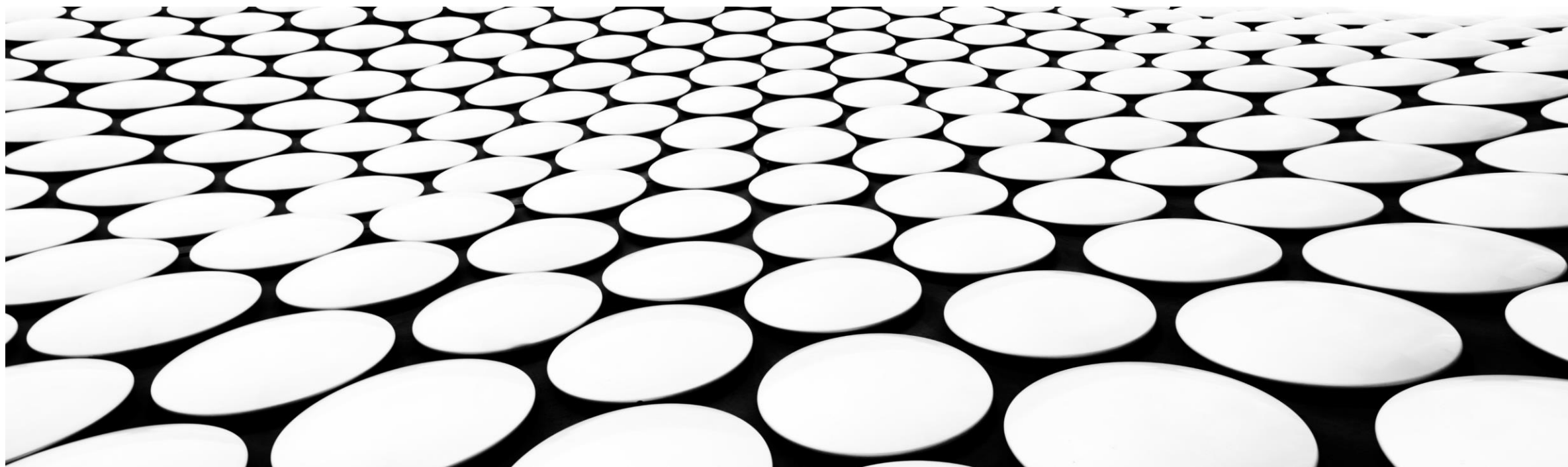


---

# 一般資訊設備與機房網通設備管理經驗分享

國立臺東高中技服組長 巫培爾



---

# 大綱

- 個人簡歷
- 資訊設備相關業務說明
- 機房規劃與維運

姓名	巫培爾	教職服務年資	20年
現職	國立臺東高級中學圖書館技服組長		
學歷	國立臺灣師範大學物理學系		
專長	物理教學 電腦硬體檢修 電腦系統維護 網通設備、伺服器機房規劃佈建與維運		
主要經歷	國立臺東高中物理科教師(92迄今) 國立臺東高中導師(92、94~96、97~99、101~102) 國立臺東高中設備組長(103) 國立臺東高中教務主任(104~105) 國立臺東高中圖書館技服組長(108迄今) 國教署資通安全輔導委員會委員(110迄今) 國教署資通安全輔導委員會地區輔導員(110迄今) 國教署數位學習推動辦公室資訊輔導團委員(112)		

Certificate 43203297 / 133797440

CQI / IRCA 71753

**PEI-ER WU**

**SGS**



has been awarded a Certificate of Achievement for  
**ISO/IEC 27001:2013 - Information Security  
Management Systems Auditor/Lead  
Auditor Training Course**

by passing the written examination and continuous assessment

Held at  
**Taipei, Taiwan**  
Completed on  
**3 November 2017**

This course meets the formal training requirements for individuals seeking certification under the IRCA Auditor Certification Scheme and for this purpose is valid for five years from the date of completion

Course Number 17279 - PR 320  
Certified by the International Register of Certificated Auditors (IRCA)



Jan Saunders  
UK Business Manager

Amanda Mangan  
Global Training Manager

Issued by SGS United Kingdom Ltd. Registered in England No 1193985  
Registered Office SGS United Kingdom Ltd. Rossmore Business Park  
Ellesmere Port, Cheshire, CH65 3EN  
SGS United Kingdom Ltd. Certification and Business Enhancement  
SGS House, 217-221 London Road, Camberley, Surrey, GU15 3EY  
t +44(0) 1276 697 777 f +44(0) 1276 697 696 [www.sgs.com](http://www.sgs.com)



Certification Number  
**ECC0156923874**



# Computer Hacking Forensic Investigator

This is to acknowledge that

**Peier Wu**

has successfully completed all requirements and criteria for  
**Computer Hacking Forensic Investigator**

certification through examination administered by EC-Council

Issue Date: **12 October, 2018**

Expiry Date: **11 October, 2021**



**EC-Council**

Sanjay Bavisli, President



# 資訊設備相關業務說明



# 資訊設備相關業務說明

- 資訊設備相關業務的歸屬？學校機房歸誰管？資安工作算誰的？
  - 教務處設備組？
  - 圖書館資媒組？
  - 圖書館技服組？
  - 其他?(如：職業學校資處科主任)

# 資訊設備相關業務說明

- 理想狀況
  - 設備組負責資訊設備採購與教師教學用資訊設備借用管理。  
(主因：多數經費併入教學設備中)
  - 資媒組或技服組負責資訊設備維護服務與機房網通設備維運與資安工作。(含維護服務廠商外包管理)
- 現實狀況：牽涉到經費支出來源與控管，很難分清楚。

# 資訊設備相關業務說明-盤點自身業務內容

## 設備組

- 數理實驗班計畫
- 教學設備採購與維護
- 資訊設備採購與維護
- 機房網通設備與網路維運
- 教科書、科展、能力競賽...等等等。

## 資媒組或技服組

- 圖書相關業務
- 自主學習計畫
- 資訊設備採購與維護
- 機房網通設備與網路維運
- 其他專案計畫



# 資訊設備相關業務說明-盤點可用經費

- 一般設備費
- 各處室業務費
- 計畫經費
- 實習實驗費
- 電腦使用費
- 網路通訊費(TANET、HINET)
- 資訊設備維護合約
- 機房維運合約(Firewall等)
- 全校防毒授權
- 資訊設備汰換(保固年限拉長)

# 資訊設備相關業務說明-善用可用資源

Hello! 技服組長 [登出](#)

**我要租借** 請從下方設備清單中選取想要租借的設備，並滑鼠點擊[租借]鈕，完成租借請求。

分類 [全部](#) 地點 [全部](#) 查詢

設備編號	設備名稱	保管人	類別	地點	租借
1-3140101-03-1732	Apple iPad	技服組長	平板電腦(含原廠充電頭、充電線、包包)	圖書館機房	<a href="#">租借</a>
1-60114-58	D-Link 4G USB行動網卡	技服組長	4G行動網卡(USB)(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-59	D-Link 4G USB行動網卡	技服組長	4G行動網卡(USB)(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-60	D-Link 4G USB行動網卡	技服組長	4G行動網卡(USB)(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-96	Zyxel LTE行動路由器	技服組長	4G無線分享器(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-97	Zyxel LTE行動路由器	技服組長	4G無線分享器(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-98	Zyxel LTE行動路由器	技服組長	4G無線分享器(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-99	Zyxel LTE行動路由器	技服組長	4G無線分享器(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-100	Zyxel LTE行動路由器	技服組長	4G無線分享器(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-101	Zyxel LTE行動路由器	技服組長	4G無線分享器(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-102	Zyxel LTE行動路由器	技服組長	4G無線分享器(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-103	Zyxel LTE行動路由器	技服組長	4G無線分享器(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-57	D-Link 4G USB行動網卡	技服組長	4G行動網卡(USB)(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-60114-56	D-Link 4G USB行動網卡	技服組長	4G行動網卡(USB)(含SIM卡)	圖書館機房	<a href="#">租借</a>
1-3140101-03-1733	Apple iPad	技服組長	平板電腦(含原廠充電頭、充電線、包包)	圖書館機房	<a href="#">租借</a>

[回首頁](#)

# 資訊設備相關業務說明-善用可用資源

Hello! 技服組長 [登出](#) 場地預約查詢

系統時間: 2023/8/30 23:50:18

各位同仁好，此為本校各專科教室及會議室預約使用系統。  
 教室類以各項即定課程優先使用；  
 各會議室以其管理單位有即定用途者優先使用；  
 校長會議室以會議性質為主，研習性質請優先使用其他場地。  
 以上基本原則煩請大家協助遵守與維護。

上一週 今天 下一週 時間: 2023/08/27 - 2023/09/02 地點: 自主學習教室1(監書報討論室(校長室樓上))

節次	時間	日 08/27	一 08/28	二 08/29	三 08/30	四 08/31	五 09/01	六 09/02
早自習	07:30   08:00	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)
第1節	08:00   09:00	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)
第2節	09:00   10:00	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)
第3節	10:00   11:00	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)
第4節	11:00   12:00	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)
午休	12:00   13:15	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)	自主學習教室4 監書報討論室(校長室樓上)
第5節	13:15   14:15	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)
第6節	14:15   15:15	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)	自主學習教室1 監書報討論室(校長室樓上)

Hello! 技服組長 [登出](#) 處理狀態 全部  查詢

[我要修繕回報](#)

填寫報修系統時，請務必選擇正確報修類別，否則可能通報至錯誤的單位或負責人。

教學設備：單槍、擴音系統、廣播系統、無線投影等教室內之教學相關設備。

資訊設備：電腦軟硬體及各項資訊週邊產品等。

其他設備：黑板、門窗、冷氣、電話系統、電風扇、水電等相關教室內固形資產與設備。

麻煩不同類型請分案報修，以利信件轉送通知！

編號	類別	地點	回報主旨	回報內容	填報日	填報人	維修進度	回應
3771	教學設備	自然科辦公室	<a href="#">黃千姿桌椅</a>	PPT有些檔案開不了，似乎新接收的PPT開不了，隨身碟的PPT就可以	2023-08-30 21:54:05	黃千姿	待處理	<a href="#">0</a>
3770	教學設備	304	<a href="#">麥市風扇有雜音</a>	如題，請協助處理，謝謝!	2023-08-30 18:02:33	簡宛儀	待處理	<a href="#">0</a>
3769	教學設備	304	<a href="#">投影機螢幕有橫線、閃爍</a>	如題，請協助修繕，謝謝!	2023-08-30 18:01:25	簡宛儀	待處理	<a href="#">0</a>
3768	資訊設備	綜合禮堂	<a href="#">單槍會不定時閃爍</a>	禮堂二樓單槍(投影機)接上電腦播放PPT後，會不定時閃爍(一次會暗個10秒左右，一分鐘也許會暗個2-3次)，煩請協助維修。	2023-08-30 17:21:42	訓育組長	待處理	<a href="#">0</a>
3767	資訊設備	英文科辦公室	<a href="#">6204</a>	6204電話不通	2023-08-30 15:14:39	陳熾羽	待處理	<a href="#">0</a>
3766	其他設備	教務處	<a href="#">設備組旁水龍頭會滴水</a>	設備組旁水龍頭會滴水	2023-08-30 14:39:29		待處理	<a href="#">0</a>
3765	其他設備	210	<a href="#">教室電話學生聽不見鈴聲</a>	教室電話學生聽不見鈴聲	2023-08-30 11:31:45	設備組幹事	待處理	<a href="#">0</a>
3764	其他設備	206	<a href="#">教室電話學生聽不見對方聲音</a>	教室電話學生聽不見對方聲音	2023-08-30 11:31:07	設備組幹事	待處理	<a href="#">0</a>
3763	其他設備	圖書館階梯教室	<a href="#">電話故障</a>	電話發出雜音，無法撥打。	2023-08-30 08:18:08	謝光明	待處理	<a href="#">0</a>
3762	資訊設備	英文科辦公室	<a href="#">無法列印，電腦尚未安裝設定辦公室印表機</a>	電腦尚未安裝設定英文科辦公室印表機	2023-08-29 12:52:44	劉俊偉	待處理	<a href="#">0</a>
3761	資訊設備	206	<a href="#">沒有網路，冷氣跳電無法使用</a>	8/28下午老師上重補修課程時 沒有網路、冷氣跳電，不知道是不是206教室有斷電或不供電?謝謝	2023-08-29 11:31:35	胡惠君	待處理	<a href="#">0</a>

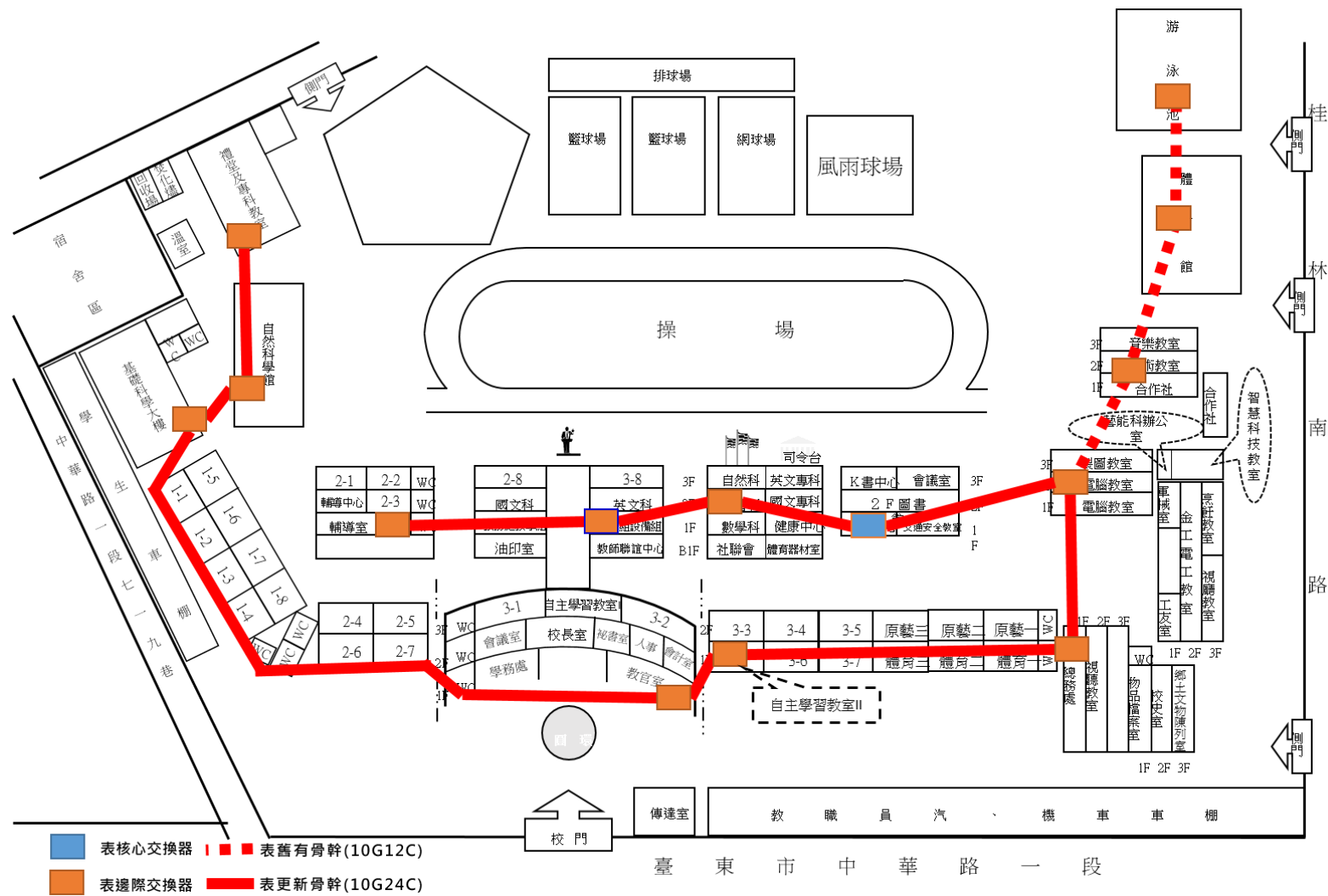


# 機房規劃與維運



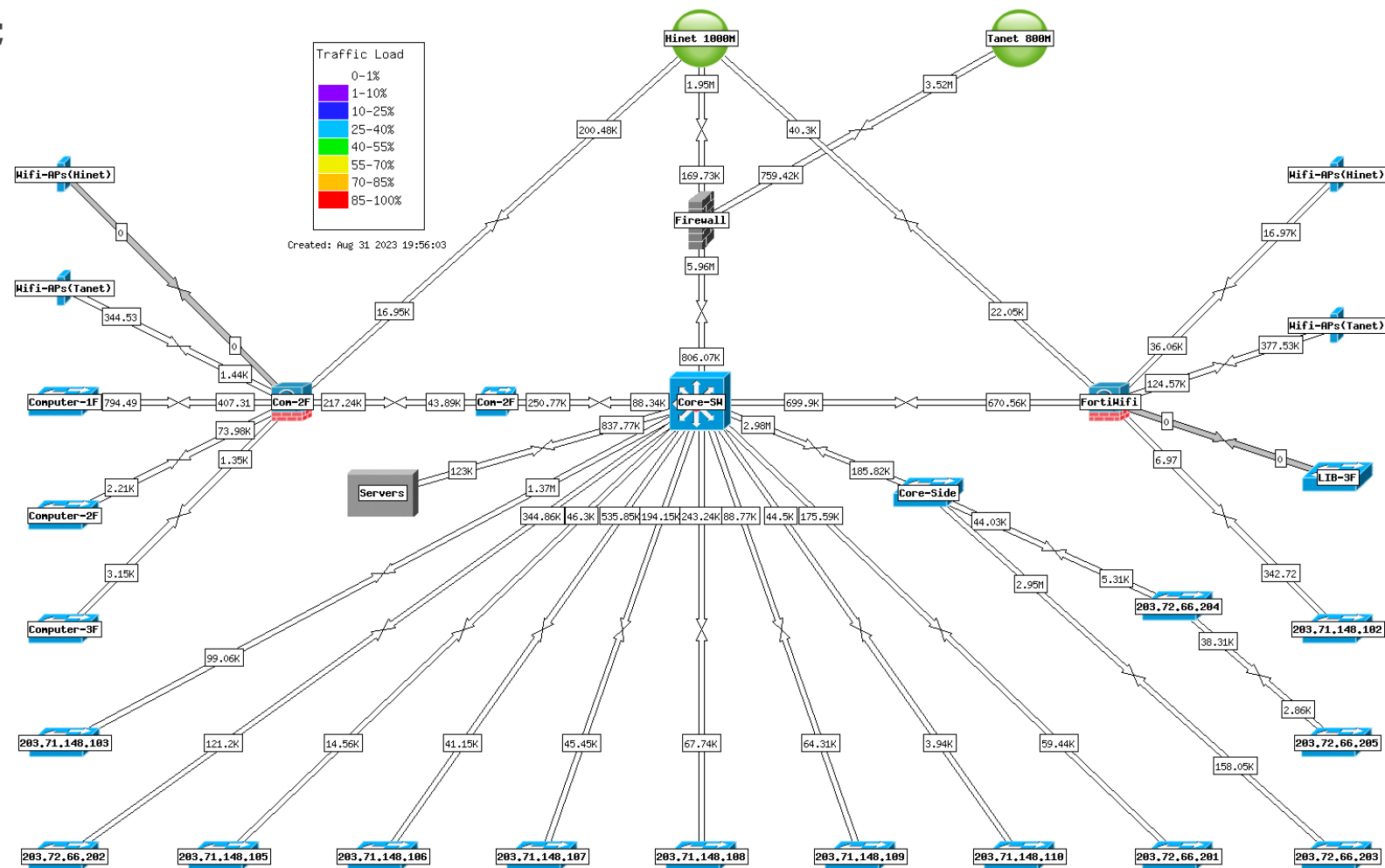
# 機房規劃與維運

## ■ 校內網路架構



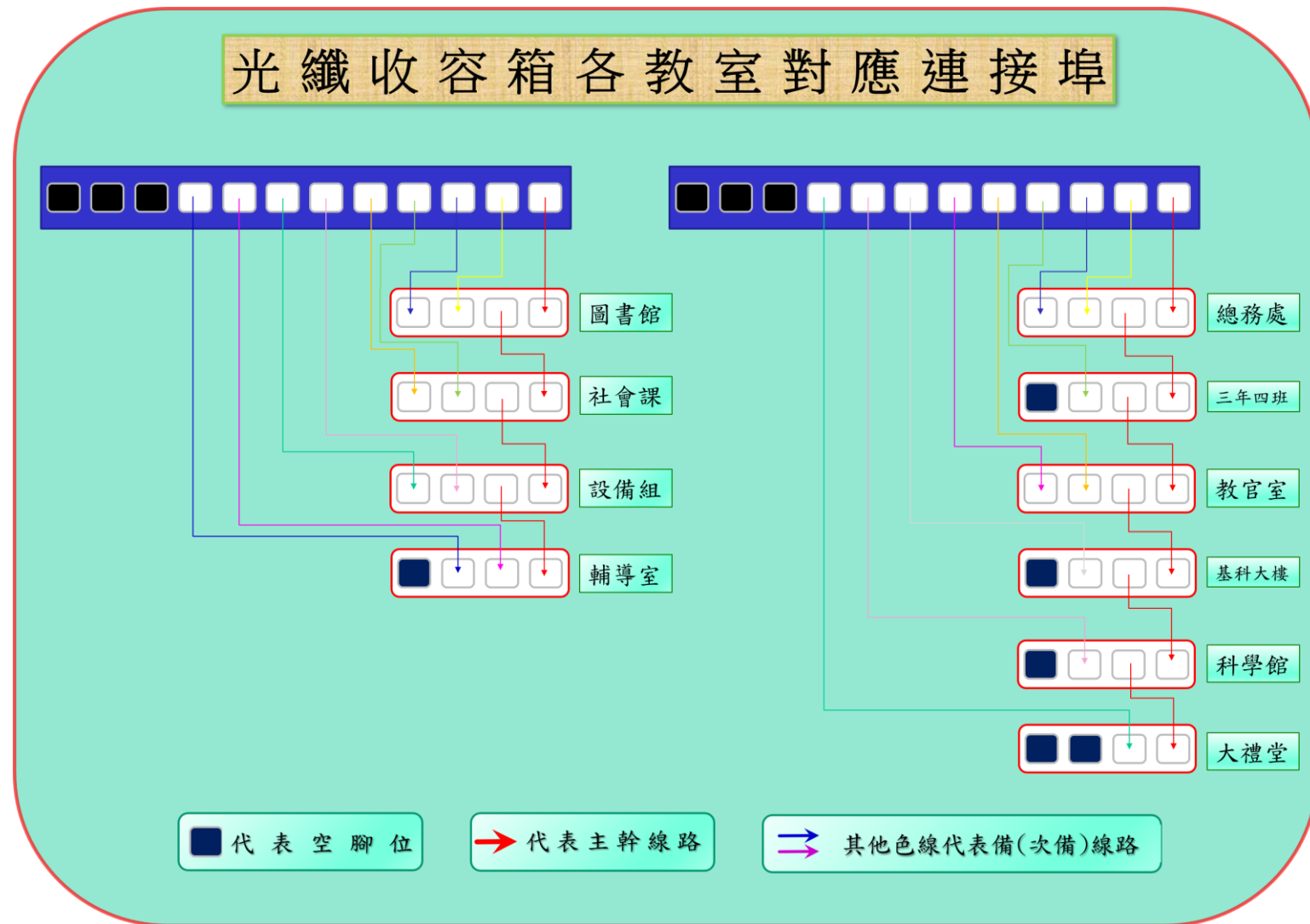
# 機房規劃與維運

## ■ 校內網路架構



# 機房規劃與維運

## ■ 校內網路架構







# 機房規劃與維運-從管理面切入

- 第一步，先進行資產盤點，了解現行架構狀態與運作邏輯。
- 校內各項運作正常，毋需急迫介入網路架構與資通系統運作改善。
- 沒有人天生就會做機房管理，做到那學到那。



# 機房規劃與維運-從管理面切入

- 利用資產盤點工作，了解資產分類的意涵，並對資產加以分類。
  - 人員(PE)、文件(DC)、軟體(SW)、通訊(CM)、硬體(HW)、資料(DA)、環境(EV)



# 機房規劃與維運-從管理面切入

- 閱讀學校的資通安全維運計畫。
  - 資通安全責任等級分級及應辦事項。
  - 資通安全防護等級分級。
  - 資訊資產分級與風險評估。
  - 資通安全組織與管理。
  - 資通安全政策及各項程序書。



# 機房規劃與維運-從管理面切入

- 附件一：資訊安全政策
- 附件二：資訊安全組織
- 附件三：資訊安全組織成員表
- 附件四：校內人員保密切結書
- 附件五：資訊資產管理
- 附件六：風險評鑑與管理
- 附件七：資訊資產異動作業
- 附件八：存取控制管理
- 附件九：實體安全管理
- 附件十：通信與作業管理
- 附件十一：資通安全事件通報及應變程序
- 附件十二：委外廠商保密同意書
- 附件十三：委外廠商執行人員保密切結書
- 附件十四：委外廠商查核項目表
- 附件十五：內部稽核計畫
- 附件十六：稽核項目紀錄表
- 附件十七：內部稽核報告
- 附件十八：矯正與預防處理單

# 機房規劃與維運-從管理面切入

## 附件六-風險評鑑與管理程序書

1. 資訊資產管理程序書
2. 風險評鑑彙整表
3. 風險改善計畫表
4. 適用性聲明書
5. 威脅及弱點評估表

## 附件六-風險評鑑與管理程序書

1. 資訊資產清單
2. 人員進出機房登記表
3. 設備進出紀錄表
4. 異常事件紀錄表
5. 委外廠商保密切結書

# 機房規劃與維運-從管理面切入

- 每年填報資安維護計畫執行情形，資料從何而來??

6.資通安全風險評估	6.1資通安全風險評估及因應？			資訊資產盤點清冊、威脅弱點評估表、風險評估彙整表、風險改善紀錄表
7.資通安全防護及控制措施	7.1資通安全防護及控制措施			實體安全管理程序書、存取控制管理程序書、通訊與作業管理程序書、系統開發及維護管理程序書

- 其實這些都在ISMS四階文件中。

# 機房規劃與維運-設備與架構更新

- 以虛擬器代替實體伺服器，能用Linux就不用Windows。
- 利用合適的NAS來進行各項服務系統備份與異地備援。
- 適當切割VLAN來控管網路。
- 善用GOOGLE來進行教學網路控管，例如：推送WIFI SSID/Pass。
- 利用教育雲帳號進行EDUROAM與教室無線投影。
- 使用LibreNMS實現網路流量即時監控。(管理者需要技術維護)
- 使用Log Server來節省經費。(管理者需要技術維護)

# 機房規劃與維運-設備與架構更新

## ■ 虛擬機好處

- 節省伺服器硬體開銷，附帶節省實體空間。
- 系統統一管理，連KVM都可以少花一點錢。
- 選對設備，備份還原操作簡單，還可順道解決還原演練與系統永續相關資料。

## ■ 虛擬機缺點

- 硬體設備門檻高，單價不親民，且完整架構需再花一筆軟體費用。
- 架建完整虛擬機架構。(可於購置軟硬體時一併提出需求或列入合約內容)
- 底層維護與更新有技術門檻。(可技術外包)



# 機房規劃與維運-設備與架構更新

- 在虛擬器的架構下，市售某些品牌的NAS，可直接支援整機完整、差異備份
- 可規劃添購第二台，與原備份用NAS進行1:1備份支援，逐步達成異地備援目標，該資料安全更有保障。

# 機房規劃與維運-設備與架構更新

- 利用教育雲帳號進行EDUROAM與教室無線投影。
  - 事先規劃並完成佈建，讓每個教室一個獨立VLAN。
  - 各教室不會因學校網路大環境導致無線投影功能不佳。
  - 無線AP使用5G前段頻道，並隔間錯開，2.4G單純留給無線投影等各式無線設備，避免干擾。
  - 適度調整無線AP發射功率，將涵蓋率降至教室範圍。

# 機房規劃與維運-設備與架構更新



# 機房規劃與維運-架構與設備更新

- 以防火牆為例，經費應用該怎麼考量？Log Server？

IPS	NGFW	Threat Protection	Interfaces	F品牌200系列(E)
2.2 Gbps	1.8 Gbps	1.2 Gbps	Multiple GE RJ45, GE SFP Slots	
IPS	NGFW	Threat Protection	Interfaces	F品牌200系列(F)
5 Gbps	3.5 Gbps	3 Gbps	Multiple GE RJ45, GE SFP, and 10 GE SFP+ slots	

# 機房規劃與維運-資安工作分享

- 防火牆規則，除必要開放服務以外，一律設限。
- 遠端控制務必使用“應用程式控制”加以控管，達到「原則禁止、例外開放」。
- 備份機制是否符合維護計畫的RTO與RPO內容。

# 機房規劃與維運-資安工作分享

- 機房環境與管理：
  - 是否堆有雜物或可燃物品。
  - 氣體滅火器建置與保養記錄(利用總務處消防設施定期維護)。
  - 巡查表(請注意溫、濕度記錄)。
  - 機房進出管制。(記錄留存)
  - 設備進出管制。(記錄留存)

# 機房規劃與維運-資安工作分享

- 資通服務合約的資安條款，很難有一套合約能一體適用，一定要依系統進行調整，務必把握住幾個必要內容：
  - 合約內容：明列資通系統責任等級、防護基準、聯合查核條款、備份條款、資料返還條款。
  - 合約附件：委外廠商保密同意書、執行人員保密切結書、查核項目表等。
- 這個工作需要時間與耐心和廠商說明與溝通。

# 機房規劃與維運-資安工作分享

## ■ 備份條款：

- 維護期間，乙方需使用自動執行序，協助設定備份資料庫至甲方指定之資料夾（至少異機備份，若為異地連線備份為佳），並由甲方指定人員定期管理並記錄備份狀態，若因主機硬體故障造成資料遺失，需由甲方自行負責。
- 前項自動備份程序，至少每日進行完整備份，完整備份至少保留一個，由甲方提供足夠的資料庫備份硬碟空間。甲方如需進行資料庫還原演練，乙方以遠端方式協助進行，每次另加收技術服務費用由雙方另行議價之。



# 機房規劃與維運-資安工作分享

- 系統更新條款：
  - 如甲方為保障系統穩定及資料遺失之顧慮，維護期間內主機(SERVER) 及資料庫(由甲方提供)因版本不支援需汰舊換新之搬移及環境設定，以乙次為限，逾乙次則由雙方另行議價之。
- 資安等級與防護基準告知義務：
  - 本合約系統置於甲方機房，為非核心系統，防護等級為普級，乙方於系統各項運作與設定，需配合甲方普級系統防護規範。

# 機房規劃與維運-資安工作分享

## ■ 聯合查核條款：

- 依「資通安全管理法」第九條、「資通安全管理法施行細則」第四條內容，於合約期間，甲方有權對乙方進行相關查核，並依行政院數發部資安署「受託者資通安全聯合查核指引」之專案查核模式進行之，如有因查核延伸相關費用，由雙方另行議定。

## ■ 資料返還條款：

- 於本契約終止或期滿時，乙方應立即返還以前持有屬於甲方所有之資料，或經甲方同意在其監督下以自己之費用銷毀所有屬於甲方之資料。

# 機房規劃與維運-資安工作分享

- 委外廠商保密同意書
- 委外廠商執行人員保密切結書



# 結語

## 結語-行政工作上

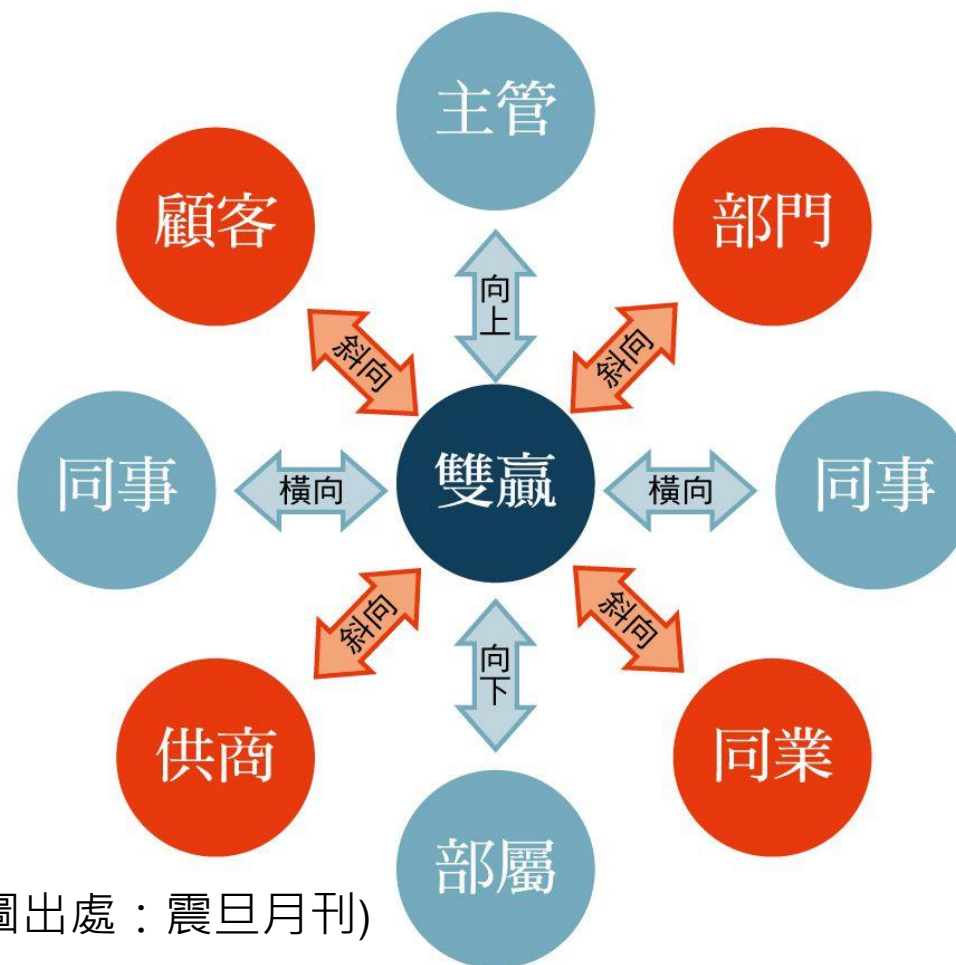
- 跨處室溝通協調務必具備同理心。
- 用正式溝通建立慣例，非正式溝通協調共識。



(插圖出處：震旦月刊)

## 結語-行政工作上

- 橫向協調，斜向說服。
- 助人者，人恆助之。



## 結語-機房管理工作上

- 審酌考量技術外包的必要性。
- 利用文件化管理，作為技術工作或是技術外包時的檢核機制。
- 不要害怕ISMS，完整的資安維護計畫本身就包含一部份ISMS四階文件內容，適度部份導入，當用則用，不合用則棄。
- 第四階文件內容，可以幫助我們有邏輯的管理機房，但絕非照單全收，應依自身環境與情況需求進行部份修改。
- 機房管理並不可怕，可怕的是「你先害怕」。

---

# 感謝大家耐心聆聽

