同時管控使用者連線。

唯心聖教學院
資訊管理發展委員會議簽到表

主　　席：校務發展處　石處長國慶

時　　間：民國 113 年 11 月 22 日(五)

地　　點：唯心聖教學院教育行政大樓一樓會議室

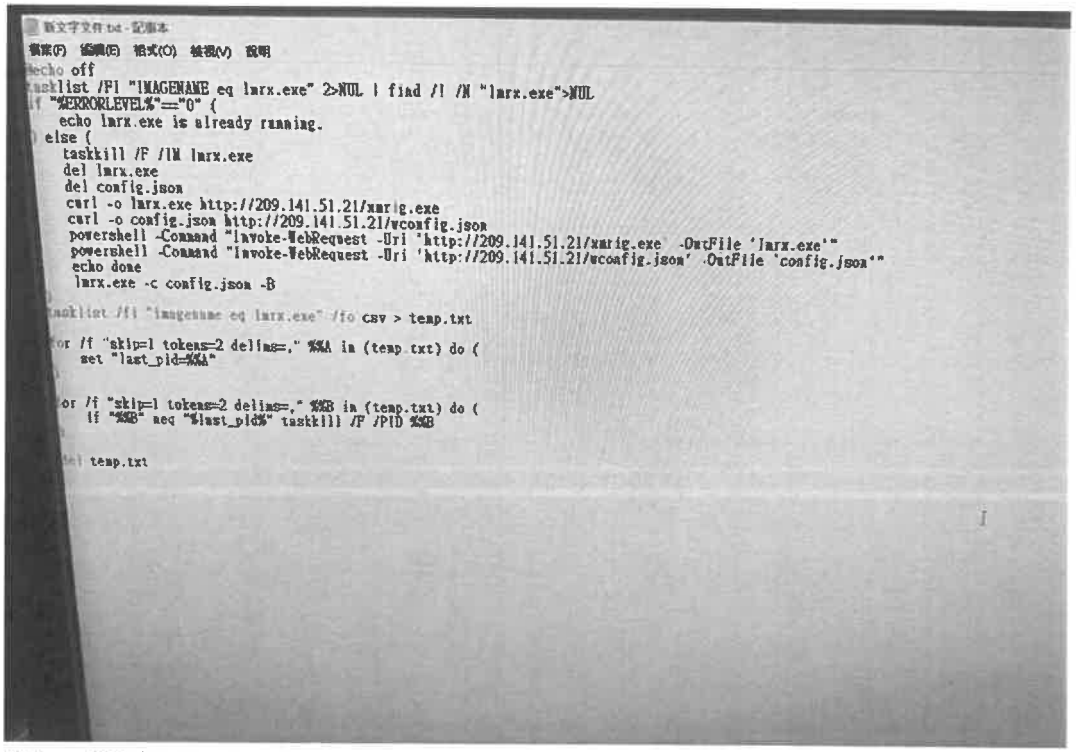
職稱	姓名	簽名
副校長 兼行政處處長	李珍玫	李珍玫
校務發展處處長	石國慶	石國慶
會計室主任	李珍玫(代)	李珍玫代
應用易經研究所所長	洪瑞良	**請假**
教授	朱克剛	朱克剛
律師代表	陳佳伶	**請假**
偉晟科技有限公司 董事長	林榮隆	林榮隆
偉晟科技有限公司	林瑋恩	林瑋恩
校務發展處圖書資訊組 組員	顏鈺珊	顏鈺珊
校務發展處圖書資訊組 助理	蕭丞廷	蕭丞廷

唯心聖教學院-

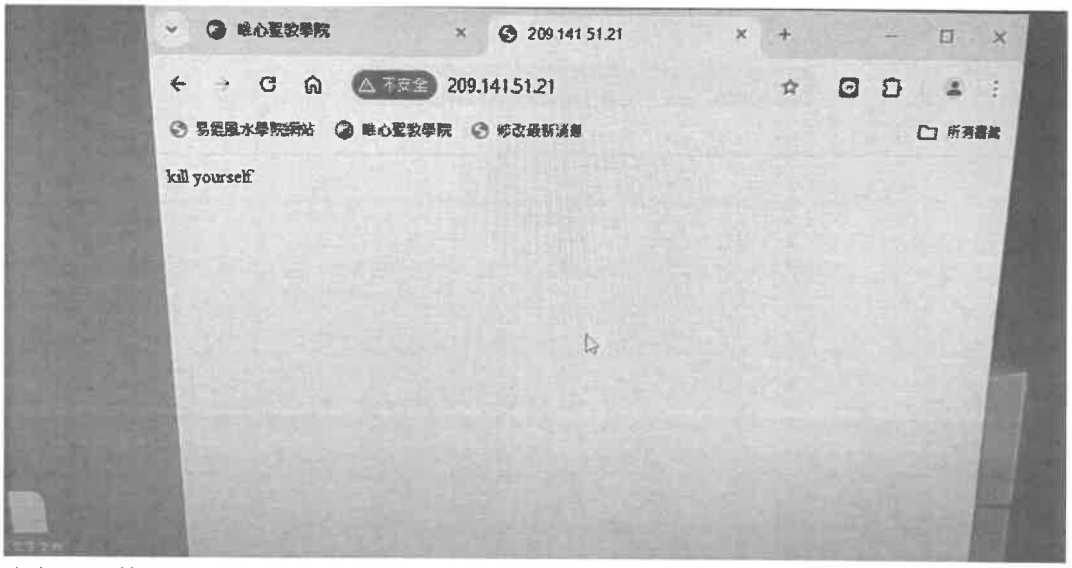
網路與系統環境建議改善事項

摘要：

近期學校首頁內容被置換(圖一)&(圖二)，基於目前學院網路與系統環境提供建議改善事項。



(圖一)首頁置換程式碼



(圖二)置換過後的首頁

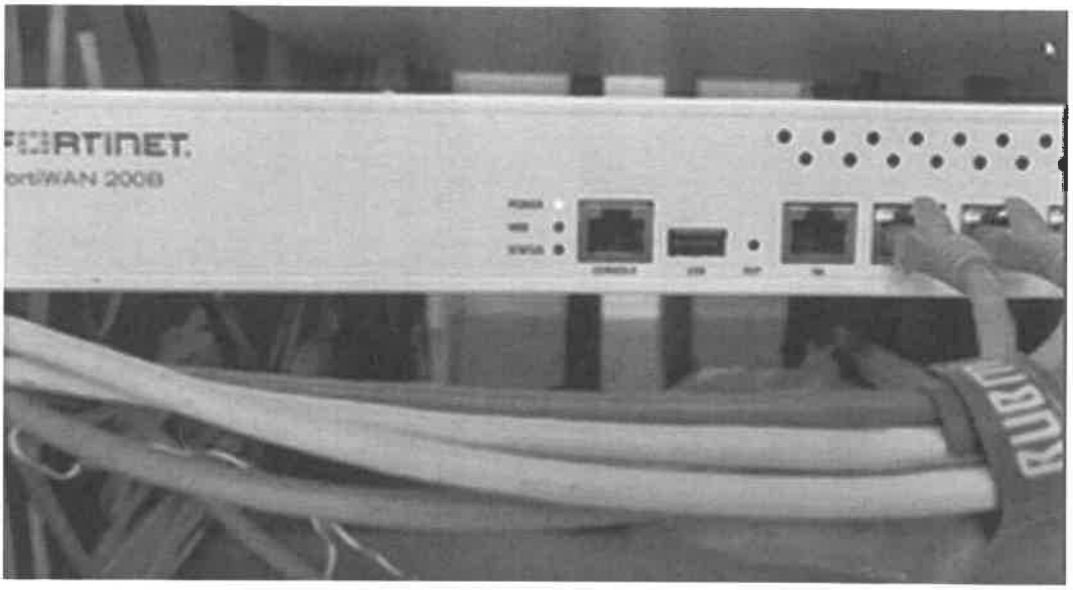
建議事項一(防火牆 Paloalto PA820 授權續約)：

機房防火牆 Paloalto PA820 Premium Partner 與 Threat Prevention 授權已過期，防火牆無法在執行系統與更新新型資安威脅的資料庫，建議續約防火牆授權。

↑ Paloalto PA820 授權到期

建議事項二(負載平衡器更換)：

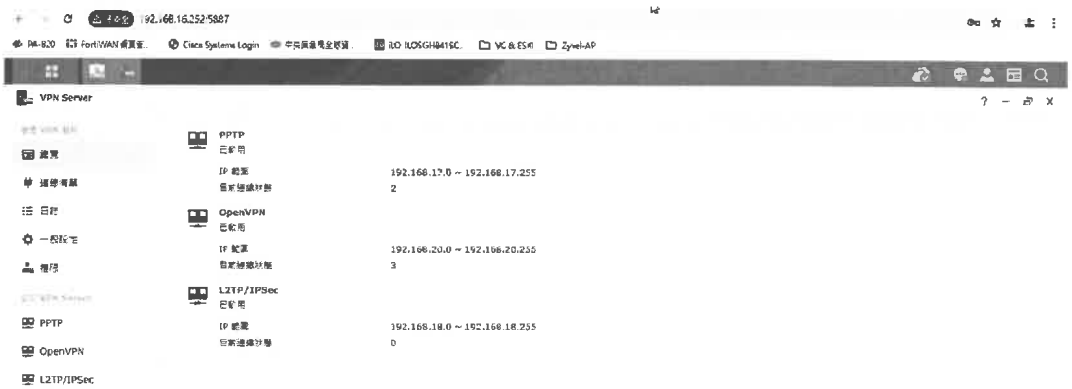
機房附載平衡器 FortiWAN 200B 因之前跳電導致設備故障，
此設備已過保且停產，目前使用本公司借貸 Fortigate 600D 暫時頂替使用，
此 Fortigate 600D 授權已過期，病毒資料庫與防火牆本身無法再做更新，
建議採購新型附載平衡器 FortiADC 或是防火牆 Fortigate 來使用。



↑機房 Fortiwan200B，目前已故障

建議事項三(VPN 控管)：

目前學院既有的 VPN 為 Synology NAS(檔案伺服器)所提供的附加功能，
當使用者連上 VPN 後形同直接使用學院內網可直接對內網設備連線，
目前學院使用者連線 VPN 主要目的為透過學院的 IP 去連線華藝線上圖書館以及 EBSCOhost 資料庫等網站，建議可使用 Fortigate 防火牆的 Forticlient VPN，Forticlient VPN 可以針對使用者設定防火牆政策，限制使用者對內網設備的連線降低因為 VPN 連線所產生的資安風險。



↑ Synology VPN

建議事項四(校首頁系統整機備份以及虛擬主機平台儲存空間擴充)：

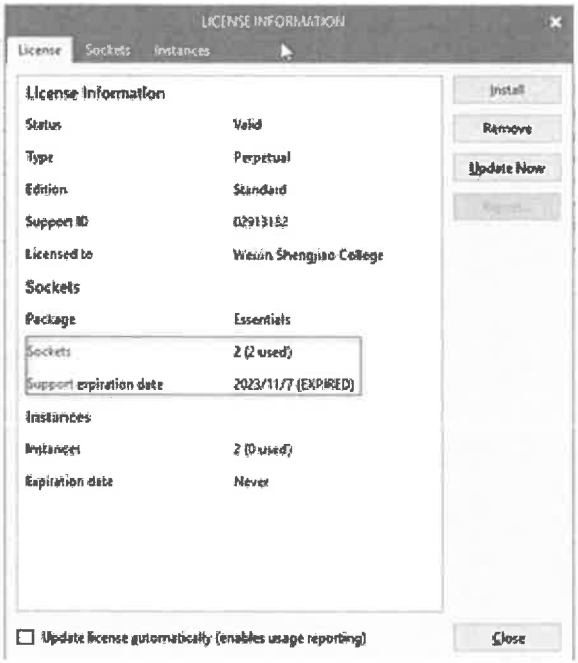
校首頁系統目前只有原廠商設定的網頁程式備份，
建議規劃將校首頁主機虛擬化轉移至學校的虛擬主機平台(Vmware)，
透過學校既有的備份軟體(Veeam)去做備份。
另外關於學校虛擬主機平台部分，目前學校的兩台虛擬主機平台可使用空間各為 550GB(圖一)與 388GB(圖二)，建議學校可另購儲存設備(Storage)去擴充以及整合學校系統的儲存空間，讓學校的兩個虛擬主機平台可使用共用儲存空間來做到容錯轉移(A 主機因意外或是未知原因而被關機時自動由 B 主機接手)。

↑(圖一)虛擬主機平台一，儲存空間剩餘 550GB

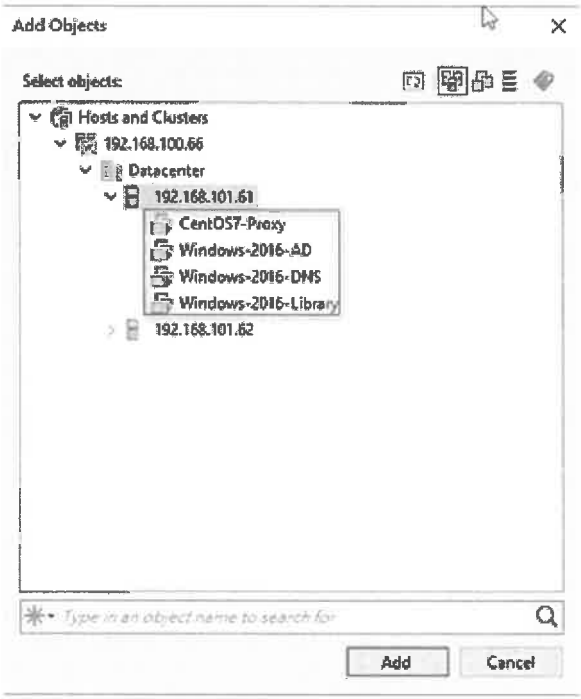
↑(圖二)虛擬主機平台一，儲存空間剩餘 388GB

建議事項五(系統備份軟體(Veeam)授權更新 Or 新購授權)：

學校目前系統備份軟體(Veeam)所購買的授權已過期(圖一)且授權數為 2 Socket(一台實體主機)，無法對校內所有系統執行整機備份(圖二)，建議更新 Veeam 授權且擴充授權數來備份學校重要系統。



↑(圖一)Veeam 軟體授權



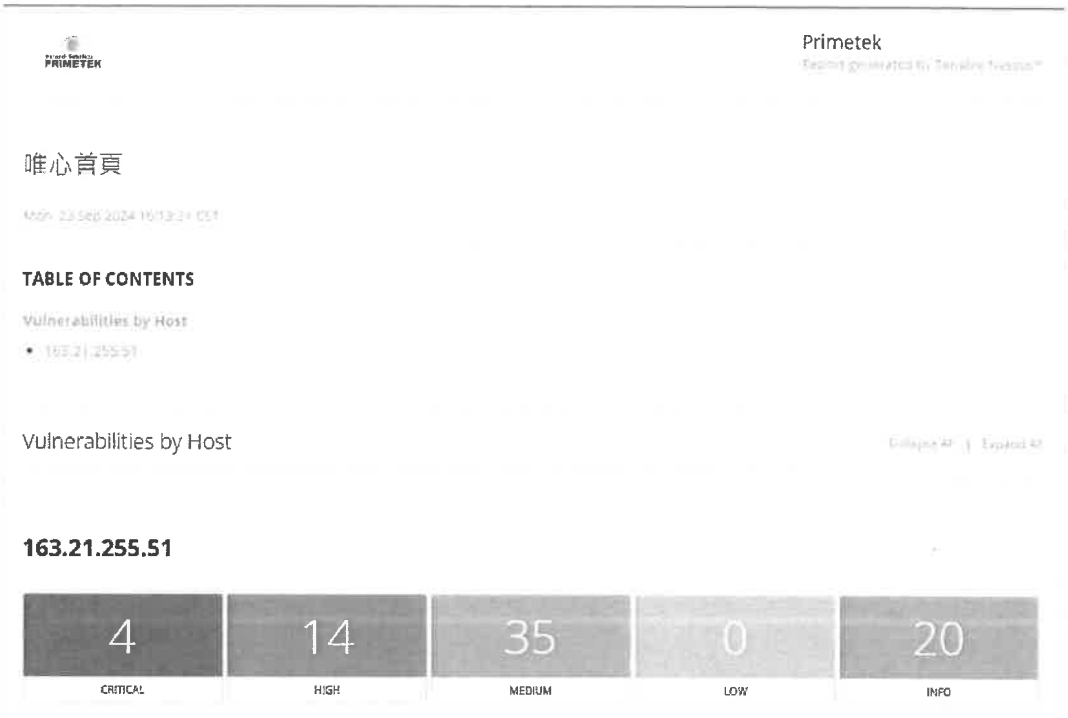
↑(圖二)Veeam 目前可備份系統

建議事項六(重要系統弱點掃描)：

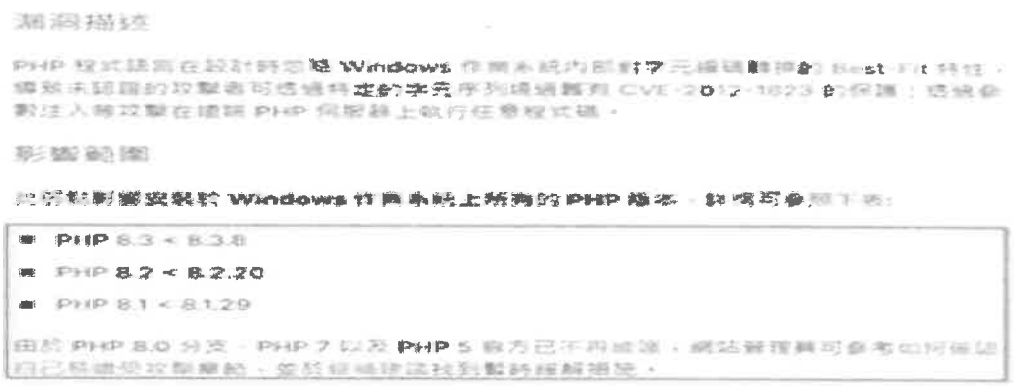
今日檢視學校首頁系統主機發現首頁主機的網頁伺服器主控台 xampp 在資安漏洞 CVE-2024-4577 的影響範圍，詳細內容請參考 https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/ 。

透過本公司弱點掃描主機掃描確認校首頁主機含有 4 項嚴重風險弱點與 14 項高風險弱點與 35 項中風險弱點(圖一)，根據 CVE-2024-4577 說明文件，若網頁 PHP 版本在 8.3<8.3.8、8.2<8.2.20、8.1<8.1.29 以及低於 8.1 的話就會受此風險影響(圖二)。

目前檢測校首頁主機版本為 PHP 7.1.11(圖三)處於系統漏洞影響範圍中，建議廠商根據系統漏洞說明報告修補相關漏洞(圖四)



↑(圖一)校首頁主機弱點掃描結果



↑(圖二)網頁系統漏洞影響範圍

(圖三)校首頁 PHP 版本

情境一: 將 PHP 設定於 CGI 模式下執行

```
AddHandler cgi-script .php
Action cgi-script "/cgi-bin/php-cgi.exe"
```

或

```
<FilesMatch "\.(?:php|php3|php4|php5|php7|php8|phtml)$">
    SetHandler application/x-httpd-php-cgi
</FilesMatch>

Action application/x-httpd-php-cgi "/cgi-bin/php-cgi.exe"
```

情境二: 將 PHP 執行檔暴露在外 (XAMPP 預設安裝設定)

即使未設定 PHP 於 CGI 模式下執行，僅將 PHP 執行檔暴露在 CGI 目錄下也會此漏洞成立，常見情況包含但不限於：

1. 將 php.exe 或 php-cgi.exe 複製到 /cgi-bin/ 目錄中
2. 將 PHP 安裝目錄透過 ScriptAlias 暴露出來，如：

```
ScriptAlias /php-cgi/ "C:/xampp/php/"
```

解決方案

漏洞中的邏輯性錯誤機制，實際上的運作原理已經很明顯了，要如何修補：

```
RewriteEngine On
RewriteCond %{QUERY_STRING} ^%[a-f] [NC]
RewriteRule .? - [F,L]
```

2. 對 XAMPP for Windows 使用者

在撰寫本文的當下，XAMPP 尚未針對此漏洞發出修補程式的更新安裝檔，如確認自己的 XAMPP 並未使用到 PHP CGI 之功能，可透過修改下列 Apache Httpd 設定檔以避免暴露在弱點中：

> C:/xampp/apache/conf/extra/httpd-xampp.conf

找到相關的設定行數：

```
ScriptAlias /php-cgi/ "C:/xampp/php/"
```

並將其註解：

```
# ScriptAlias /php-cgi/ "C:/xampp/php/"
```

漏洞回報時間軸

↑(圖四)建議修補事項

提 案 五：為配合本校資訊安全制定，有關本校資安相關軟體續約情形，請討論。

說　　明：本校今年度尚未續

一、 paloalto PA-820 防火牆硬體

二、 paloalto PA-820 防火牆 IPS 入侵防禦資料庫

三、 Veeam Backup Essentials Standard 2 socket bundle

決　　議：

一、 原購置資安相關軟體續約事宜，廠商於到期前一個月會主動通知校方。

二、 目前學校使用的 PA-820 防火牆已停產，2025 年不再提供續約方案，目前機器仍具防護功能，但面對新病毒的防護無法再更新，須再另案評估。

肆、臨時動議

案 由 一：有關學生是否一定要透過 VPN 才可選課？

決　　議：

有關學生選課是否須透過 VPN 才可連線一案：

一、 選課系統可透過 Web，惟須轉換為公有 ip 外部才能連線。

二、 VPN 使用須考量短時間內密集性流量負荷問題，惟因學校現有人數不多尚不受影響。

伍、主席結論

一、 下次開會時間：113.12.1(日)上午 9:30。

二、 請廠商提供一個完整的簡報方案，針對本校機房給予軟體、設備相關採購、續約與授權的建議，並預估相關經費金額，以利校方進行後續評估。

陸、散會

承辦單位	會辦單位	核決
組員顏鈺珊 1219 1200 校務發展處處長石國慶 1226 1250 唯心生醫學院副校長李珍玉 0104 1450		唯心聖教學院校長陳立岳 0105 1. 此次會議之事項請儘速處理 1400 2. 確實要求合約廠商提供相關資訊 3. 校內設備盡量選課之設備以集思廣益