教育部國民及學前教育署

K-12 Education Administration, Ministry of Education

111年度校園資通安全專責人員知能研習

資通系統硬體管理實務

硬體設備

稽核重點

法規依循

輔助作業

總結

Prezi

法規依循

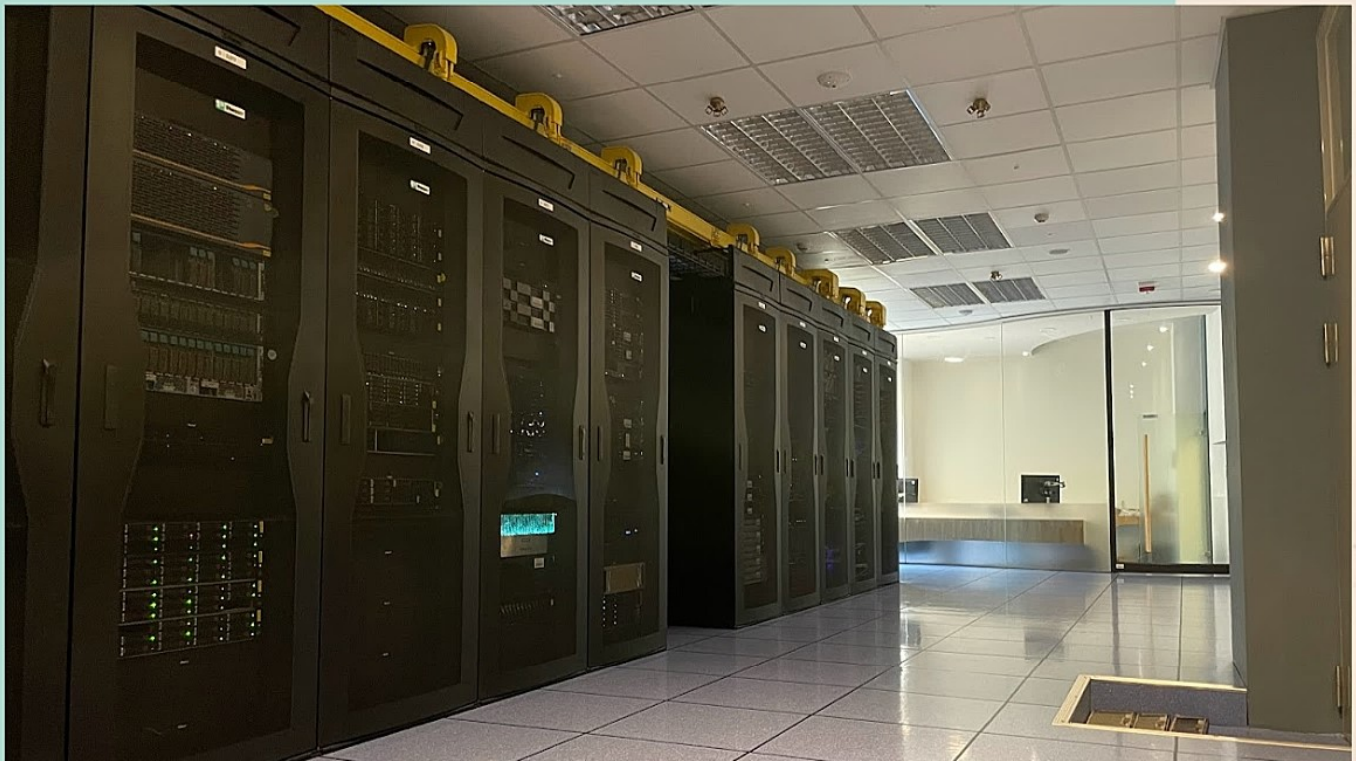
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		一、 初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	

相關內容可參閱110年研習課程

Prezi

資通系統之硬體設備

資通系統所涵蓋之硬體設備以資訊機房為主，對包含環境支援、伺服器設備、儲存設備、網通設備及個人設備。



- 環境支援
- 伺服器設備
- 儲存設備
- 網通設備
- 個人設備

Prezi

設備應定期執行維護及保養作業，並留存紀錄（5.11）

環境設備

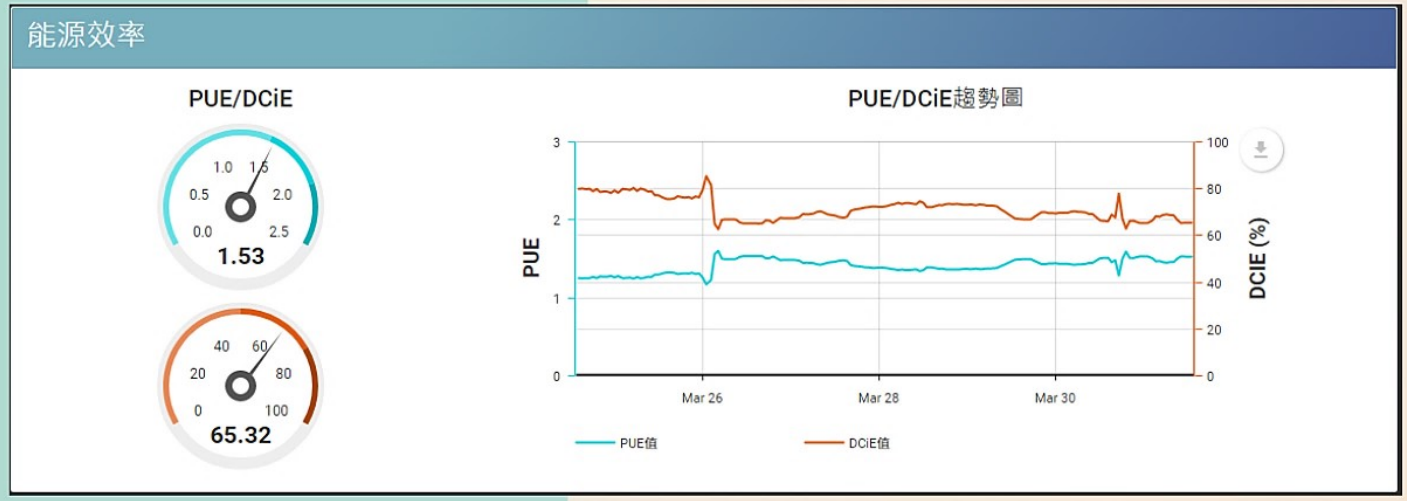
- 空調設備
- 電力設備
- 消防設備
- 其他設備

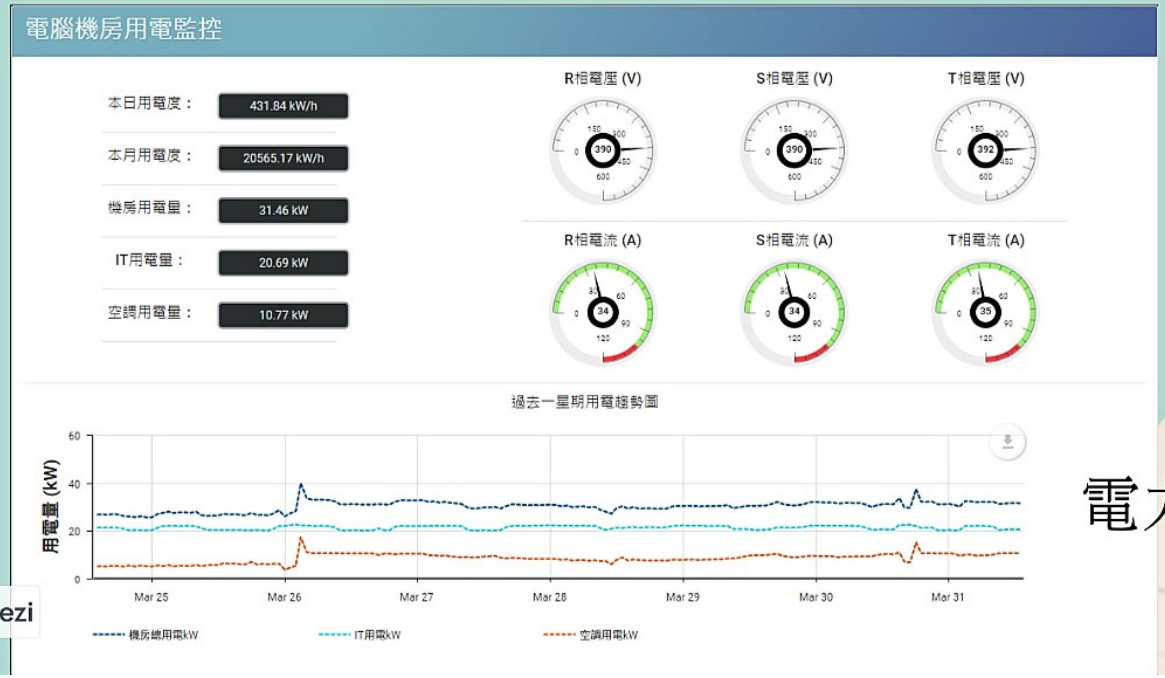
Prezi

記錄溫度變化，有助於預警設備異常狀況 5.4

Prezi

電力系統 5.9





UPS

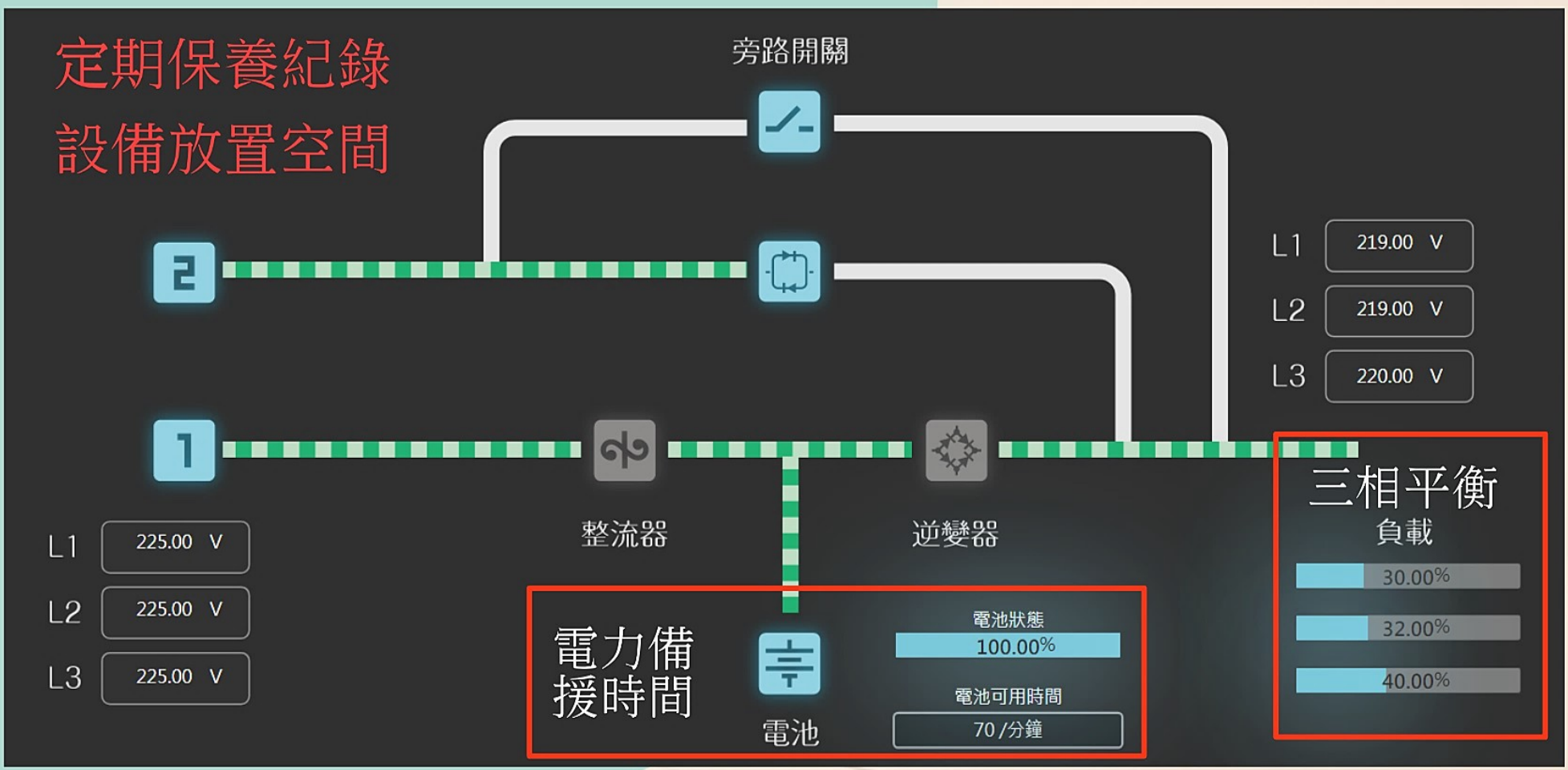
發電機

接地系統

電力監控是機房節能的第一步

Prezi

不斷電系統之維護重點



Prezi

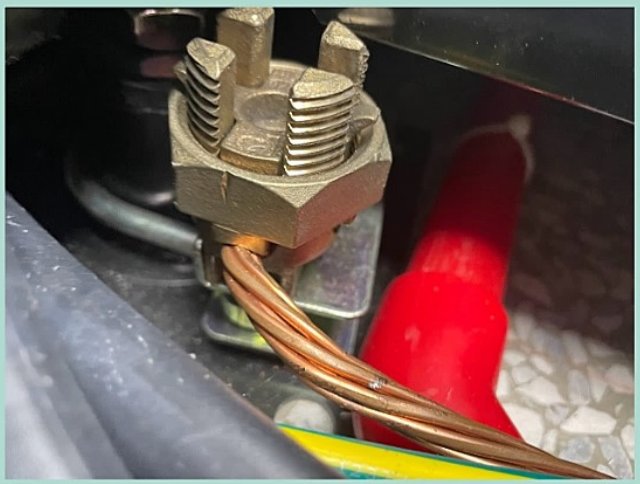
發電機之維護重點

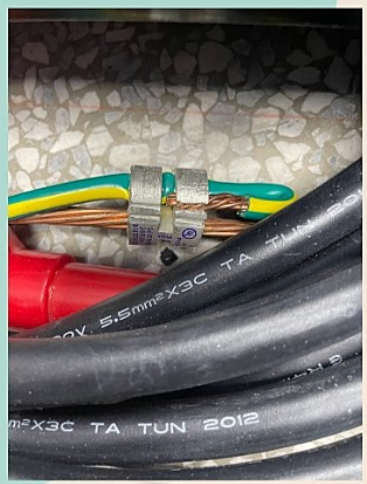
自動切換
定期維護
油量監測
有載運轉測試

Prezi

等電位接地系統配置

透過以建築物本身之等電位接地系統配置，降低建築物內可能出現的電位差以確保人員安全





Prezi

消防系統之維護重點

5.8

定期申報及維護(有效性確認)
選擇適當的滅火設備
C02 海龍 FM200 氫氣

Prezi

其他環境設備

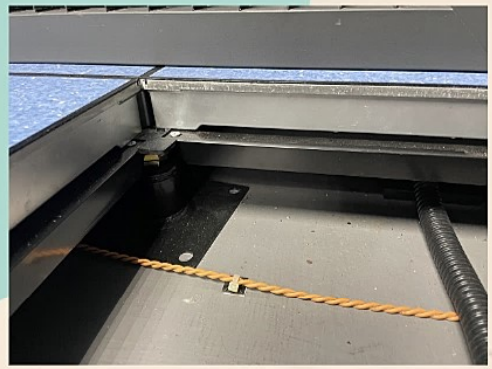
CCTV 監視設備 5.3

門禁管理設備 5.1 5.2

設備進出登記 5.7 5.12

人員進出登記 5.6

漏液偵測



換氣系統

Prezi

伺服器設備維護作業

定期帳號清查作業　5.25 5.26

網站、系統弱點掃描、資安健診　5.19

鐘訊同步設定

Web Server Https 通訊協定　5.23

Prezi

儲存設備之管理維護

備份政策制定 (RPO)　5.21 5.22

設備異常告警(Log Review)

備份結果通知

Prezi

網路設備之維護

建立網路架構圖

管理權限

設定檔之備份

防火牆政策清查

IP派送與管理
網路區隔配置 5.16 5.29

遠端連線管理
(RDP、Anydesk) 5.30

資安設備

線路管理

無線網路

Prezi

資安設備

防火牆&入侵偵測系統

網頁防火牆

資料庫稽核系統

Prezi

防火牆

FW_Policy

- 應採用正面表列
- 避免開啟RDP 等遠端桌面連入
- 防火牆政策的申請(S_IP、D_IP、Port_NO、Time)
- 防火牆政策的定期清查
- 防火牆政策群組化分類
- 特殊連線作業宜再定義可連線時段

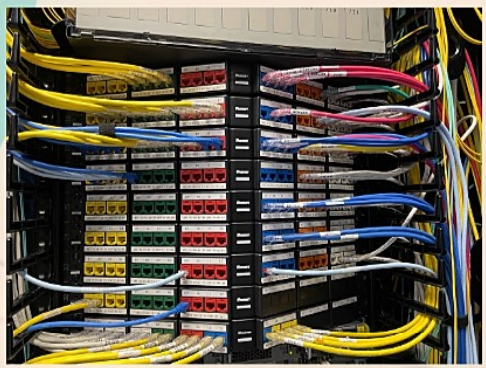
Prezi

項目	來源IP	目的IP	連線Port	備註
1	Any	140.120.X.1	Tcp_80、Tcp_443	
2	Any	140.120.X.2	Tcp_80、Tcp_443	
3	Any	140.120.X.3	Tcp_80、Tcp_443、Tcp_8080	
4	168.1.1.1	140.120.X.3	Tcp_1433	
5	Any	140.120.X.4	Tcp_8080	

項目	來源IP	目的IP	連線Port	備註
1	Any	140.120.X.1 140.120.X.2 140.120.X.3	Tcp_80、Tcp_443	
2	Any	140.120.X.3 140.120.X.4	Tcp_8080	
3	168.1.1.1	140.120.X.3	Tcp_1433	

Prezi

良好的線路管理提供高可靠度的網路服務及快速的故障排除 5.10



Prezi

無線網路管理重點

5.29　5.30

須提供具備驗證機制之無線環境

無線網路使用者之連線限制

Thin AP / Fat AP 特性

Prezi

個人設備之管理

可攜式電腦設備之管理 5.13 5.24

作業系統之版本、防毒軟體更新、軟體授權 5.17 5.18 5.19 5.20

NB及平板電腦之管理 5.13 5.31

Prezi

其他配合作業項目

演練作業　5.22

重大異動及變更管理　5.33

危害國家資通安全設備清查及對應作法　5.35 5.36

人員資訊安全管理之落實　5.15 5.27 5.28

資通設備報廢流程　5.14

資安通報平台　5.34

Prezi

稽核重點

5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢?

5.22備份資料是否定期回復測試，以確保備份資料之有效性?

5.19是否定期執行各項系統漏洞修補程式?

5.5各項安全設備是否定期檢查? 同仁有否施予適當的安全設備使用訓練?

5.34是否可即時取得系統弱點的資訊並作風險評估及採取必要措施?

Prezi

總結

硬體配置及規劃宜整體規劃

防火牆規則應重整並定期審查

資安風險及弱點應盡速完成修補

落實日常巡檢紀錄

Prezi