校園網路規劃管理經驗分享

臺東高中技服組-巫培爾

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)		

SGS

Certificate 43203297 / 133797440

CQI / IRCA 71753

PEI-ER WU

ACADEMY 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

CQI | IRCA
CERTIFIED COURSE

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
Certificated by the International Register of Certificated Auditors (IRCA)

CQI | IRCA
APPROVED TRAINING PARTNER

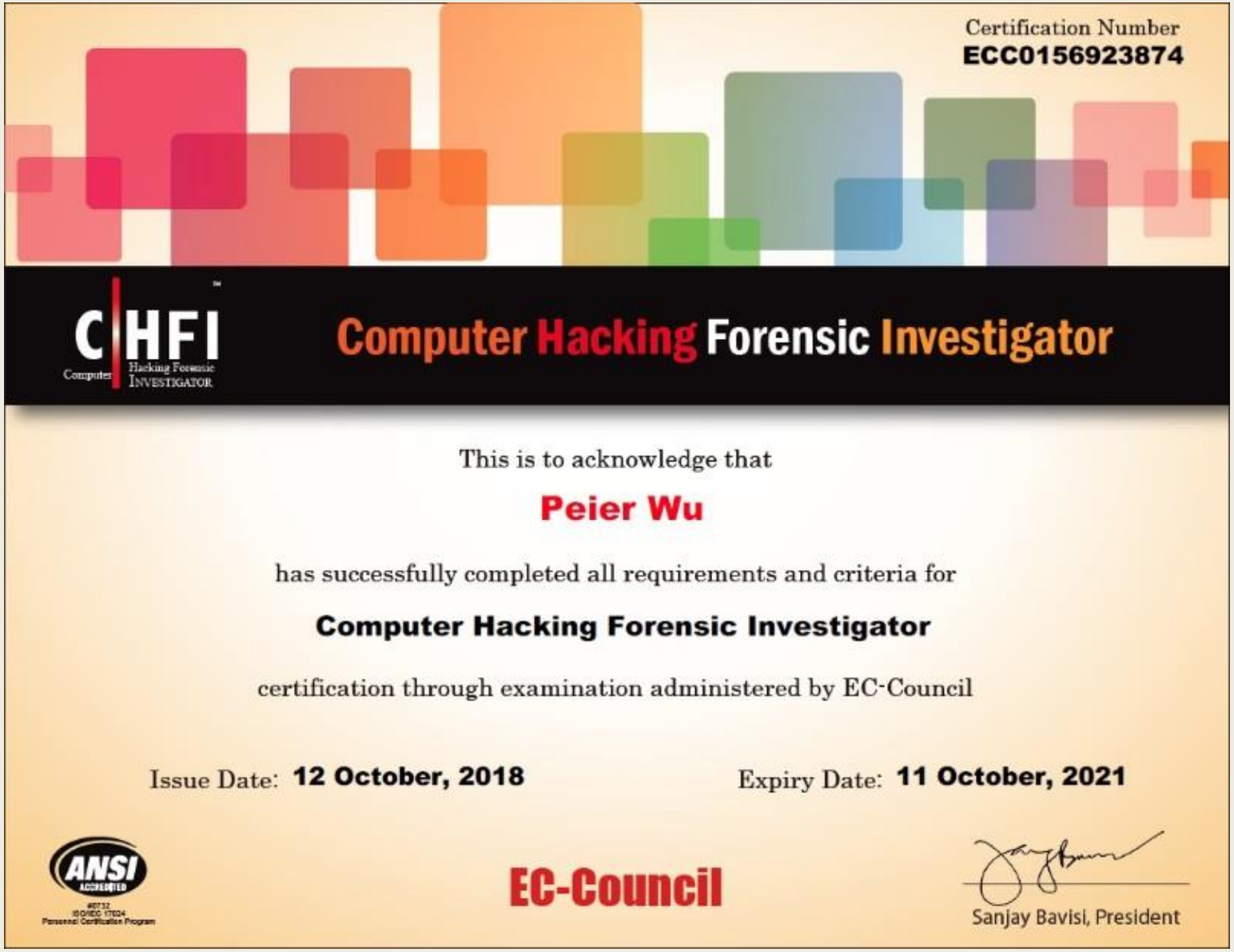
Jan Saunders
UK Business Manager

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

British Quality FOUNDATION

SGS



Certification Number
ECC0156923874

C|HFI Computer Hacking Forensic Investigator

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**

ANSI ACCREDITED
#0732
ISO/IEC 17024
Personnel Certification Program

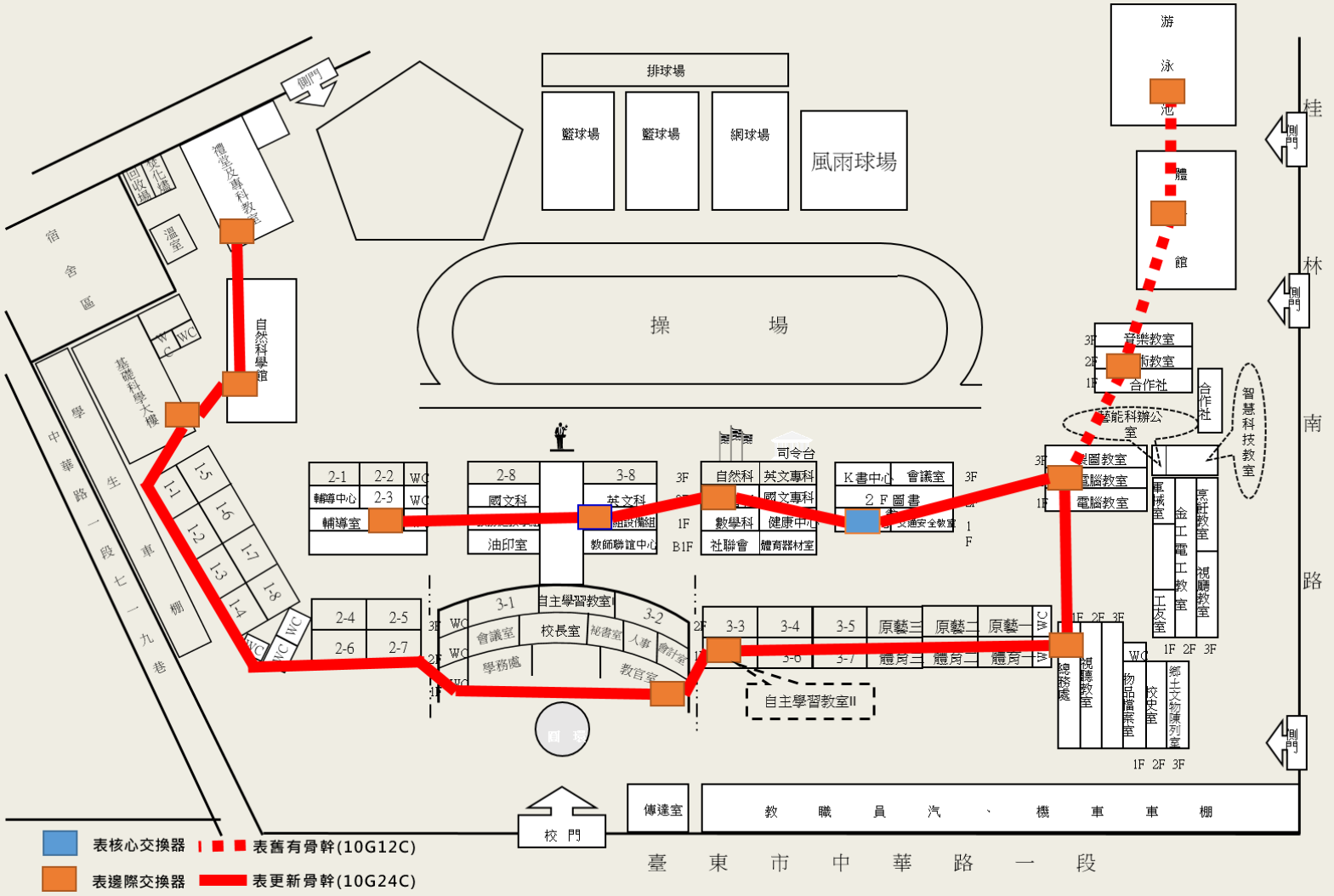
EC-Council

Sanjay Bavisi, President

網路架構簡介
—以東中為例

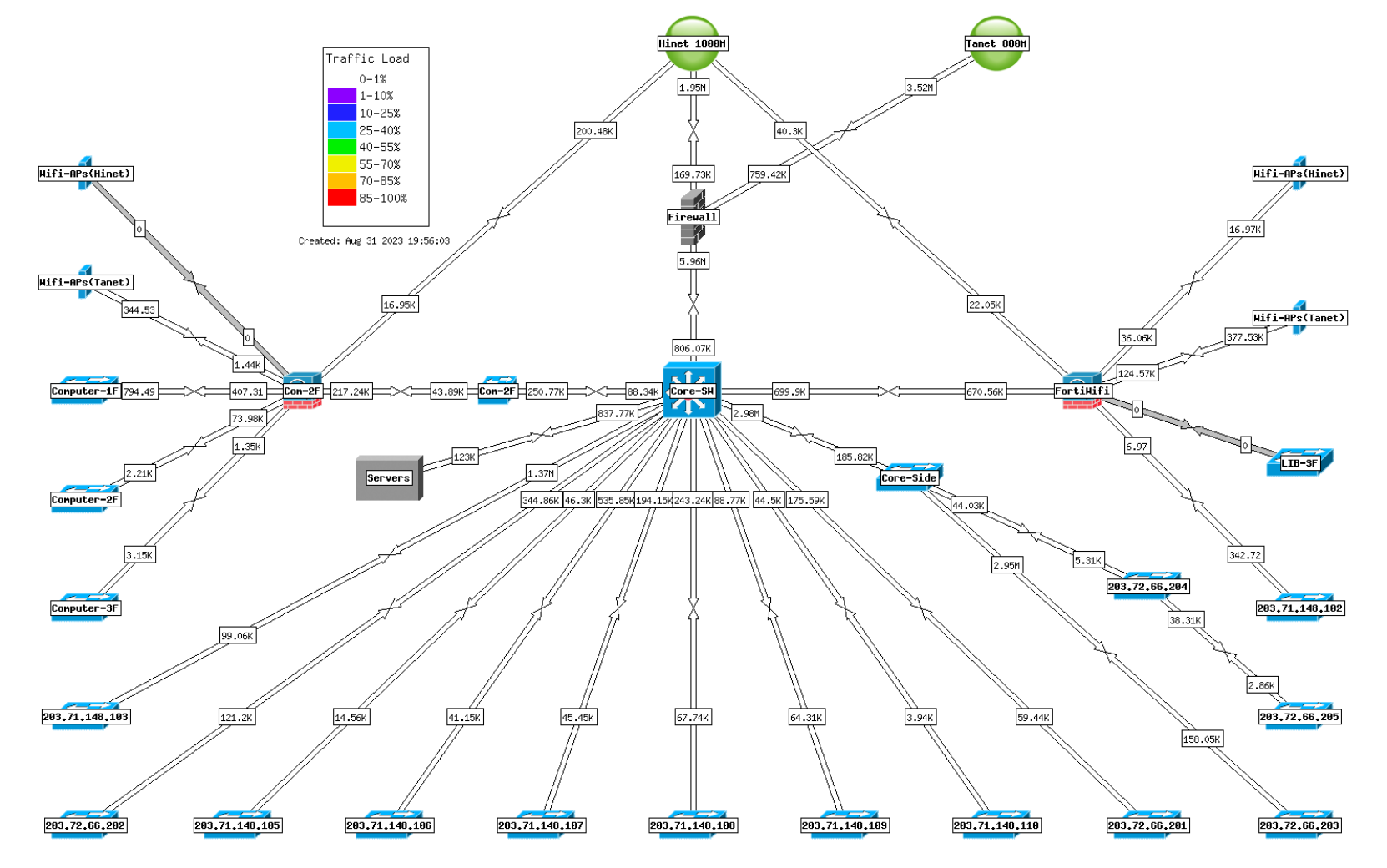
機房規劃與維運

- 校內網路架構



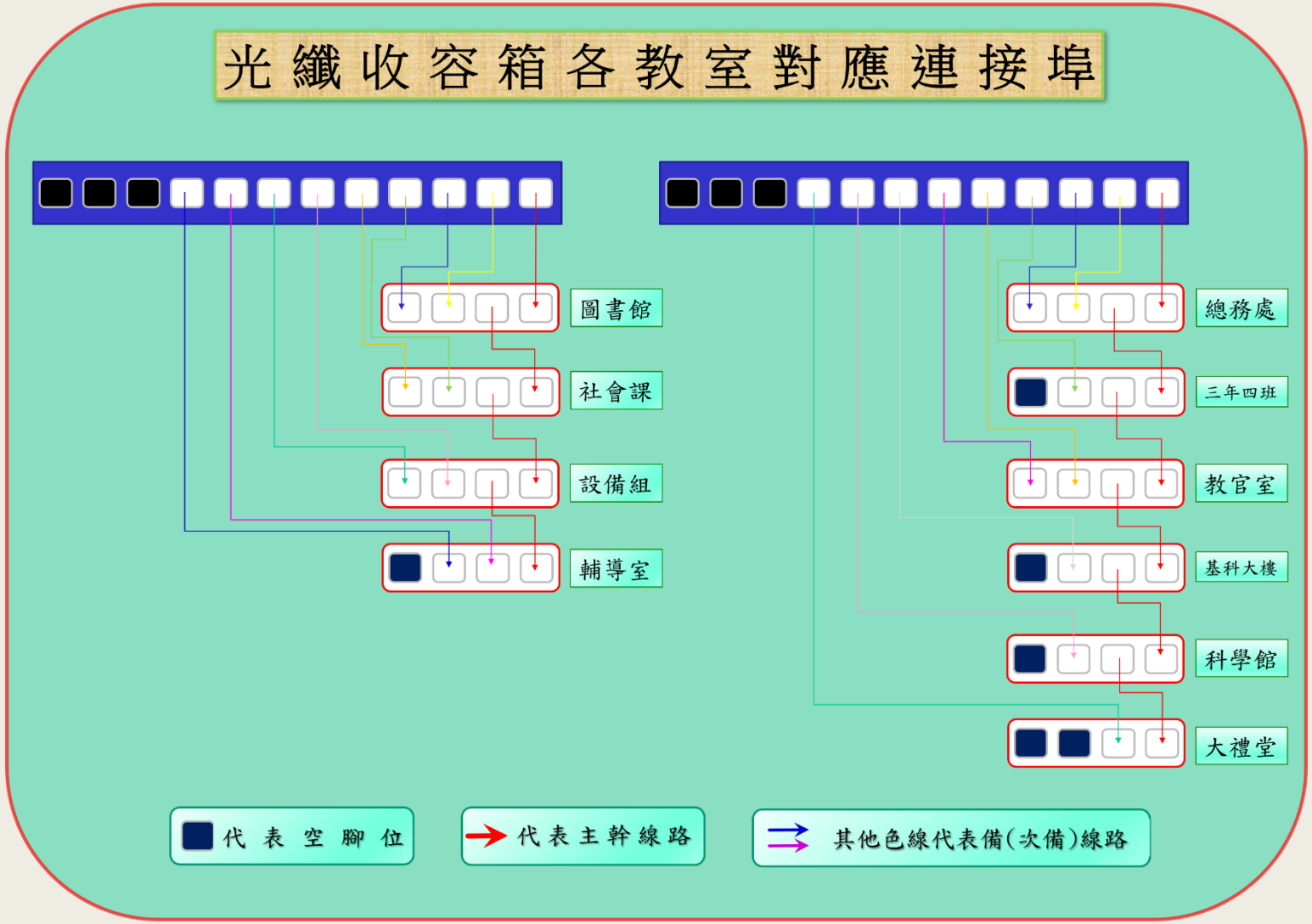
機房規劃與維運

- 校內網路架構



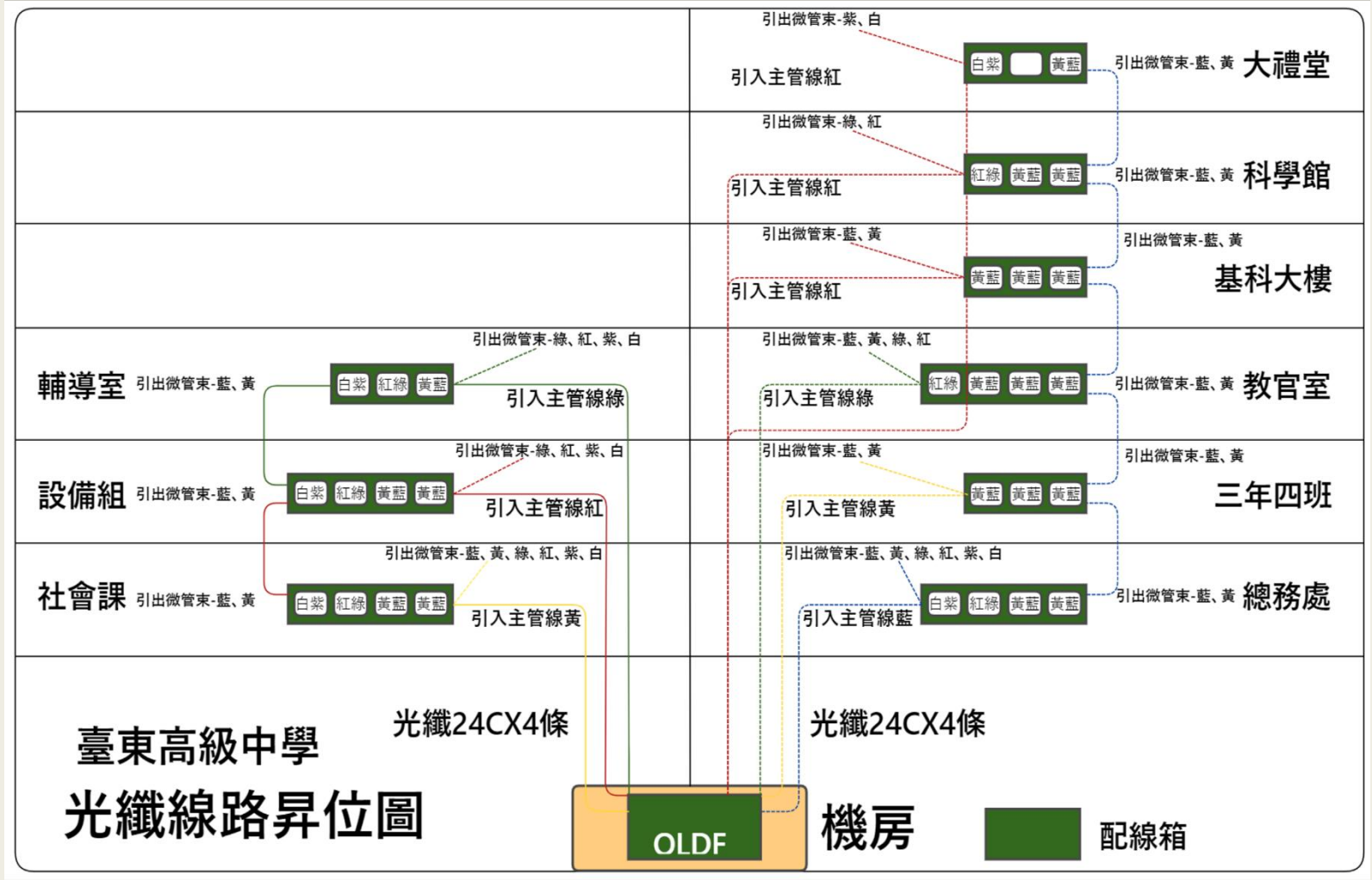
機房規劃與維運

- 校內網路架構



機房規劃與維運

- 校內網路架構



機房設備規畫與調整

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)

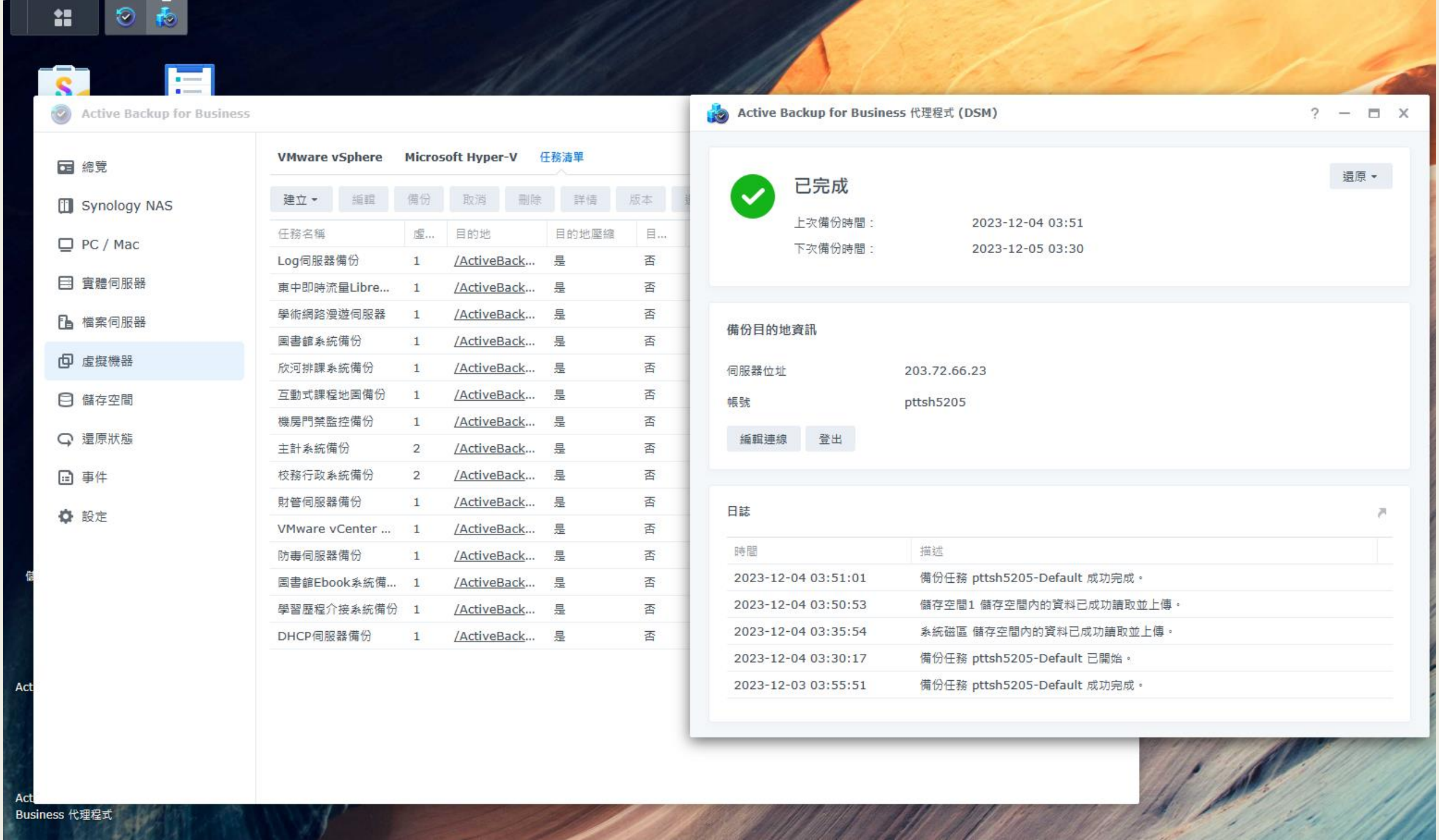
機房規劃與維運-設備與架構更新

- 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有難度。(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)


vSphere Client
功能表
在所有環境中搜尋
172.16.66.10
Pttsh
172.16.66.8
AlienVault-OSSIM-Server-Lite_5.8.11
KMS Server
Portfolio
Singher_Class_System
SKY_Web
Sky_Web-DB
互動式課程地圖系統
學術網路漫遊伺服器
東中即時流量(LibreNMS)
財管系統伺服器
172.16.66.9
dhcp_vlan_all
Library
Log Server
Money_A-(財政伺服器)
Money_B-(網頁伺服器)
TrendMicro_ApexOne_Server2022
VMware vCenter Server Appliance
圖書館Ebook系統
機房門禁監控
172.16.66.8
動作
摘要
監控
設定
權限
虛擬機器
資源集區
資料存放區
網路
更新
Hypervisor: VMware ESXi, 6.7.0, 20497097
型號: PowerEdge R720
處理器類型: Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz
邏輯處理器: 12
NIC: 6
虛擬機器: 10
狀態: 已連線
運作時間: 253 天
DELL EMC
硬體
製造商 Dell Inc.
型號 PowerEdge R720
CPU 12 個 CPU x 2 GHz
記憶體 61.22 GB / 127.96 GB
虛擬 Flash 資源 0 B / 0 B
網路 NODE-A.pttsh.ttct.edu.tw
儲存區 2 個資料存放區

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。

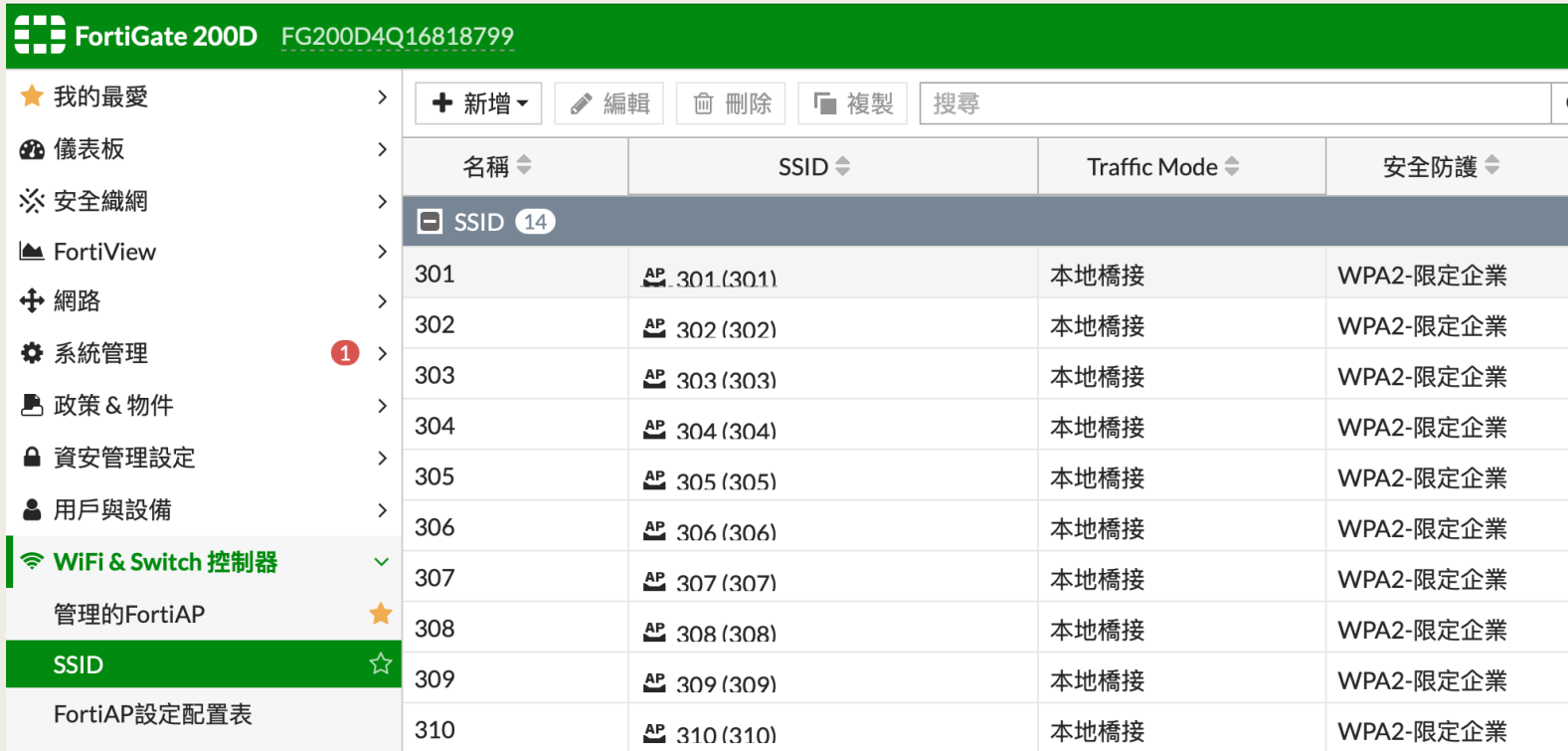

Active Backup for Business
總覽
Synology NAS
PC / Mac
實體伺服器
檔案伺服器
虛擬機器
儲存空間
還原狀態
事件
設定
VMware vSphere
Microsoft Hyper-V
任務清單
建立
編輯
備份
取消
刪除
詳情
版本
任務名稱
虛...
目的地
目的地壓縮
目...
Log伺服器備份 1 /ActiveBack... 是 否
東中即時流量Libre... 1 /ActiveBack... 是 否
學術網路漫遊伺服器 1 /ActiveBack... 是 否
圖書館系統備份 1 /ActiveBack... 是 否
欣河排課系統備份 1 /ActiveBack... 是 否
互動式課程地圖備份 1 /ActiveBack... 是 否
機房門禁監控備份 1 /ActiveBack... 是 否
主計系統備份 2 /ActiveBack... 是 否
校務行政系統備份 2 /ActiveBack... 是 否
財管伺服器備份 1 /ActiveBack... 是 否
VMware vCenter ... 1 /ActiveBack... 是 否
防毒伺服器備份 1 /ActiveBack... 是 否
圖書館Ebook系統備... 1 /ActiveBack... 是 否
學習歷程介接系統備份 1 /ActiveBack... 是 否
DHCP伺服器備份 1 /ActiveBack... 是 否
Active Backup for Business 代理程式 (DSM)
已完成
還原
上次備份時間： 2023-12-04 03:51
下次備份時間： 2023-12-05 03:30
備份目的地資訊
伺服器位址 203.72.66.23
帳號 pttsh5205
編輯連線
登出
日誌
時間
描述
2023-12-04 03:51:01 備份任務 pttsh5205-Default 成功完成。
2023-12-04 03:50:53 儲存空間1 儲存空間內的資料已成功讀取並上傳。
2023-12-04 03:35:54 系統磁區 儲存空間內的資料已成功讀取並上傳。
2023-12-04 03:30:17 備份任務 pttsh5205-Default 已開始。
2023-12-03 03:55:51 備份任務 pttsh5205-Default 成功完成。
Business 代理程式

機房規劃與維運-設備與架構更新

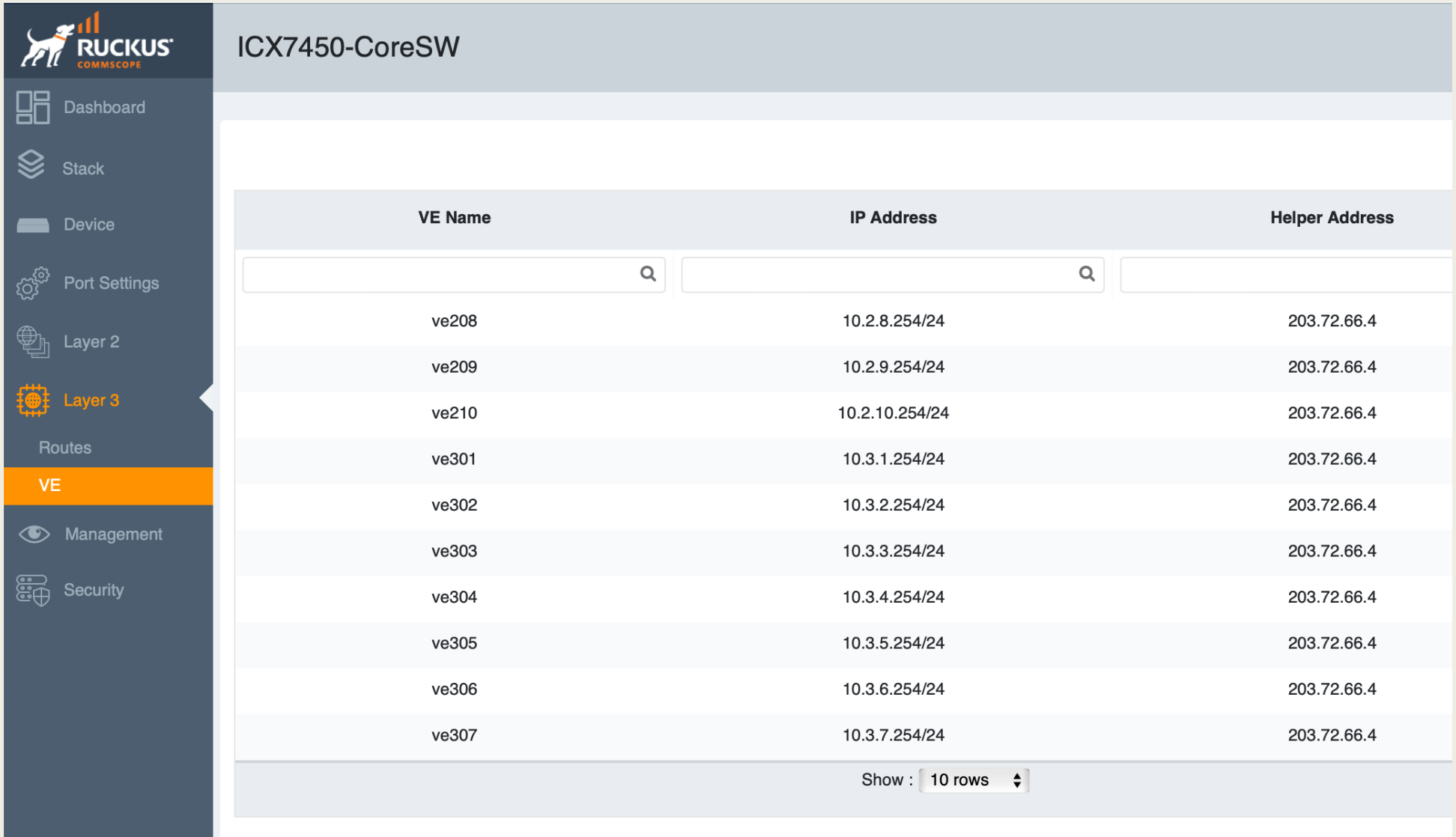
- 利用教育雲帳號進行EDUROAM與教室無線投影。
  - 事先規劃並完成佈建，讓每個教室一個獨立VLAN。
  - 各教室不會因學校網路大環境導致無線投影功能不佳。
  - 無線AP使用5G頻道，並隔間錯開，2.4G單純留給無線投影等各式無線設備，避免干擾。
  - 適度調整無線AP發射功率，將涵蓋率降至教室範圍。
- 校內教師除使用Google Policy推送外，亦可使用Gmail Ldap進行Wi-Fi認證上網。(興大附農林孟郁委員教學檔)

機房規劃與維運-設備與架構更新

- 改用Debian架設Radius Server。
  (漫遊Server架設、仿漫遊中心說明Debian版)
- 將教室VLAN切分。



機房規劃與維運-設備與架構更新



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？

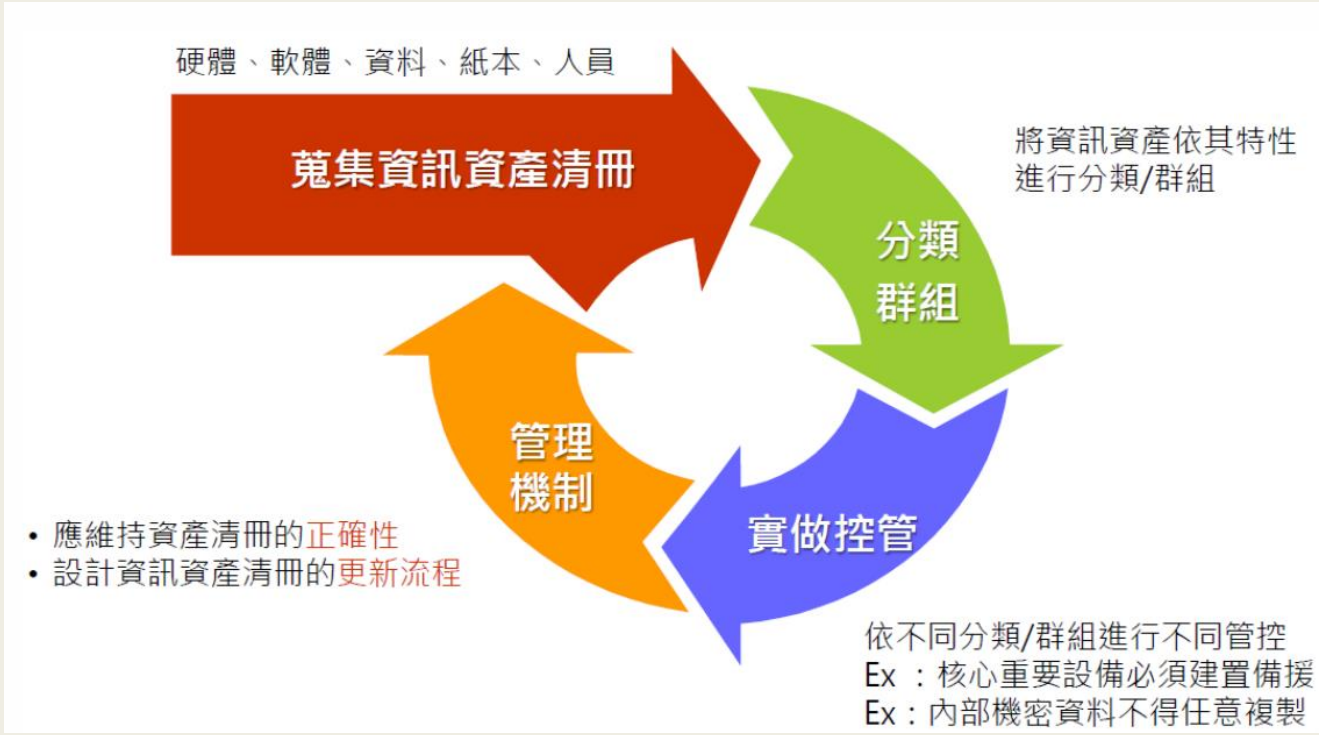
IPS	NGFW	Threat Protection	Interfaces	F品牌200系列(E)
2.2 Gbps	1.8 Gbps	1.2 Gbps	Multiple GE RJ45, GE SFP Slots	

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	

機房資安工作初始化

資產盤點

- 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-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書的RTO與內容。
  - 註1：RTO為Recovery Time Objective，系統恢復運作時間(不包含資料)，使用虛擬器完整還原時，因已包含資料同時還原，故可與MTPD相同。
  - 註2： RPO為Recovery Point Objective，最大可容忍資料損失時間。

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

- 委外合約書
- 資安附約
- 委外廠商保密同意書
- 委外廠商執行人員保密切結書
- 委外廠商查核表

機房管理經驗分享

臺東高中技服組-巫培爾

機房管理相關法規

臺東高中資安與機房管理經驗分享

- 了解各項規範。(相關法規)
- 進行資產盤點。
- 閱讀自己校內的資安維護計畫。(範本、國立臺東高中)
- 準備ISMS文件。(各項文件範本)
- 逐步修改與導入。(國立臺東高中)
- 資通系統風險評鑑參考指引(修訂)(V4.1)
- 校園網路管理規劃。

各項規範(相關法規)

- 教育體系資通安全暨個人資料管理規範。
- 資安六法。
- 資通安全責任等級分級辦法中，需特別注意的事項。
  - 附表05-資通安全責任等級C級之公務機關應辦事項
  - 附表07-資通安全責任等級D級之各機關應辦事項
  - 附表09-資通系統防護需求分級原則
  - 附表10-資通系統防護基準

教育體系資通安全暨個人資料管理規範

- 附件 A-1 各級教育機構適用控制項對照表
  - 適用類型一：建議教育體系各機關（構）、常 設試務機構(如財團法人大學入學考試中心基金會)、公立學校經 資通安全管理法主管機關核定資通安全責任等級為 A 級者可參考

				教版規範 2007 年版	ISO 27001: 2005	適用類型		
A.5 資訊安全政策				A.5	A.5	三	二	一
控制目標	A.5.1	資訊安全之管理指導方針		A.5.1	A.5.1			
控制項	A.5.1.1 (I/P)	資訊安全政策	資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。	A.5.1.1	A.5.1.1	V	V	V

教育體系資通安全暨個人資料管理規範

- 附件 A-1 各級教育機構適用控制項對照表
  - 適用類型二：建議部屬機關(構)、各大學、臺灣學術網路區域 網路中心、各縣市教育網路中心或教育體系各機關（構）、公立 學校經資通安全管理法主管機關核定資通安全責任等級為 B級者可參考

				教版規範 2007 年版	ISO 27001: 2005	適用類型		
A.5 資訊安全政策				A.5	A.5	三	二	一
控制目標	A.5.1	資訊安全之管理指導方針		A.5.1	A.5.1			
控制項	A.5.1.1 (I/P)	資訊安全政策	資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。	A.5.1.1	A.5.1.1	V	V	V

教育體系資通安全暨個人資料管理規範

- 附件 A-1 各級教育機構適用控制項對照表
  - 適用類型三：建議各私立大學、學院、專科學校、高級中等以 下學校納入導入使用。惟欲申請驗證者，仍須採適用類型二之 控制項。
- 應注意，部份內容已過時。

				教版規範 2007 年版	ISO 27001: 2005	適用類型		
A.5 資訊安全政策				A.5	A.5	三	二	一
控制目標	A.5.1	資訊安全之管理指導方針		A.5.1	A.5.1			
控制項	A.5.1.1 (I/P)	資訊安全政策	資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。	A.5.1.1	A.5.1.1	V	V	V

C級之公務機關應辦事項-管理面

- 一年內完成資通系統分級
- 每年至少檢視一次資通系統分級妥適性
- 受核定或等級變更後之二年內，完成附表十之控制措施
- 二年內，全部核心資通系統導入 CNS 27001 或ISO 27001
- 一年內，配置一名專職人員
- 每二年辦理一次內部資通安全稽核
- 全部核心資通系統每二年辦理一次業務持續運作演練

C級之公務機關應辦事項-技術面

- 全部核心資通系統每二年辦理一次
  - 弱點掃描、滲透測試、資通安全健診 、完成導入資通安全弱點通報機制(VANS)
- 一年內啟用各項資通安全防護措施
  - 防毒軟體、網路防火牆、電子郵件過濾機制
- 資通安全教育訓練
  - 專職人員：專業職能課程12小時/年，證照及證書各一張
  - 資訊人員：專業職能課程3小時/2年、資安通識3小時/年
  - 一般使用者：資安通識3小時/年

D級之公務機關應辦事項

- 技術面：一年內完成防毒軟體、網路防火牆，並持續使用及適時進行軟、硬體之必要更新或升級。
- 認知與訓練：每人每年接受三小時以上之資通安全通識教育訓練。(毋需專職人員或專責人員)

資通系統防護需求分級原則–機密性

- 發生資通安全事件，可能造成**未經授權之資訊揭露**，對機關影響：
  - 高：機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。
  - 中：機關之營運、資產或信譽等方面將產生嚴重之影響。
  - 普：對機關之營運、資產或信譽等方面將產生有限之影響。

資通系統防護需求分級原則–完整性

- 發生資通安全事件，可能造成**資訊錯誤或遭竄改**等情事：
  - 高：機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。
  - 中：機關之營運、資產或信譽等方面將產生嚴重之影響。
  - 普：對機關之營運、資產或信譽等方面將產生有限之影響。

資通系統防護需求分級原則–可用性

- 發生資通安全事件，可能造成**對資訊、資通系統之存取或使用之中斷**等情事：
  - 高：機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。
  - 中：機關之營運、資產或信譽等方面將產生嚴重之影響。
  - 普：對機關之營運、資產或信譽等方面將產生有限之影響。

資通系統防護需求分級原則–法律遵循性

- 如**未確實遵循資通系統設置或運作涉及之資通安全相關法令**：
  - 高：使資通系統受影響而導致資安事件，或影響他人合法權益或機關執行業務之公正性及正當性，並**使機關所屬人員負刑事責任**。
  - 中：使資通系統受影響而導致資安事件，或影響他人合法權益或機關執行業務之公正性及正當性，並**使機關或其所屬人員受行政罰、懲戒或懲處**。
  - 普：其他資通系統設置或運作於法令有相關規範之情形。

資通系統防護需求分級原則

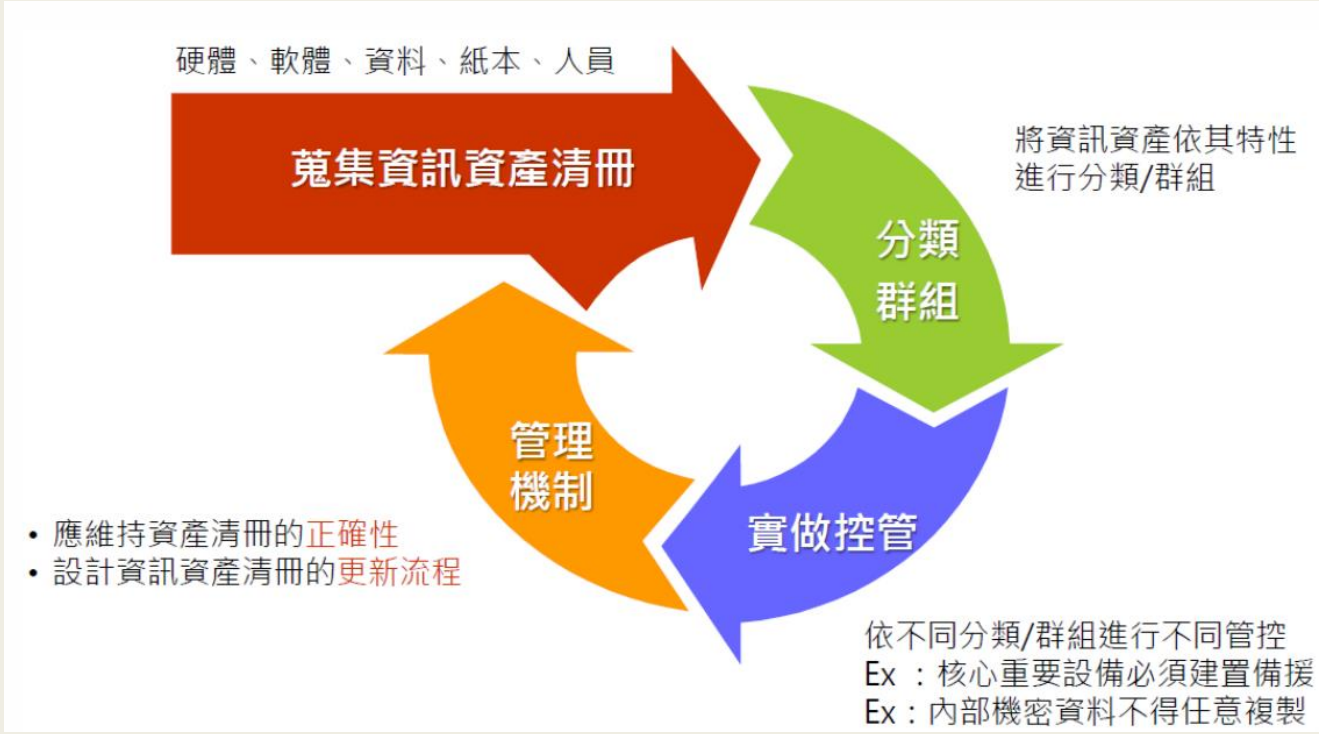
- 資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

文件化管理流程

資產盤點

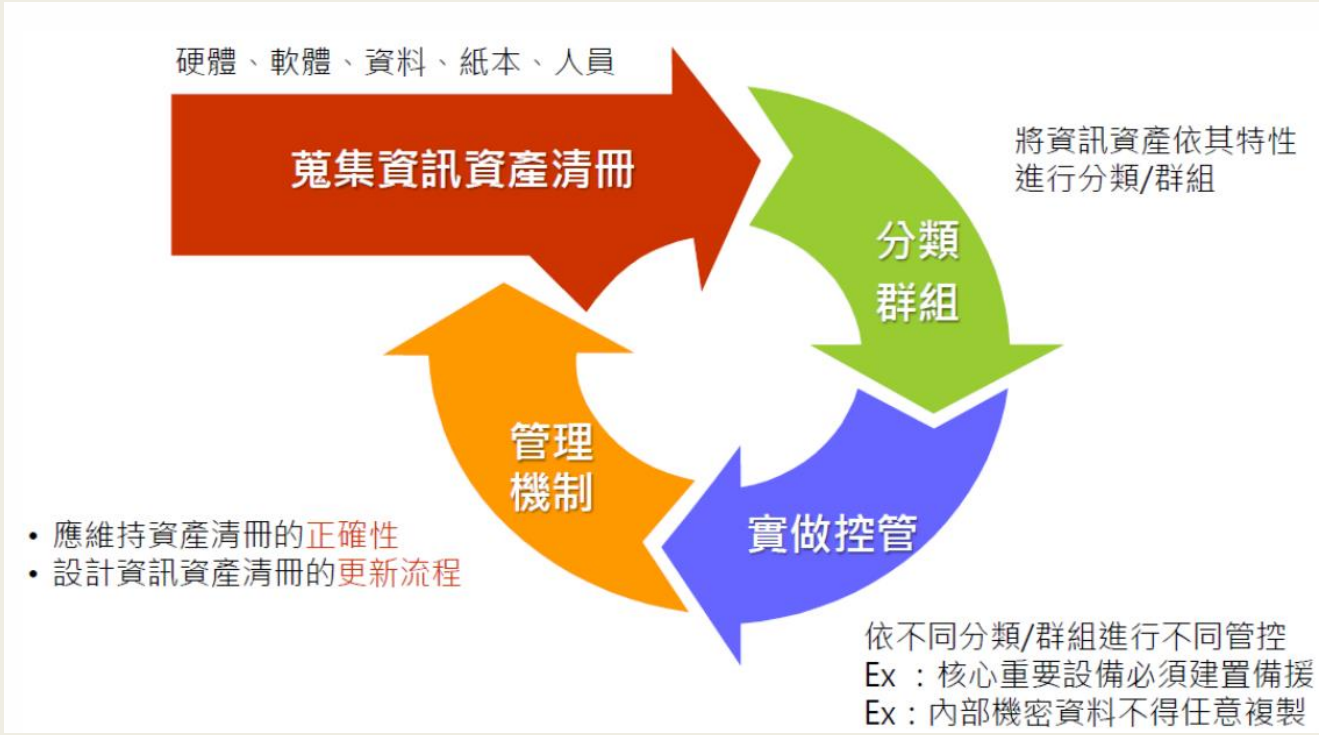
- 萬事起頭難，我該怎麼開始????
  - 先進行資產盤點
  - 先進行資產盤點
  - 先進行資產盤點

  很重要，所以說三次!!!!



資產盤點

- 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。



資產盤點

- 資產盤點，從機房做起，並學會資產分類，共七大類。
  - 通訊(CM)：防火牆、Wifi控管器、交換器、光纖及網路線路。
  - 資料(DA)：校務行政系統資料內容(學生學籍資料、成績資料、缺曠資料等)。
  - 文件(DC)：相關公文、法規、合約內容等。
  - 環境(EV)：UPS、滅火器、冷氣、CCTV等。
  - 硬體(HW)：Server、NAS等硬體。
  - 人員(PE)：資安專職(責)人員。
  - 軟體(SW)：Windows Server、SQL、防毒程式等。

資產盤點

- 機房以外要不要盤？
  - 當然要，先求有，再求好。
- 全校電腦有好幾百台，該怎麼盤？
  - 分類對應進行盤點。
- 校務行政系統管理操作人員要不要盤進來？
  - 嚴格說來，要，但資安訓練要求將不同。**(請審慎考慮!!)**

閱讀自己校內的資安維護計畫

- 核心業務及重要性：
  - 初始：核心系統為中級，非核心為普級。(資安菜鳥)
  - 進階：使用機密性、完整性、可用性與法規遵循性進行資產分級，取其最高等級，作為該資通系統正確分級。高中職較少有高級資通系統，故一般中級必為核心，但普級卻未必非核心(如首頁系統)。

本校之核心業務及重要性如下表：

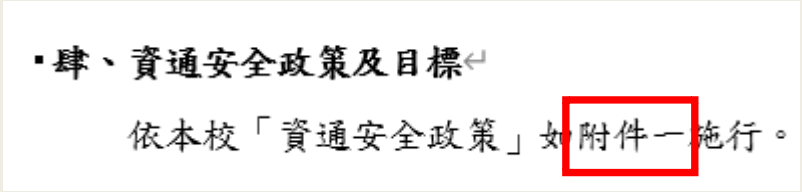
核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間	資通系統分級
校務學生資料管理	天方校務行政系統	為本校依組織法執掌，	1.違反法遵義務：依個	24小時	中

閱讀自己校內的資安維護計畫

- RPO(Recovery Point Objective，復原點目標)
  - 最大可容忍資料損失時間，與備份時間設定有關。
- RTO(Recovery Time Objective，復原時間目標)
  - 最大可容忍中斷時間(不含資料復原)。
- MTPD(Maximum Tolerable Period of Disruption，最大可容忍中斷時間)
  - 最大可容忍中斷時間(含資料復原)。
- 一般而言，RTO ≤ MTPD，若為虛擬器進行完整還原，則RTO=MTPD。

閱讀自己校內的資安維護計畫

- 注意文件中所提及的每個附件。



- 專職(責)人力及資源之配置(C與D不同)

閱讀自己校內的資安維護計畫

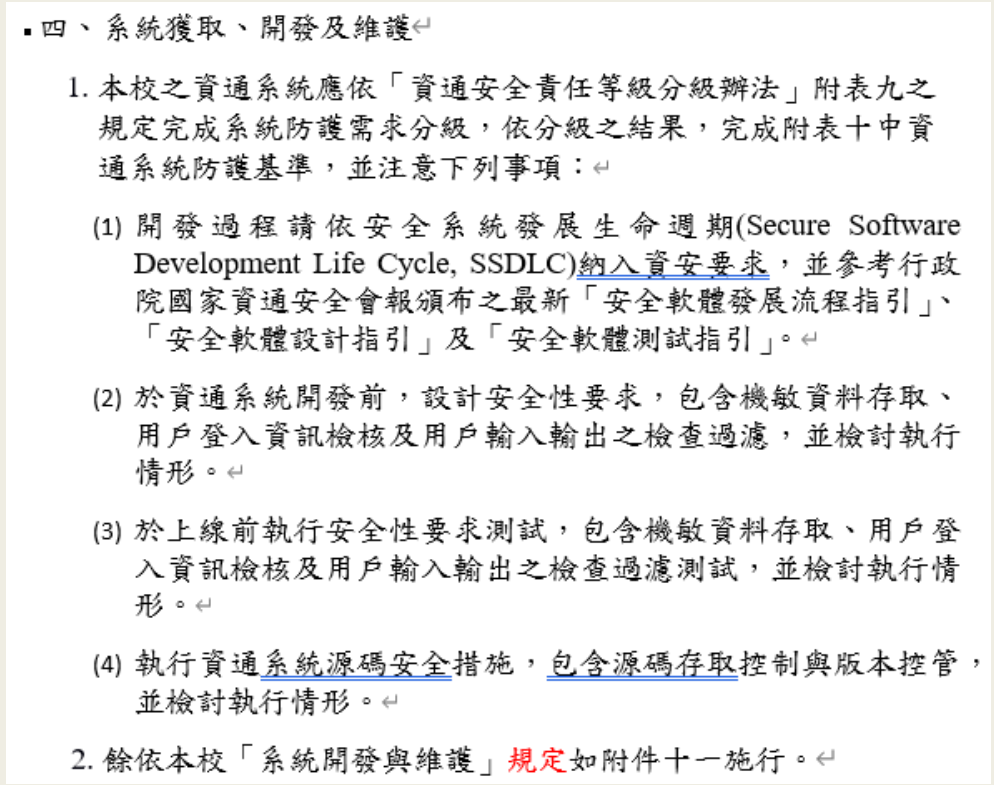
- 資通安全風險評估：請注意RPO與RTO時間設定之合理性。
- 此處的資訊資產，對應資產盤點資料。

二、核心資通系統及最大可容忍資料損失時間

核心資通系統	資訊資產	核心資通系統主要功能	最大可容忍資料損失時間
天方校務行政系統	1. VMWARE 擬虛主機二台 2. Server 2012R2 二套 3. Sybase 資料庫系統一套 4. Microsoft IIS 一套	學籍管理、學生修課、出缺席、輔導狀況資料。	36小時

閱讀自己校內的資安維護計畫

- 審視計畫內容的必要性或符合性，需依自身防護基準與資安責任等級要求修正之。。



▪四、系統獲取、開發及維護↵

1. 本校之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十中資通系統防護基準，並注意下列事項：↵

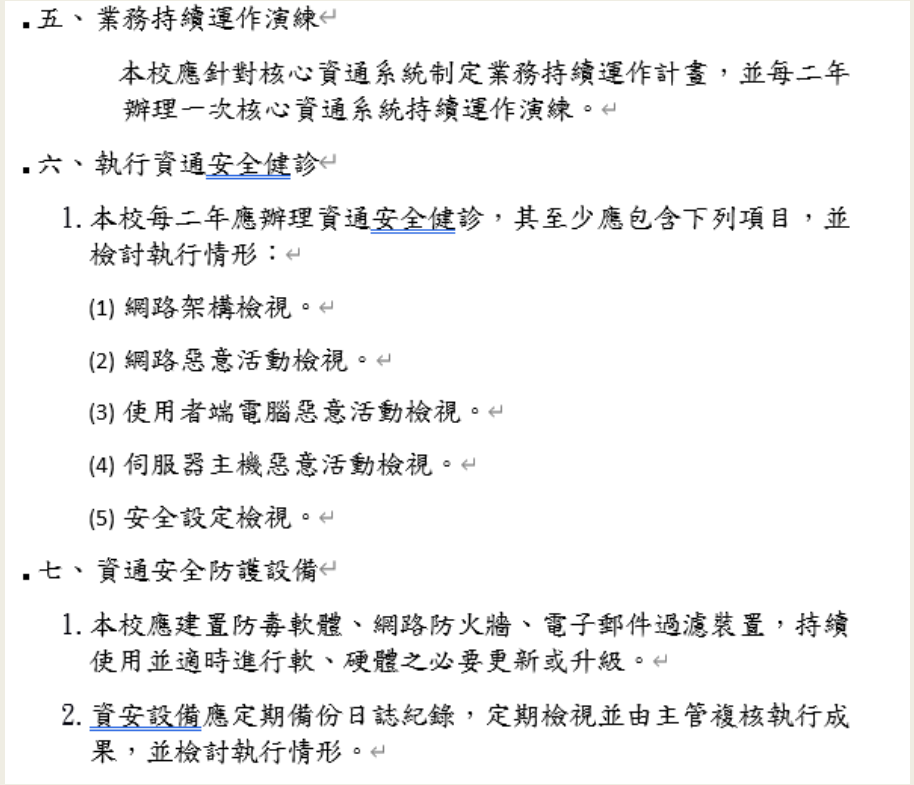
(1) 開發過程請依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。↵

(2) 於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。↵

(3) 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。↵

(4) 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。↵

2. 餘依本校「系統開發與維護」規定如附件十一施行。↵



▪五、業務持續運作演練↵

本校應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。↵

▪六、執行資通安全健診↵

1. 本校每二年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：↵

(1) 網路架構檢視。↵

(2) 網路惡意活動檢視。↵

(3) 使用者端電腦惡意活動檢視。↵

(4) 伺服器主機惡意活動檢視。↵

(5) 安全設定檢視。↵

▪七、資通安全防護設備↵

1. 本校應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。↵

2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。↵

閱讀自己校內的資安維護計畫

- 資通安全教育訓練，如果盤點有納入資訊人員，則此處應修改加入資訊人員的訊練要求。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

1. 本校資安及資訊人員每年至少接受12小時以上之資安專業課程訓練或資安職能訓練。
2. 本校之一般使用者與主管，每人每年接受3小時以上之一般資通安全教育訓練。

閱讀自己校內的資安維護計畫

- 資通安全維護計畫實施情形之稽核機制(D可修)

二、資通安全維護計畫實施情形之稽核機制

(一) 稽核機制之實施

1. 資訊安全稽核小組應定期(至少每二年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

2. 辦理稽核前資通安全小組應擬定「內部稽核計畫」如附件十六並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務（稽核委員簽署「保密切結書」如附件四）、稽核方式、基準與項目及受稽單位協助

閱讀自己校內的資安維護計畫

- 資通安全維護計畫實施情形之稽核機制(D可修)
  - 資訊安全稽核小組應定期(每年一次)以自我檢核表，確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。
  - 發生資安事件時，稽核小組應依內部稽核計畫(附件十五)，對事件相關單位進行實地稽核。

(一) 稽核機制之實施↵

1. 資訊安全稽核小組應定期(每年一次)以自我檢核表，確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。↵
2. 發生資安事件時，稽核小組應依內部稽核計畫(附件十五)，對事件相關單位進行實地稽核。↵

閱讀自己校內的資安維護計畫–管審會

- 過往管理審查議案之處理狀態。
- 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。
- 資通安全維護計畫內容之適切性。
- 資通安全績效之回饋，包括：
  - 資通安全政策及目標之實施情形。
  - 資通安全人力及資源之配置之實施情形。
  - 資通安全防護及控制措施之實施情形。
  - 稽核結果。
  - 不符合項目及矯正措施。
- 風險評鑑結果及風險處理計畫執行進度。
- 重大資通安全事件之處理及改善情形。
- 利害關係人之回饋。
- 持續改善之機會。

閱讀自己校內的資安維護計畫—相關法規

- 資通安全管理法
- 資通安全管理法施行細則
- 資通安全責任等級分級辦法
- 資通安全事件通報及應變辦法
- 資通安全情資分享辦法
- 公務機關所屬人員資通安全事項獎懲辦法

- 資訊系統風險評鑑參考指引
- 政府資訊作業委外安全參考指引
- 無線網路安全參考指引
- 網路架構規劃參考指引
- 行政裝置資安防護規劃報告
- 政府行動化安全防護規劃報告
- 安全軟體發展流程指引
- 安全軟體設計指引
- 安全軟體測試指引
- 資訊作業委外安全參考指引

閱讀自己校內的資安維護計畫—相關表件

- 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**

資通安全政策

- 資安維護計畫修正稽核內容後，務必在資通安全政策附件上也要修正。

4 目標↵

維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由本校全體同仁共同努力來達成下列定性及定量目標：↵

4.1 定性目標：↵

4.1.1 確保相關資通安全措施或規範符合政策與現行法令的要求每二年至少進行一次內部稽核。↵

4.1.2 每二年至少進行一次業務持續計畫之測試或檢核。↵

風險評鑑與管理程序書

- 資訊安全委員會每年召開會議檢討可接受風險值。
- 高於可接受風險值項目，產出「風險評鑑彙整表」，並產出「風險改善計畫表」，說明風險控管措施之執行辦法。

5.2.3風險值的計算↵

評估威脅發生之可能性及弱點受到威脅利用之容易度，計算出風險值。↵

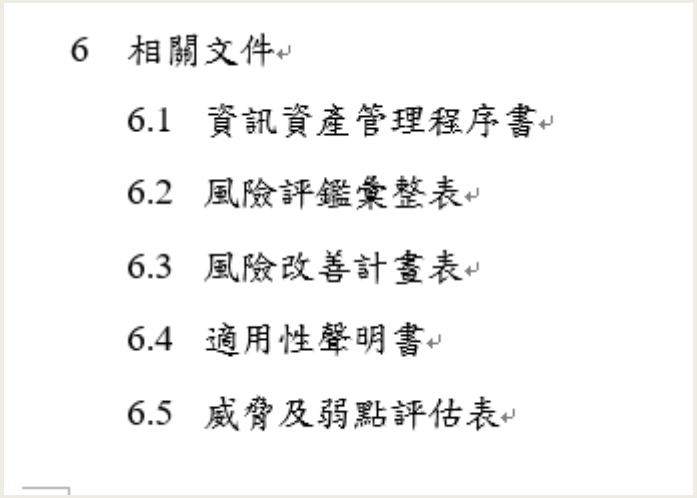
風險值=（資訊資產價值 × 威脅等級 × 弱點等級）↵

準備ISMS文件(範本)


A-001資訊安全政策.docx
Microsoft Word 文件
23.9 KB
B-001資訊安全組織程序書.docx
Microsoft Word 文件
B-002文件管理程序書.docx
Microsoft Word 文件
98.5 KB
B-003資訊資產管理程序書.docx
Microsoft Word 文件
B-004風險評鑑與管理程序書.docx
Microsoft Word 文件
B-005人力資源安全管理程序書.docx
Microsoft Word 文件
B-006實體安全管理程序書.docx
Microsoft Word 文件
B-007通信與作業管理程序書.docx
Microsoft Word 文件
B-008存取控制管理程序書.docx
Microsoft Word 文件
B-009系統開發與維護.docx
Microsoft Word 文件
33.2 KB
B-010委外管理程序書.docx
Microsoft Word 文件
31.6 KB
B-011資通安全事件通報及應變管理程序.docx
Microsoft Word 文件
B-012業務永續運作管理程序書.docx
Microsoft Word 文件
B-013內部稽核計畫.docx
Microsoft Word 文件
29.5 KB
B-014矯正及預防管理程序書.docx
Microsoft Word 文件
C-001資訊資產異動作業說明書.docx
Microsoft Word 文件
D-001資訊安全組織成員表(去個資公告版).docx
Microsoft Word 文件
D-001資訊安全組織成員表.docx
Microsoft Word 文件
D-002外來文件一覽表.docx
Microsoft Word 文件
23.8 KB
D-003外部單位聯絡清單.docx
Microsoft Word 文件
D-004ISMS有效性量測表.docx
Microsoft Word 文件
D-005資通安全管理審查會議記錄.docx
Microsoft Word 文件
D-006文件調閱申請單.docx
Microsoft Word 文件
22.3 KB
D-007文件修改建議表.docx
Microsoft Word 文件
21.5 KB
D-008資訊安全管理文件列表.docx
Microsoft Word 文件
D-009資訊資產清單.docx
Microsoft Word 文件
33.6 KB
D-011威脅及弱點評估表.docx
Microsoft Word 文件
D-012風險評鑑彙整表(全部).docx
Microsoft Word 文件
D-012風險評鑑彙整表(高風險).docx
Microsoft Word 文件
D-013風險改善計畫表.docx
Microsoft Word 文件
21.6 KB
D-014適用性聲明書.docx
Microsoft Word 文件
34.7 KB
D-015人員資通安全守則.docx
Microsoft Word 文件
D-016保密切結書(校內人員).docx
Microsoft Word 文件
D-019人員進出機房登記表.docx
Microsoft Word 文件
D-020異常事件紀錄表.docx
Microsoft Word 文件
20.9 KB
D-021設備進出紀錄表.docx
Microsoft Word 文件
21.9 KB
D-022-1委外廠商保密同意書.docx
Microsoft Word 文件
D-022-2委外廠商執行人員保密切結書.docx
Microsoft Word 文件
D-022-3委外廠商查核項目表.docx
Microsoft Word 文件
D-023巡查紀錄表.docx
Microsoft Word 文件
23.0 KB
D-024防火牆進出規則申請表.docx
Microsoft Word 文件
D-025備份狀況紀錄表.docx
Microsoft Word 文件
21.2 KB
D-027資訊服務申請表.docx
Microsoft Word 文件
22.3 KB
D-028帳號清查紀錄表.docx
Microsoft Word 文件
22.4 KB
D-029帳號異動與清查報告.docx
Microsoft Word 文件
D-036資訊安全事件報告單.docx
Microsoft Word 文件
D-037業務永續運作計畫演練活動紀錄.docx
Microsoft Word 文件
D-038業務流程衝擊分析表.docx
Microsoft Word 文件
D-039-1資訊安全管理制度內部稽核表.docx
Microsoft Word 文件
D-039-2內部稽核項目記錄表.docx
Microsoft Word 文件
D-040矯正與預防處理單.docx
Microsoft Word 文件
D-041內部稽核報告.docx
Microsoft Word 文件
23.1 KB

準備ISMS文件

- 會用到那一些文件????



6 相關文件

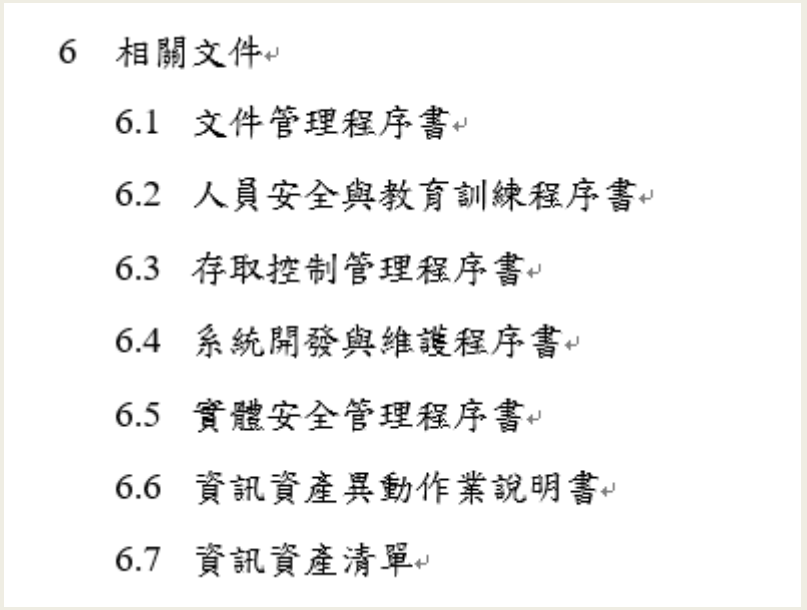
6.1 資訊資產管理程序書

6.2 風險評鑑彙整表

6.3 風險改善計畫表

6.4 適用性聲明書

6.5 威脅及弱點評估表



6 相關文件

6.1 文件管理程序書

6.2 人員安全與教育訓練程序書

6.3 存取控制管理程序書

6.4 系統開發與維護程序書

6.5 實體安全管理程序書

6.6 資訊資產異動作業說明書

6.7 資訊資產清單

逐步修改與導入(國立臺東高中)

巡查紀錄表

文件編號	LIB-D-023	機密等級	限閱	版次	1.2

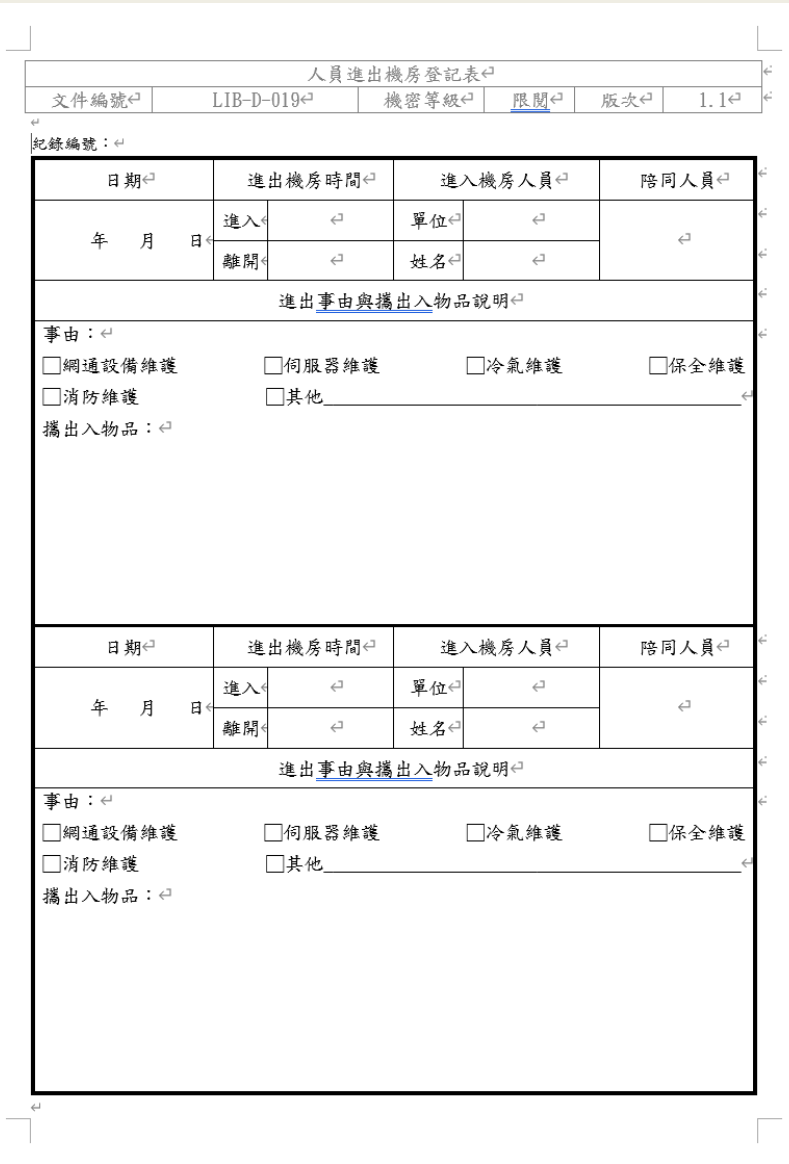
紀錄編號：

年 月	週次	日期	星期	伺服主機狀態	設備燈號	網路狀況	溫度(℃)	溼度(%)	防火牆政策及設定（每月第一個工作天）其他事件說明	簽章
	第一週		一						每月第一個工作天：	
			二						□主防火牆設定備份	
			三						□主防火牆政策檢核	
			四						□Wifi 控管設定備份	
			五						□Wifi 控管設定檢核	
	第二週		一						□電教控管設定備份	
			二						□電教控管設定檢核	
			三							
			四						其他事件說明：	
			五						□無(每月最後一天)	
	第三週		一						□有，說明如下。	
			二							
			三							
			四							
			五							
	第四週		一							
			二							
			三							
			四							
			五							
	第五週		一							
			二							
			三							
			四							
			五							

填表說明：

1. 項目檢查後請於該日簽章，每月結束併同異常事件紀錄表呈交主管審閱，後交文管編號存參。
2. 項目檢查週期內，負責人因外務無法檢查，請由代理人檢查相關項目。
3. 無異常用∨符號、異常用Λ符號，並將異常狀況紀錄於異常事件紀錄表，檢查項次太多表格不足請自行延伸。

主管審閱



人員進出機房登記表

文件編號	LIB-D-019	機密等級	限閱	版次	1.1

紀錄編號：

日期	進出機房時間		進入機房人員		陪同人員
年 月 日	進入		單位		
	離開		姓名		

進出事由與攜出入物品說明

事由：

□網通設備維護 □伺服器維護 □冷氣維護 □保全維護

□消防維護 □其他_____

攜出入物品：

日期	進出機房時間		進入機房人員		陪同人員
年 月 日	進入		單位		
	離開		姓名		

進出事由與攜出入物品說明

事由：

□網通設備維護 □伺服器維護 □冷氣維護 □保全維護

□消防維護 □其他_____

攜出入物品：

資通系統風險評鑑參考指引

- 配合資訊資產清單，建立**威脅及弱點評估表**。
  - 內部弱點、外部威脅。
  - 內部弱點與外部威脅可互為因果，可以因內而外，亦可能由外而內。
- 風險值的判斷，請依照維護計畫–**風險評鑑與管理程序書**。

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級（發生之可能性）低(1) 中(2) 高(3)	弱點等級（受到威脅利用之容易度）低(1) 中(2) 高(3)	風險值
	CM	光纖(單模 24 芯)	2	運作不良	線路老舊	1	1	2
				中斷	施工意外或遭破壞	1	1	2

資通系統風險評鑑參考指引

- 高風險資產，請建立風險評鑑彙整表，並建議風險改善計畫表。

項次	資產編號	資產類別	資產名稱	資產說明	權責單位	資產價值	風險事件		風險值	風險再評估			
							威脅	弱點		資產價值	威脅等級	弱點等級	風險值
1		HW	機架式伺服器	Dell PowerEdge R720(Vmware-A)	技服組	3	故障	已過使用年限	27				
2		HW	機架式伺服器	Dell PowerEdge R720(Vmware-B)	技服組	3	故障	已過使用年限	27				
3		HW	網路陣列儲存媒體	Dell MD3600f	技服組	3	故障	已過使用年限	27				

教育體系資通安全管理規範控制目標	現況說明	風險改善建議措施	教育體系資通安全管理規範條文	建議權責單位	預計改善時間與處理方式	與高風險資產之風險評估彙整表對照
A.17.1	校內虛擬機用伺服器已超過使用年限，且達 10 年，發生硬體性故障的機率相對提高。	規劃今年爭取計畫補助款或是明年以校內設備費用進行太換。	A.17.1.1：規劃資訊安全持續	圖書館 技服組	112.6.30	1、2
A.17.1	校內虛擬機用磁碟陣列儲存系統已超過使用年限，且已達 10 年，發生硬體性故障的機率相對提高。	規劃今年爭取計畫補助款或是明年以校內設備費用進行太換。	A.17.1.1：規劃資訊安全持續	圖書館 技服組	112.6.30	3

感謝大家耐心聆聽
Q & A