遠離校務系統遭駭與個資外洩
-
IBM Guardium 資料稽核保護與合規性安全

國立臺中科技大學資訊管理系 專任教授
柯志坤

內容大綱

1. 現行教育單位遵循的資料稽核與資料保護政策
2. 資安稽核實例介紹
3. 實務需求與省思
4. 總結

現行資料稽核與保護政策

- 資通安全管理法（107/5/11制定、107/6/6公布、108/1/1施行）
  - 可由全國法規資料庫查詢
    https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297

現行資料稽核與保護政策

- 高等教育深耕計畫第二期 – 三、主冊專章（資安強化）
  - 由政府（教育部）提供經費補助，落實資通安全法於教育單位
  - 工作要項-管理面
    - 資通系統責任分級及防護基準(1次/年)
    - 資訊安全管理系統之導入，聘任資通安全專責人員
    - 內部資通安全稽核(1次/2年)
    - 業務持續運作演練(1次/年)
    - 限制使用危害國家資通安全產品
  - 工作要項-技術面
    - 安全性檢測(2次/年)
    - 資通安全健診/滲透測試(1次/2年)
  - 工作要項-認知與訓練
    - 資通安全防護
    - 資通安全教育訓練
    - 資通安全專業證照及職能訓練證書

現行資料稽核與保護政策

- 教育單位校際現況
  - 普遍與業界資通安全顧問公司合作，導入資通安全稽核並通過國際標準認證取得資安 ISO27001 / 個資 ISO27701證書，滿足政府（教育部）對於落實資通安全管理法於教育單位之各項施行要求
  - 層級由資訊管理單位拉高位階至全校範疇
  - 要做到校級全面性資安管理仍是一項重大挑戰
    - 各校組織架構多元，經費來源與挹注比例
    - 組織單位的重視程度與信任
    - 面對法規與時俱進的修正，技術面是否能對應跟上
    - 人員的資安認知與素養建立
    - 業界顧問公司協助認證依責任區域範圍計價

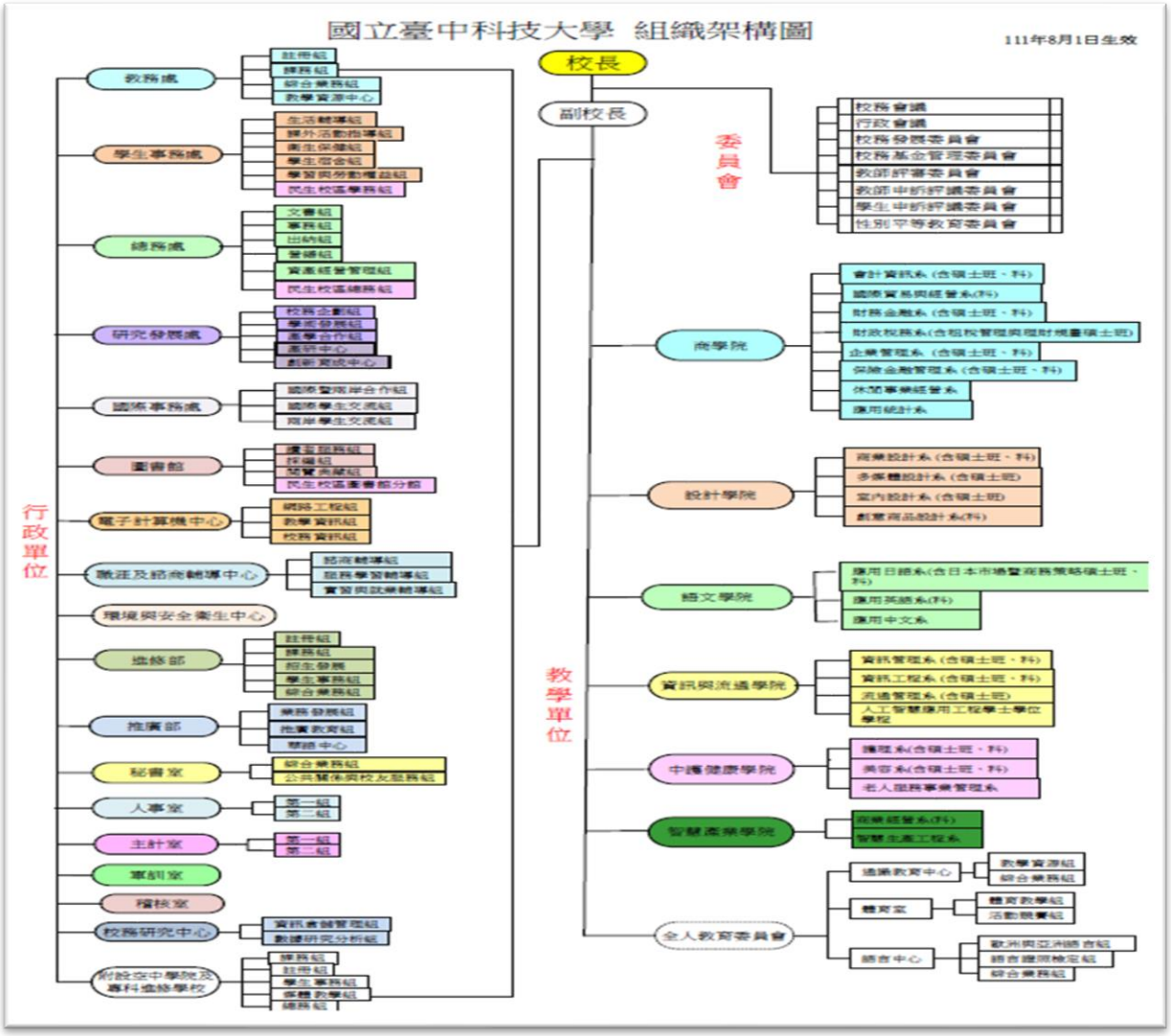
學界資安稽核實例-臺中科大

- 以國立臺中科技大學落實全校性資安稽核為實例，盤點全校性組織架構
- 設置專責人員綜理與推動資安業務：

副校長：資通安全長

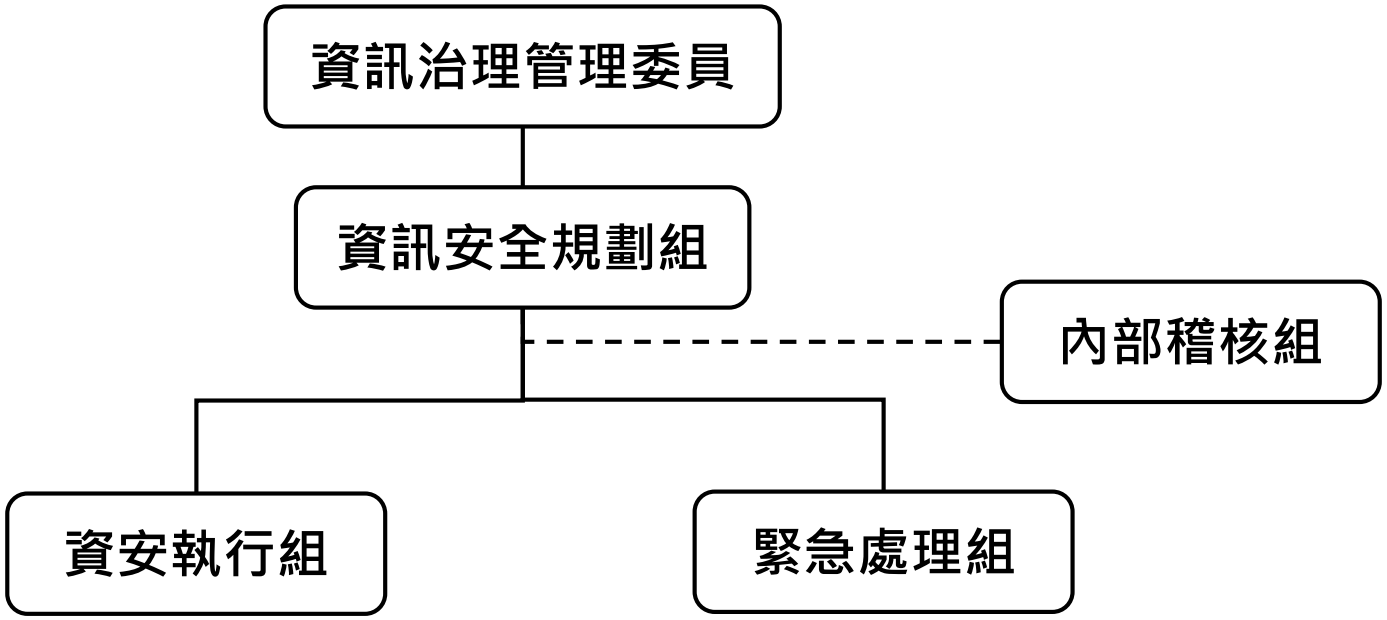
電算中心主管：執行秘書

各單位一級主管：資訊治理委員會成員



學界資安稽核實例-臺中科大

- 基於資訊安全管理系統 ISO 27001（Information Security Management System，ISMS）架構，建立全校性資安管理四階文件，依據資訊安全組織程序書所設置的資通安全組織架構：



學界資安稽核實例-臺中科大

- 對資通安全組織進行人員編制，原則上由資訊中心人員綜理執行大部分的資通安全業務，再由資訊治理委員會成員之教學與行政單位主管協助全性校資通安全業務推動：

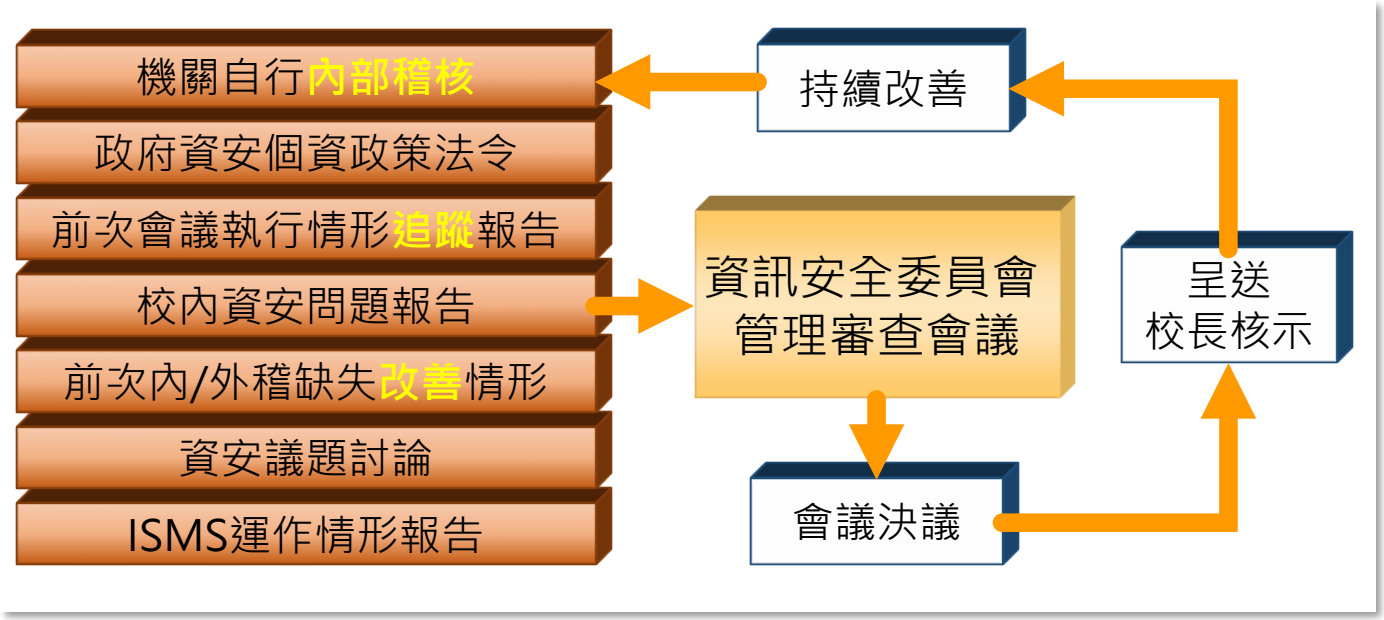
	職務	職稱	姓名	
資訊治理管理委員會	資訊安全長	副校長	陳	去識別化
	委員	秘書室主任祕書	李	
	委員	教務長	陳	
	委員	學務長	李	
	委員	總務長	林	
	委員	研發長	王	
	委員	人事主任	鄭	
	委員	主計主任	周	
	委員	進修部校務主任	魏	
	委員	空中學院校務主任	葉	
	委員	軍訓室主任	陳	
	委員	推廣部主任	林	
	委員	電算中心主任	柯	
	委員	圖書館館長	戴	
	委員	校務研究中心中心主任	黃	
	委員	稽核室主任	黃	
	委員	國際事務長	嚴	
	委員	職涯中心主任	李	
	委員	語言中心主任	程	
	委員	體育室主任	吳	
	委員	環境與安全衛生中心中心主任	藍	
	委員	通識教育中心主任	韓	
	委員	商學院院長	李	
	委員	資訊與流通學院院長	黃	
	委員	中護健康學院院長	盧	
	委員	智慧產業學院學院院長	林	
	委員	設計學院院長	蕭	
	委員	語文學院院長	李	

	職務	職稱	姓名	
資訊安全規劃小組	委員兼召集人	電算中心主任	柯	去識別化
	委員	教學資訊組組長	林	
	委員	網路工程組組長	張	
	委員	校務資訊組	林	
資安執行組	組長	網路工程組組長	張	
	組員	網路工程組	林	
	組員	教學資訊組	張	
	組員	教學資訊組	林	
	組員	教學資訊組	許	
	組員	網路工程組	李	
	組員	網路工程組	洪	
	組員	校務資訊組	邱	
	組員	校務資訊組	郭	
	組員	校務資訊組	劉	
	組員	校務資訊組	陳	
	組員	校務資訊組	巫	
	組員	校務資訊組	鄭	
	組員	校務資訊組	張	
	組員	校務資訊組	廖	
	組員	校務資訊組	陳	
	組員	校務資訊組	陳	

	職務	職稱	姓名	
內部稽核組	組員	教學資訊組	張	去識別化
	組員	校務資訊組	郭	
	組員	網路工程組	林	
	組員	網路工程組	李	
	組員	校務資訊組	巫	
	組員	校務資訊組	陳	
緊急處理組	組長	校務資訊組	林	
	組員	校務資訊組	陳	
	組員	校務資訊組	郭	
	組員	教學資訊組	張	
	組員	網路工程組	林	
	組員	網路工程組	李	
資通安全專責人員	組員	教學資訊組	張	
	組員	網路工程組	林	

學界資安稽核實例-臺中科大

- 資通安全組織運作情形
  - 資安管理與校級內控制度融合，落實自我監督機制（每年1次）
  - 管理審查會議（每年平均2次）



歷年管理審查會議

- 104年 12月
- 105年 5月、12月
- 106年 6月、10月
- 107年 6月、12月
- 108年 6月、12月
- 109年 6月、9月
- 110年 1月、8月
- 111年 1月、10月
- 112年 1月

學界資安稽核實例-臺中科大

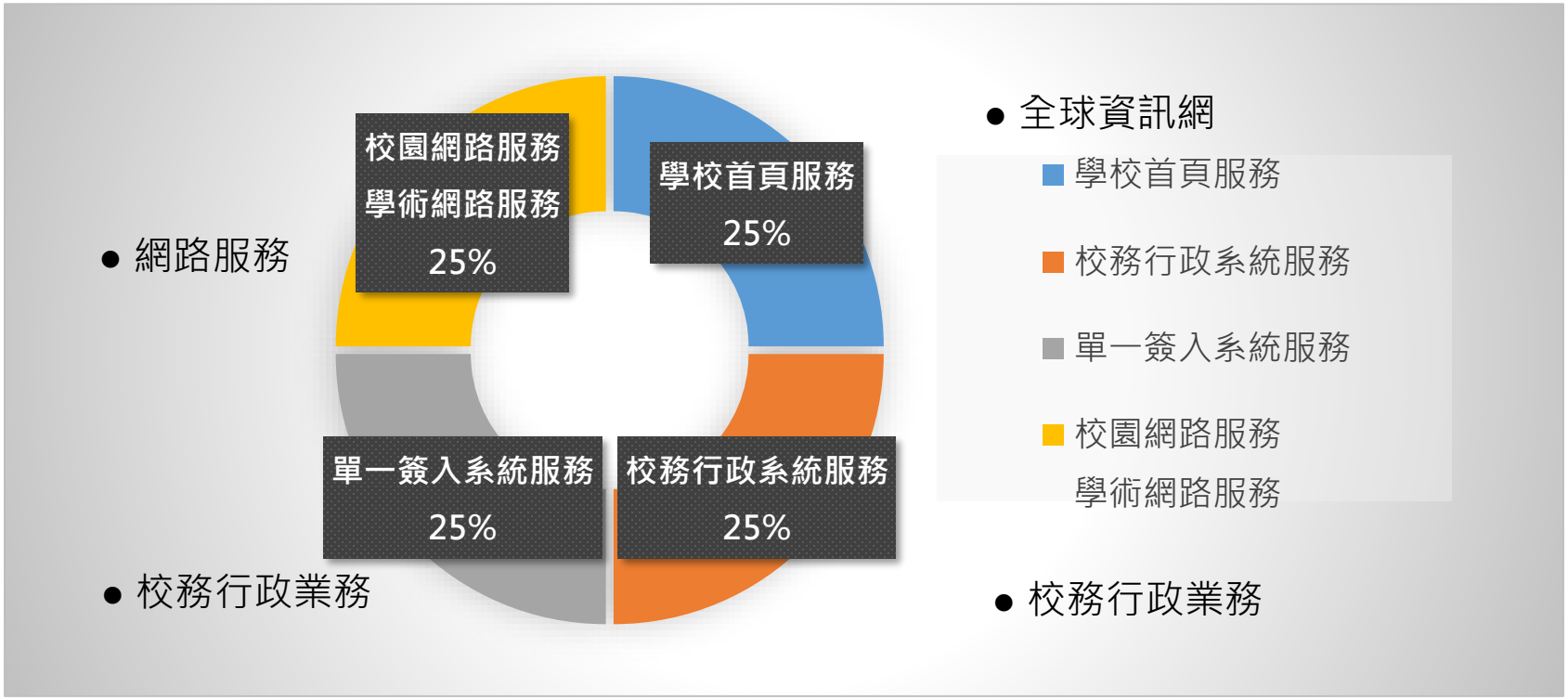
- 重要資安歷程

- 軟硬體建置朝完善資訊安全管理制度

98年3月30日	99年4月	99年6月1日	105年9月	106年9月	107年10月	108年10月	109年11月	111年6月
• 「資訊安全推行委員會」第一次會議，會中通過「國立臺中技術學院資訊安全政策」，改名科大後，本政策更名為「國立臺中科技大學資訊安全政策」	• ISO27001第二階段正評，並獲得驗證通過	• 正式取得ISO27001：2005驗證證書	• ISO27001：2013驗證通過	• ISO27001：2013複評通過	• ISO27001：2013複評通過	• ISO27001：2013複評通過	• ISO27001：2013複評通過	• ISO27001：2013續評通過

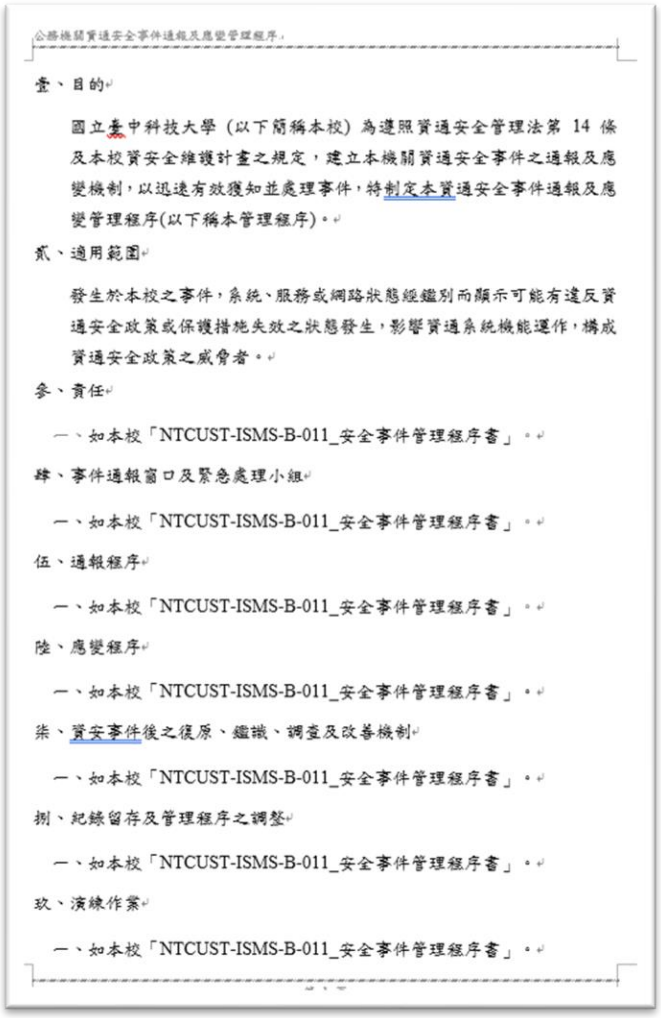
學界資安稽核實例-臺中科大

- 盤點校級資通系統（三大核心資通系統）



學界資安稽核實例-臺中科大

- 資安事件通報應變，通報流程清楚，彙整分析，防範未然



公務機關資通安全事件通報及應變管理程序。

壹、目的

國立臺中科技大學（以下簡稱本校）為遵照資通安全管理法第 14 條及本校資安全維護計畫之規定，建立本機關資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序(以下稱本管理程序)。

貳、適用範圍

發生於本校之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

參、責任

一、如本校「NTCUST-ISMS-B-011_安全事件管理程序書」。

肆、事件通報窗口及緊急處理小組

一、如本校「NTCUST-ISMS-B-011_安全事件管理程序書」。

伍、通報程序

一、如本校「NTCUST-ISMS-B-011_安全事件管理程序書」。

陸、應變程序

一、如本校「NTCUST-ISMS-B-011_安全事件管理程序書」。

柒、資安事件後之復原、鑑識、調查及改善機制

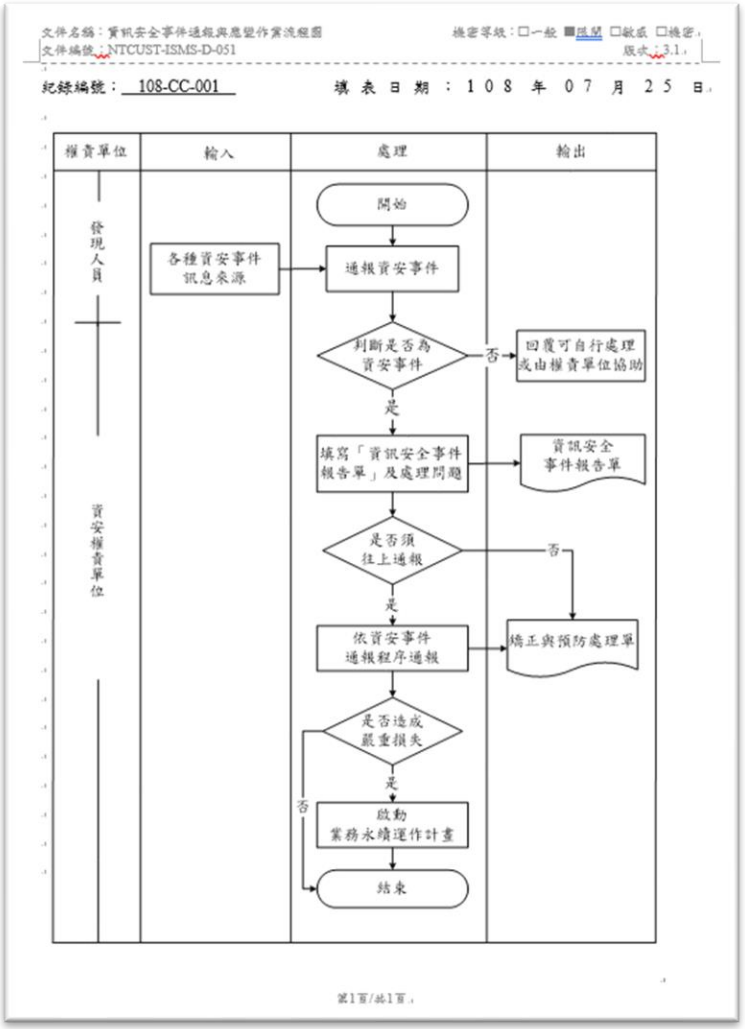
一、如本校「NTCUST-ISMS-B-011_安全事件管理程序書」。

捌、紀錄留存及管理程序之調整

一、如本校「NTCUST-ISMS-B-011_安全事件管理程序書」。

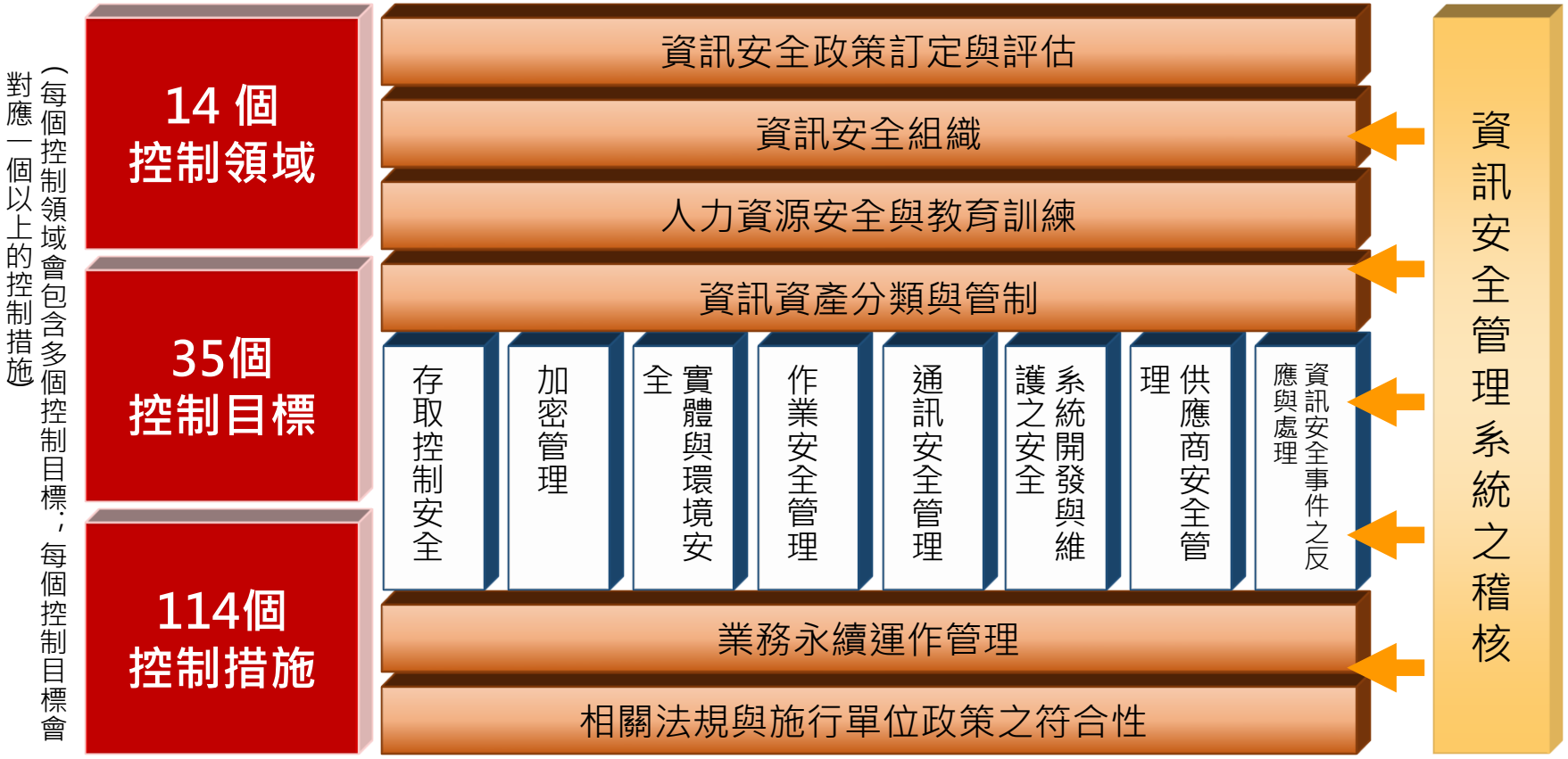
玖、演練作業

一、如本校「NTCUST-ISMS-B-011_安全事件管理程序書」。



學界資安稽核實例-臺中科大

- 資訊安全管理架構
  - ISO27001資訊安全與ISO27701個人資訊管理標準管理審查相關項目報告



學界資安稽核實例-臺中科大

- 降低資安事件發生
  - 因應行政院國家資通安全相關規定，持續推動導入政府組態基準(Government Configuration Baseline，GCB)設定，強化機關資通訊終端設備之資安能力，降低資安事件發生機率，後期公文通知，教育單位為非必要性實施

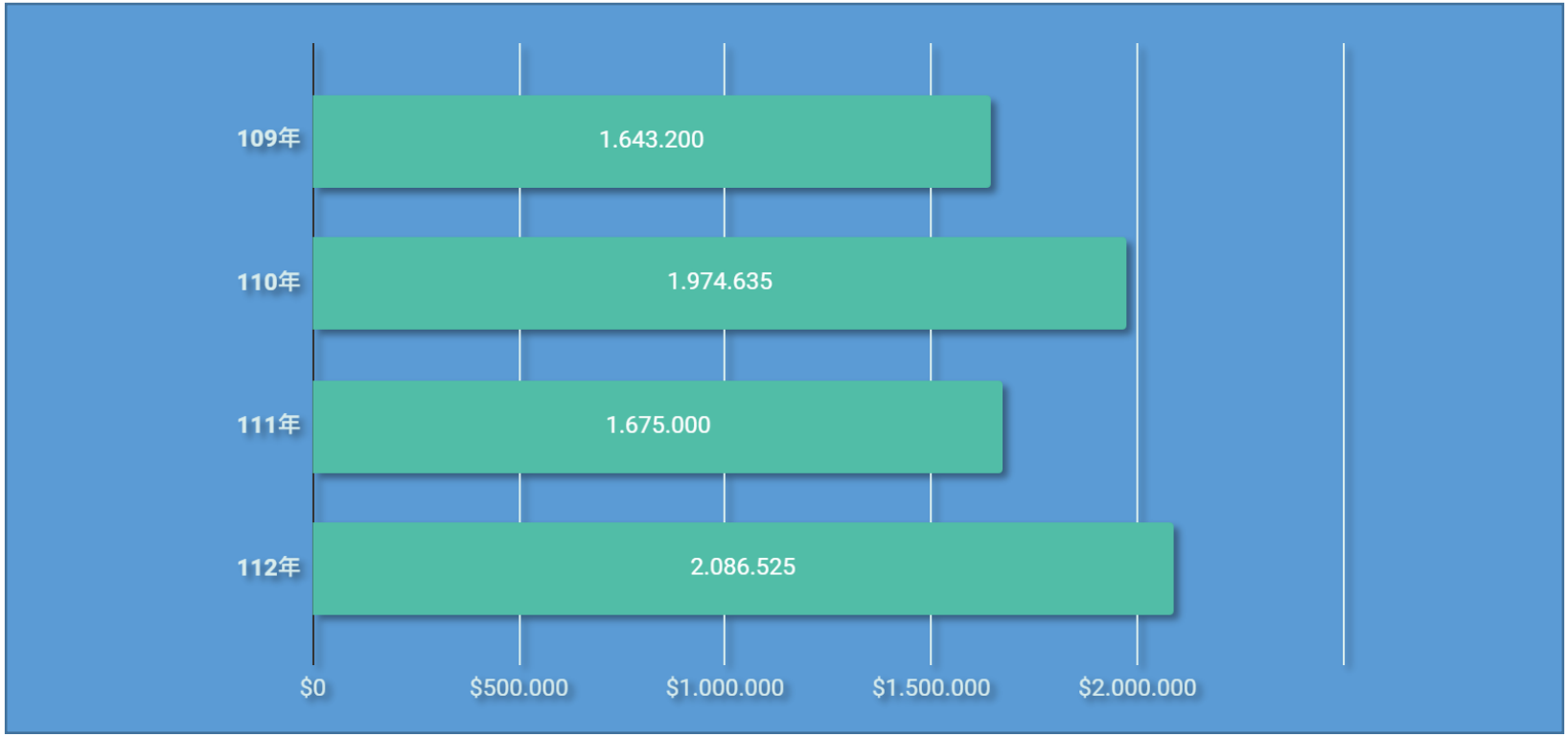
維護GCB管理系統

1. 持續維護已建置的GCB管理系統。
2. 目前共有220台個人電腦已導入GCB（含文書組46台電腦）。
3. 持續維護GCB組態範本。

  - 但有公文通知查核學校是否有落實資通安全弱點通報系統(Vulnerability Analysis and Notice System，VANS)，要求回報結果。VANS主要是結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實資通安全管理法之資產盤點與風險評估應辦事項

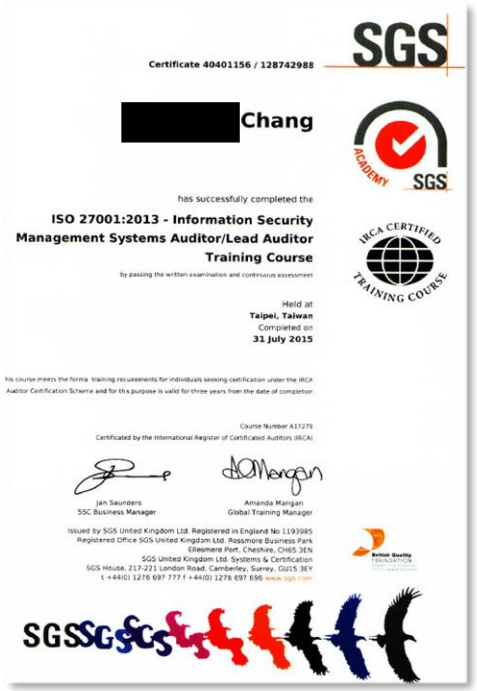
學界資安稽核實例-臺中科大

- 歷年資通安全經費配置：
  - 資安經費占機關資訊設備經費比1.7%，112年計入高教深耕計畫補助
  - 歷年資安經費編列偏高，主要用於提升人員認知素養，如圖所示



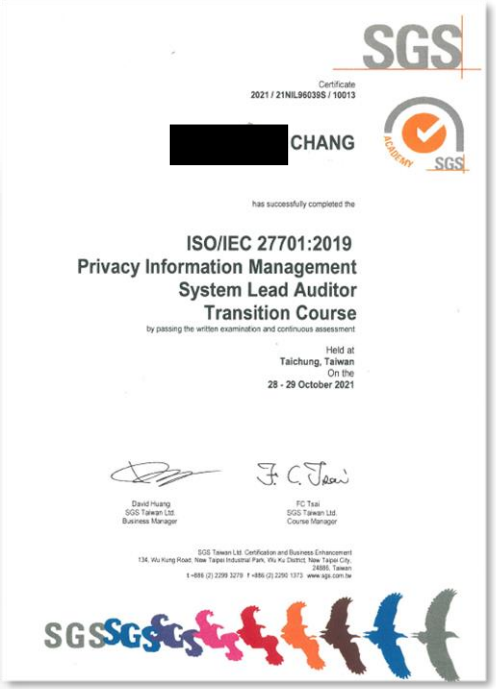
學界資安稽核實例-臺中科大

- 資安專職人員確實透過受訓並取得證書，佐證能力適任



▲ISO27001v2013主導稽核員證照

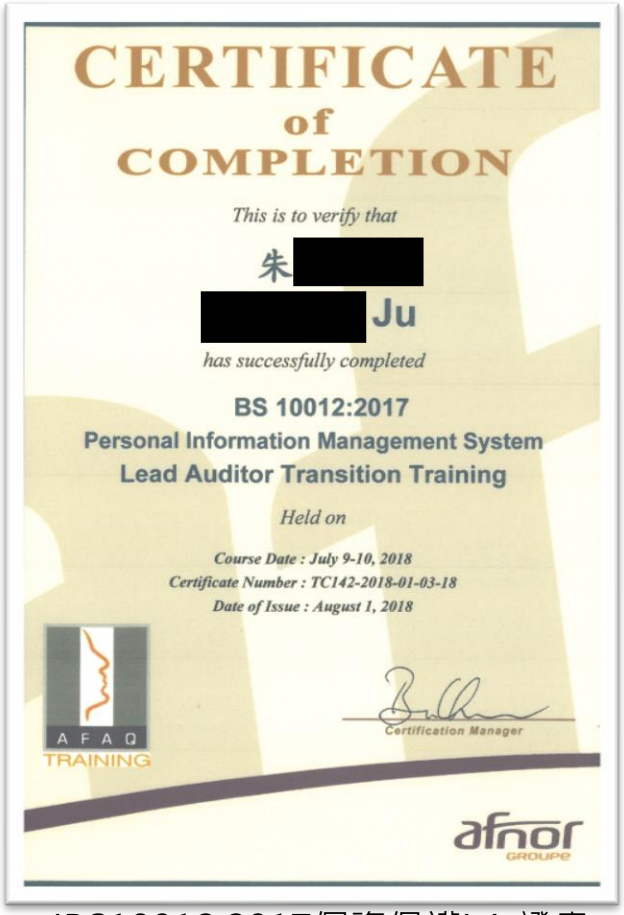
▲通過教育體系資通安全專業課程評量



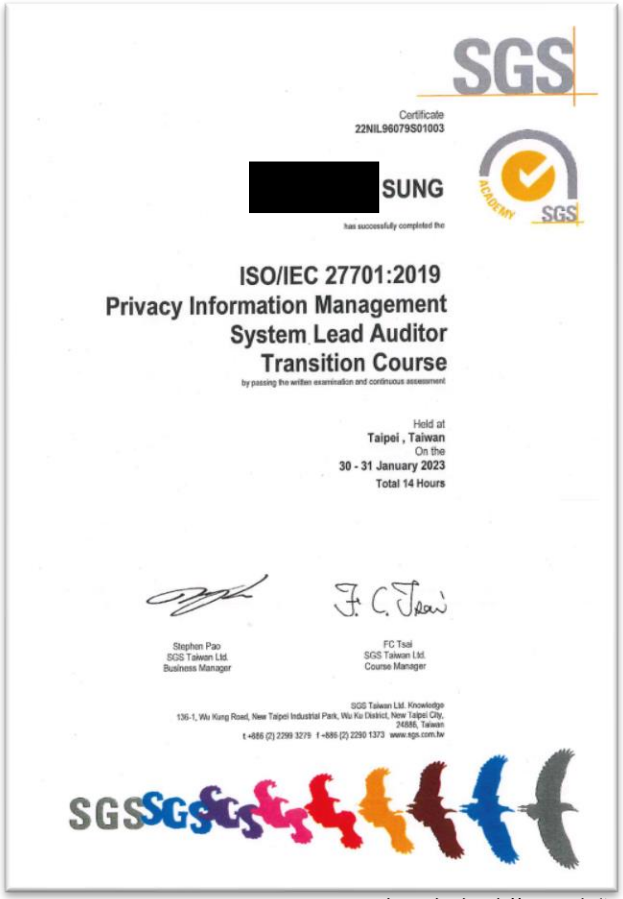
▲ISO27701v2019主導稽核員證照

學界實例-臺中科大

- 非資安專職人員參訓取證



▲IBS10012:2017個資保護LA 證書

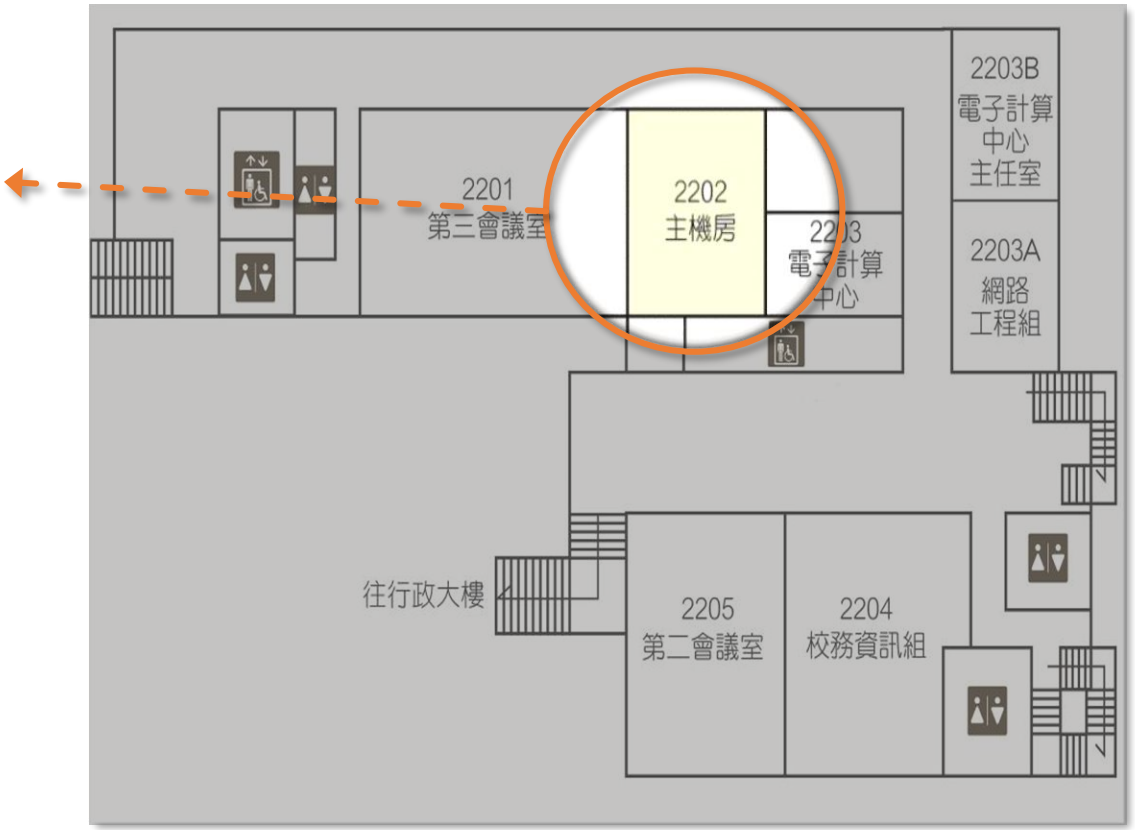


▲ISO27701:2019個資保護LA證書

學界資安稽核實例-臺中科大

- 資訊中心機房座落位置

臺中科大主機房
位於資訊大樓2樓



學界資安稽核實例-臺中科大

- 機房環境

學界資安稽核實例-臺中科大

- 機房環控
  - 空調
  - 水泵
  - 水塔
  - 溫度
  - 濕度
  - UPS
  - 漏水
  - 消防

學界資安稽核實例-臺中科大

- 機房環控-空調冷熱通道

學界資安稽核實例-臺中科大

- 資安認證檢核
  - 內稽：整合內控查核受稽單位業務是否符合資安規範
  - 管理審查會議：依法規變動與稽核審查實際情況進行調整
  - 違規缺失：若稽核過程中發現，開立矯正通知單限期改善
  - 外稽：由第三方公正單位進行稽核
  - 取證：若稽核過程與結果沒有發生缺失，或通知缺失已改善，將送公正單位認證，申請取得ISO27001資安認證通過證明。

註：目前國內教版已經停止協助教育單位認證，現行教育單位通常與業界資安顧問公司合作，協助取得資安國際認證。

學界資安稽核實例-臺中科大

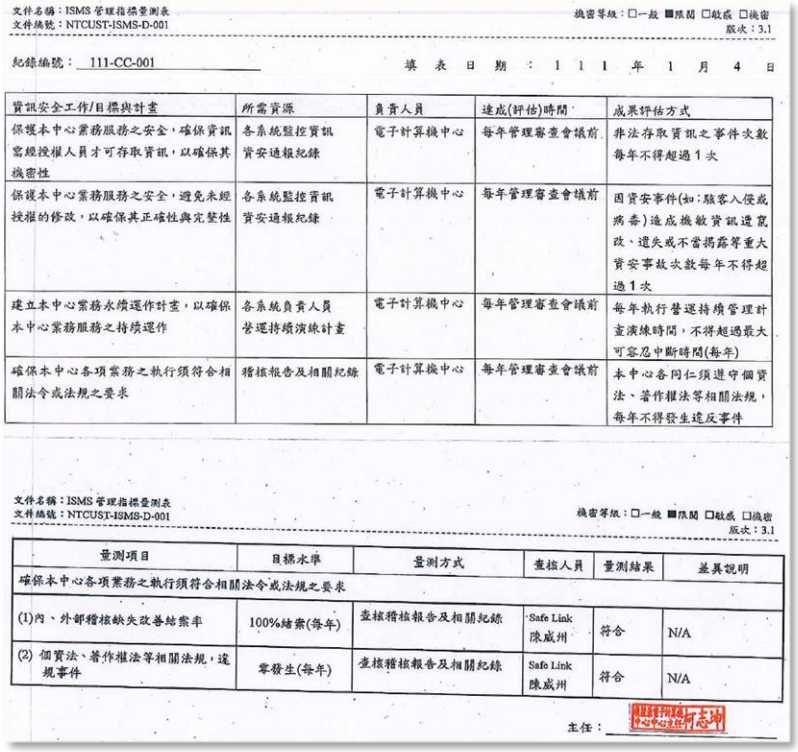
- 資安政策內容、目標
  - 四大量化指標政策

01 保護業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。

02 建立業務永續運作計畫，以確保本中心業務服務之持續運作。

03 保護業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

04 確保本中心各項業務之執行須符合相關法令或法規之要求。



文件名稱：ISMS 管理指標量測表　機密等級：□一般 ■限閱 □敏感 □機密
文件編號：NTCUST-ISMS-D-001　版次：3.1

紀錄編號：111-CC-001　填表日期：111年1月4日

資訊安全工作/目標與計畫	所需資源	負責人員	達成(評估)時間	成果評估方式
保護本中心業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性	各系統監控資訊資安通報紀錄	電子計算機中心	每年管理審查會議前	非法存取資訊之事件次數每年不得超過1次
保護本中心業務服務之安全，避免未經授權的修改，以確保其正確性與完整性	各系統監控資訊資安通報紀錄	電子計算機中心	每年管理審查會議前	因資安事件(如：駭客入侵或病毒)造成機敏資訊遭竄改、遺失或不當揭露等重大資安事故次數每年不得超過1次
建立本中心業務永續運作計畫，以確保本中心業務服務之持續運作	各系統負責人員營運持續演練計畫	電子計算機中心	每年管理審查會議前	每年執行營運持續管理計畫演練時間，不得超過最大可容忍中斷時間(每年)
確保本中心各項業務之執行須符合相關法令或法規之要求	稽核報告及相關紀錄	電子計算機中心	每年管理審查會議前	本中心各同仁須遵守個資法、著作權法等相關法規，每年不得發生違反事件

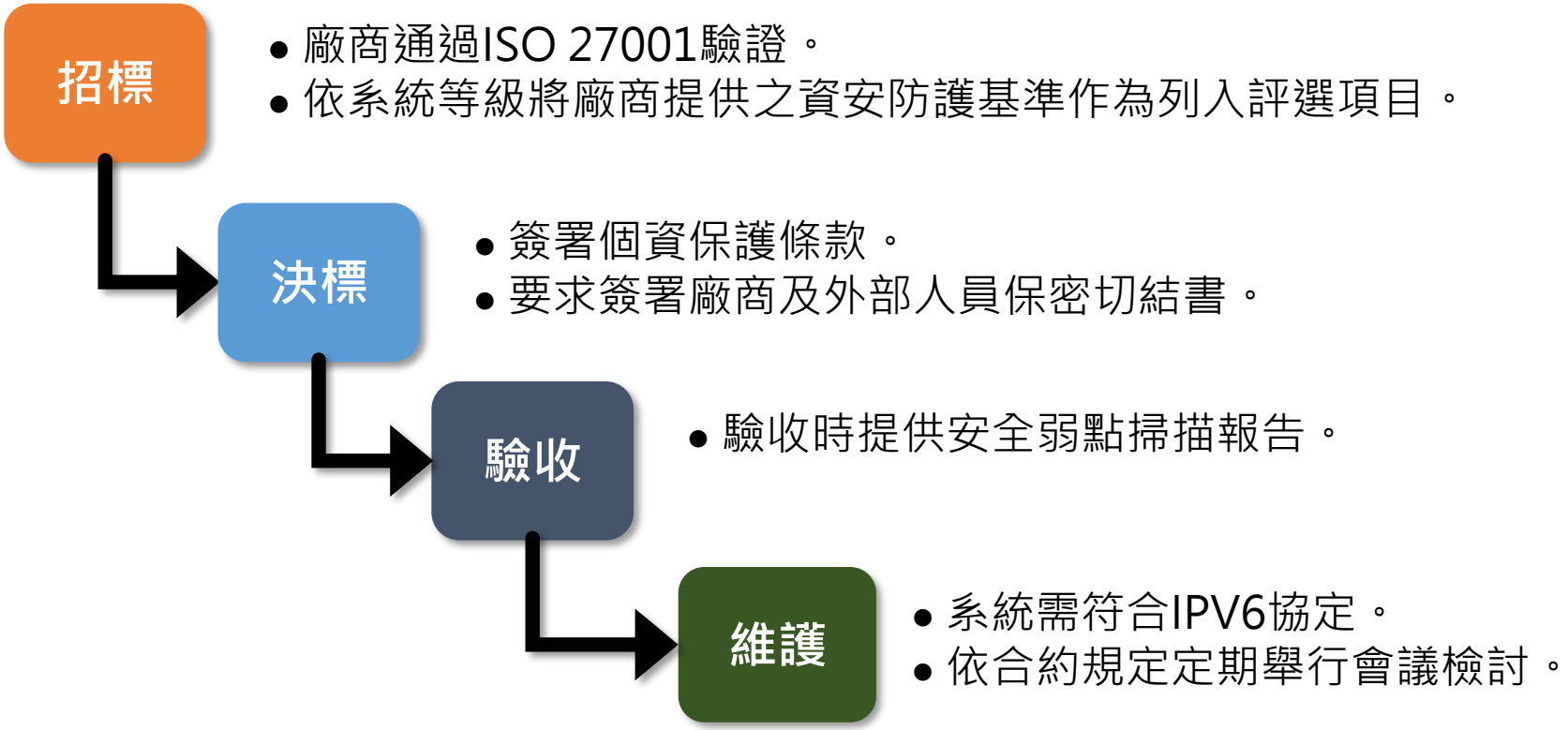
文件名稱：ISMS 管理指標量測表　機密等級：□一般 ■限閱 □敏感 □機密
文件編號：NTCUST-ISMS-D-001　版次：3.1

量測項目	目標水準	量測方式	查核人員	量測結果	差異說明
確保本中心各項業務之執行須符合相關法令或法規之要求					
(1)內、外部稽核缺失改善結案率	100%結案(每年)	查核稽核報告及相關紀錄	Safe Link 陳威州	符合	N/A
(2) 個資法、著作權法等相關法規，違規事件	零發生(每年)	查核稽核報告及相關紀錄	Safe Link 陳威州	符合	N/A

主任：

學界資安稽核實例-臺中科大

- 委外廠商管理
  - 38個查核項目管理委外廠商。
  - 各處室資訊委外作業，遵循「委外廠商資通安全要求查核表」。



學界資安稽核實例-臺中科大

- 資訊安全與個人資料保護教育訓練課程

人員類別	日期	教育訓練課程名稱	時數	梯次	應達成人數	已達成人數	達成率
一般主管	03/25	111年度臺灣學術網路防範惡意電子郵件社交工程演練宣導教育訓練	3	1	50	50	100.00%
資安專職人員	03/28	111年度臺灣學術網路防範惡意電子郵件社交工程演練宣導教育訓練	3	1	33	33	100.00%
一般使用者	09/30	個人資料保護法與案例宣導	3	1	105	50	47.62%
資安專職人員	08/30 (上午及下午)	個人資料盤點與風險評鑑實務 (含個資盤點與風險評鑑管理平台線上操作/電腦教室上課)	3	2	68	40	58.82%
資安專職人員	10/07	各單位導入ISMS以全機關為範圍教育訓練課程 (含資安設備盤點與管理線上操作/電腦教室上課)	3	1	64	35	54.69%
資安專職人員	10/07	各單位資通安全責任等級分級教育訓練課程 (含資安設備盤點與管理線上操作/電腦教室上課)	3	1	68	31	45.59%
資訊人員	10/28	個人資料保護管理制度及內部稽核實務課程	3	1	82	36	43.9%

學界資安稽核實例-臺中科大

- 資通系統相關資訊資產風險評鑑

資產類別 \ 風險值	1	2	3	4	6	8	9	12	16	24	48	總計
通訊	0	4	0	4	4	8	0	10	0	0	0	30
資料	1	3	0	7	4	8	3	1	0	2	0	29
硬體	17	4	0	0	5	4	0	2	1	2	1	36
軟體	1	10	2	7	2	1	0	2	2	0	0	27
人員	1	4	2	3	0	9	0	7	0	2	0	28
文件	2	1	2	6	1	1	0	3	0	0	0	16
環境	0	0	2	0	8	0	0	5	1	1	1	18
												184

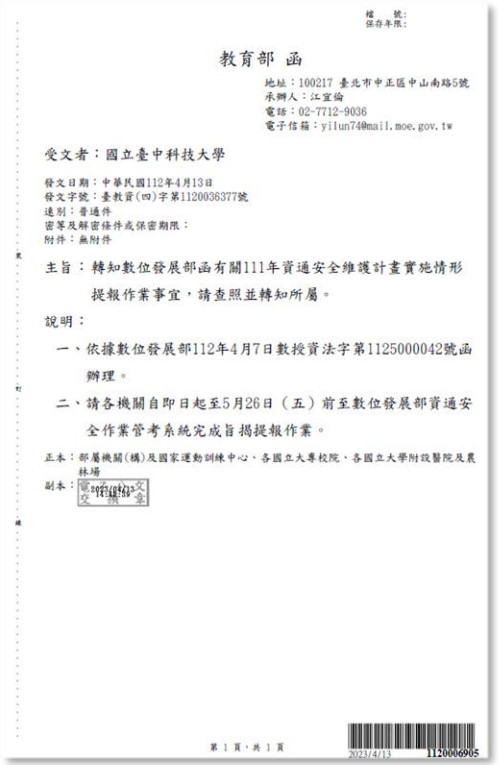
全校資訊資產共計112項，及鑑識出184項風險項目。

- **通訊類：30項**
- **資料類：29項**
- **硬體類：36項**
- **軟體類：27項**
- **人員類：28項**
- **文件類：16項**
- **環境類：18項**

可接受風險值，建議值為65（不含）以下。各項資訊資產風險值高於可接受風險值65（含）以上者，將於「風險改善計畫表」中提出風險控管之建議方案。本次未超過風險值.

學界資安稽核實例-臺中科大

- 落實核心資通系統業務衝擊分析



教育部 函

地址：100217 臺北市中正區中山南路5號
承辦人：江宜倫
電話：02-7712-9036
電子信箱：yilun74@mail.moe.gov.tw

受文者：國立臺中科技大學

發文日期：中華民國112年4月13日
發文字號：臺教資(四)字第1120036377號
速別：普通件
密等及解密條件或保密期限：
附件：無附件

主旨：轉知數位發展部函有關111年資通安全維護計畫實施情形提報作業事宜，請查照並轉知所屬。

說明：

一、依據數位發展部112年4月7日數授資法字第1125000042號函辦理。

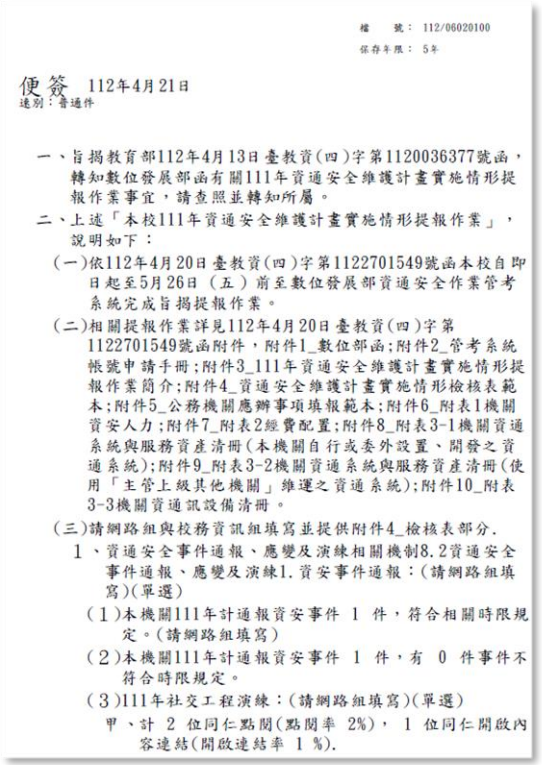
二、請各機關自即日起至5月26日（五）前至數位發展部資通安全作業管考系統完成旨揭提報作業。

正本：部屬機關(構)及國家運動訓練中心、各國立大專校院、各國立大學附設醫院及農林場

副本：

第 1 頁，共 1 頁

2023/4/13 1120006905



檔　號：112/06020100
保存年限：5年

便簽　112年4月21日
速別：普通件

一、旨揭教育部112年4月13日臺教資(四)字第1120036377號函，轉知數位發展部函有關111年資通安全維護計畫實施情形提報作業事宜，請查照並轉知所屬。

二、上述「本校111年資通安全維護計畫實施情形提報作業」，說明如下：

(一)依112年4月20日臺教資(四)字第1122701549號函本校自即日起至5月26日（五）前至數位發展部資通安全作業管考系統完成旨揭提報作業。

(二)相關提報作業詳見112年4月20日臺教資(四)字第1122701549號函附件，附件1_數位部函;附件2_管考系統帳號申請手冊;附件3_111年資通安全維護計畫實施情形提報作業簡介;附件4_資通安全維護計畫實施情形檢核表範本;附件5_公務機關應辦事項填報範本;附件6_附表1機關資安人力;附件7_附表2經費配置;附件8_附表3-1機關資通系統與服務資產清冊(本機關自行或委外設置、開發之資通系統);附件9_附表3-2機關資通系統與服務資產清冊(使用「主管上級其他機關」維運之資通系統);附件10_附表3-3機關資通訊設備清冊。

(三)請網路組與校務資訊組填寫並提供附件4_檢核表部分.

1、資通安全事件通報、應變及演練相關機制8.2資通安全事件通報、應變及演練1.資安事件通報：(請網路組填寫)(單選)

(1)本機關111年計通報資安事件 1 件，符合相關時限規定。(請網路組填寫)

(2)本機關111年計通報資安事件 1 件，有 0 件事件不符合時限規定。

(3)111年社交工程演練：(請網路組填寫)(單選)

甲、計 2 位同仁點閱(點閱率 2%)， 1 位同仁開啟內容連結(開啟連結率 1 %).

指標(如來函附件)落實執行並於112年5月5日前彙整所填資料，上傳數位部管考系統彙辦。

四、此訊息擬於本校網站公告方式強化宣導，文陳閱後存查。

會辦單位：電子計算機中心教學資訊組、電子計算機中心網路工程組、電子計算機中心校務資訊組

第一層決行

承辦單位　　會辦單位　　決行

學界資安稽核實例-臺中科大

- 實地(第三方)稽核與改善
  - 109年實地稽核2項缺失（正式表單版本不一致、未建立外部廠商聯繫清單），已於109年年底前全數改善完畢。

文件名稱：矯正措施處理單　機密等級：□一般 ■限閱 □敏感 □機密
文件編號：NTCUST-ISMS-D-056　版次：3.0

紀錄編號：109-CC00-A01

提出單位	Afnor 驗證機關	提出人員	張[redacted]	提出日期	109 年 11 月 04 日
處理單位	電算中心	處理人員	張[redacted]	填寫日期	109 年 11 月 09 日

事件分類：
□主要不符合事項 □次要不符合事項 ■觀察事項 □建議事項

事件來源：
□內部稽核 ■外部稽核 □資訊安全事件 □自行提出 □其他

問題或缺失說明：查文件名稱：系統開發暨變更需求申請書，編號：NTCUST-ISMS-D-046，紀錄編號：109-cc40-038，填表日期：109 年 9 月 7 日，需求說明：現有系統功能修改。該表並紀錄「測試結果」：通過，並由委託單位承辦人林○○及單位主管李○○；交付驗收單位承辦人鄭○○及單位主管戴○○核章，與「系統開發與維護程序書」（版本 4.0, 發行日期：109.03.1）5.4.1.1 系統使用單位若有系統開發及維護申請時，應填寫「系統及程式新增、修改、維護申請書」並敘明理由；及 5.4.3.2 程式設計初步完成後，應準備「應用系統測試記錄表」通知申請單位進行聯合測試，並請申請單位於「應用系統測試記錄表」中填寫測試結果，之規定不相符。
另查文件名稱：應用系統測試記錄表，文件編號：NTCUST-ISMS-D-042，紀錄編號：102-cc40-001，系統名稱：英文檢定輔導系統，結果：正常，並有申請單位林○○及主管程○○，及覆核單位巫○○及主管黃○○核章。此為最後有紀錄之「應用系統測試記錄表」，未見 103 至 108 年「應用系統測試記錄表」。109 年起合併「「系統及程式新增、修改、維護申請書」及「應用系統測試記錄表」為「系統開發暨變更需求申請書」，然未好相關程序書修改相關書表名稱，建議依程序書執行或修改程序書書表名稱。

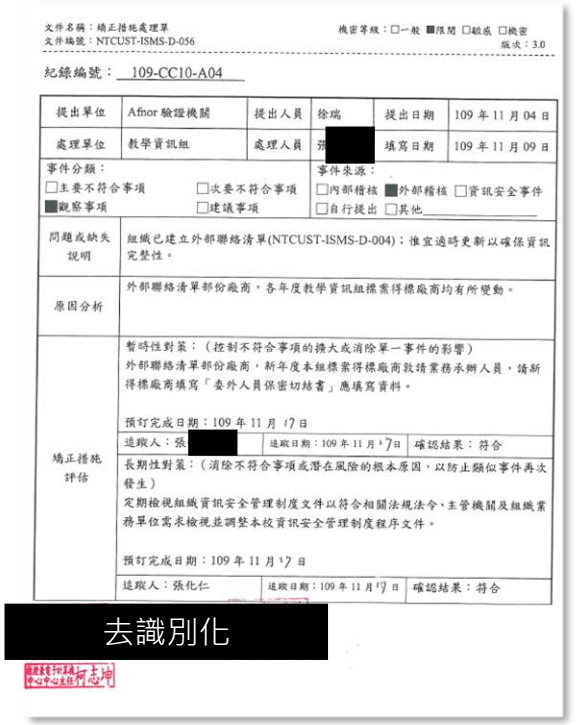
原因分析：經資訊安全規劃組確認後，稽核老師所述"「系統開發與維護程序書」（版本 4.0, 發行日期：109.03.1）5.4.1.1 系統使用單位若有系統開發及維護申請時，應填寫「系統及程式新增、修改、維護申請書」並敘明理由"為內容有誤版本，經查"修訂紀錄"，該份程序書已於 105/7/20，已將「系統及程式新增、修改、維護申請書」修改為「系統開發暨變更需求申請書」。

矯正措施評估：
暫時性對策：（控制不符合事項的擴大或消除單一事件的影響）
釐清「 NTCUST-ISMS-B-009 系統開發與維護程序書」最新版本為" V4.0" ，並將內容更換為正確內容版本。
預訂完成日期：109 年 11 月 10 日
追蹤人：張[redacted]　追蹤日期：109 年 11 月 10 日　確認結果：符合
長期性對策：（消除不符合事項或潛在風險的根本原因，以防止類似事件再次發生）
定期依據法規法令、主管機關、組織業務單位需求檢視並調整本校資訊安全管理制度程序文件，必要時進行調整以符合要求。
預訂完成日期：109 年 11 月 10 日
追蹤人：張化仁　追蹤日期：109 年 11 月 10 日　確認結果：符合

去識別化

第1頁/共 1 頁

本文件為國立臺中科技大學電子計算機中心專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。



文件名稱：矯正措施處理單　機密等級：□一般 ■限閱 □敏感 □機密
文件編號：NTCUST-ISMS-D-056　版次：3.0

紀錄編號：109-CC10-A04

提出單位	Afnor 驗證機關	提出人員	徐瑞	提出日期	109 年 11 月 04 日
處理單位	教學資訊組	處理人員	張[redacted]	填寫日期	109 年 11 月 09 日

事件分類：
□主要不符合事項 □次要不符合事項 ■觀察事項 □建議事項

事件來源：
□內部稽核 ■外部稽核 □資訊安全事件 □自行提出 □其他

問題或缺失說明：組織已建立外部聯絡清單(NTCUST-ISMS-D-004)；惟宜適時更新以確保資訊完整性。

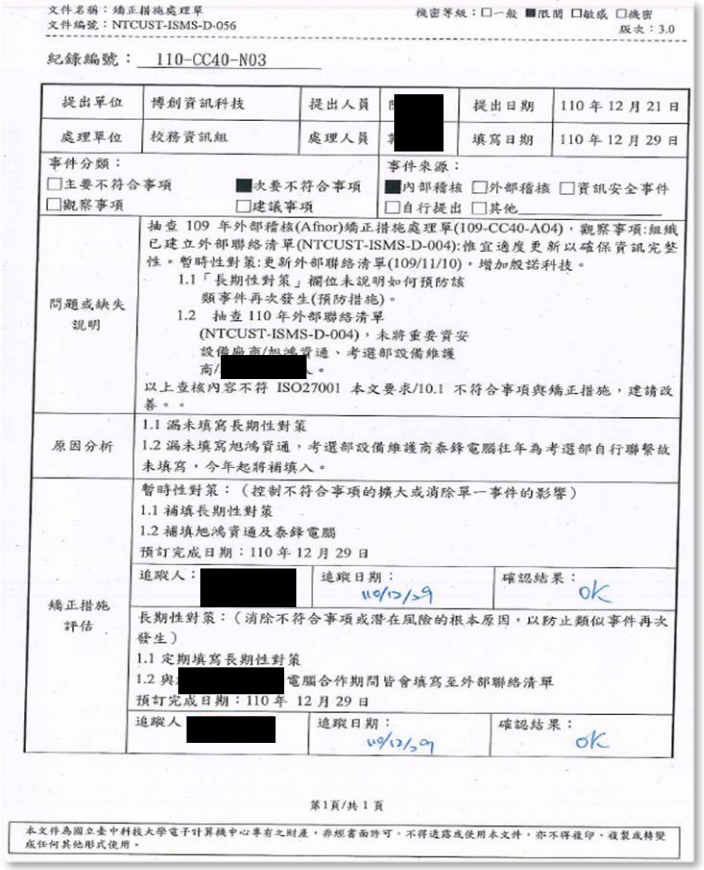
原因分析：外部聯絡清單部份廠商，各年度教學資訊組標案得標廠商均有所變動。

矯正措施評估：
暫時性對策：（控制不符合事項的擴大或消除單一事件的影響）
外部聯絡清單部份廠商，新年度本組標案得標廠商敦請業務承辦人員，請新得標廠商填寫「委外人員保密切結書」應填寫資料。
預訂完成日期：109 年 11 月 17 日
追蹤人：張[redacted]　追蹤日期：109 年 11 月 17 日　確認結果：符合
長期性對策：（消除不符合事項或潛在風險的根本原因，以防止類似事件再次發生）
定期檢視組織資訊安全管理制度文件以符合相關法規法令、主管機關及組織業務單位需求檢視並調整本校資訊安全管理制度程序文件。
預訂完成日期：109 年 11 月 17 日
追蹤人：張化仁　追蹤日期：109 年 11 月 17 日　確認結果：符合

去識別化

學界資安稽核實例-臺中科大

- 實地(第三方)稽核與改善
  - 110年實地稽核2項缺失（外部廠商聯繫清單未更新、預計汰除故障設備未列清冊），已於110年年底前全數改善完畢。



文件名稱：矯正措施處理單　機密等級：□一般 ■限閱 □敏感 □機密
文件編號：NTCUST-ISMS-D-056　版次：3.0

紀錄編號：110-CC40-N03

提出單位	博創資訊科技	提出人員	[redacted]	提出日期	110 年 12 月 21 日
處理單位	校務資訊組	處理人員	[redacted]	填寫日期	110 年 12 月 29 日

事件分類：□主要不符合事項 ■次要不符合事項 □觀察事項 □建議事項
事件來源：■內部稽核 □外部稽核 □資訊安全事件 □自行提出 □其他

問題或缺失說明

抽查 109 年外部稽核(Afnor)矯正措施處理單(109-CC40-A04)，觀察事項:組織已建立外部聯絡清單(NTCUST-ISMS-D-004):惟宜適度更新以確保資訊完整性。暫時性對策:更新外部聯絡清單(109/11/10)，增加殷諾科技。

1.1「長期性對策」欄位未說明如何預防該類事件再次發生(預防措施)。

1.2 抽查 110 年外部聯絡清單(NTCUST-ISMS-D-004)，未將重要資安設備廠商/相關資通、考選部設備維護商[redacted]。

以上查核內容不符 ISO27001 本文要求/10.1 不符合事項與矯正措施，建請改善。。

原因分析

1.1 漏未填寫長期性對策

1.2 漏未填寫旭鴻資通，考選部設備維護商泰鋒電腦往年為考選部自行聯繫故未填寫，今年起將補填入。

矯正措施評估

暫時性對策：（控制不符合事項的擴大或消除單一事件的影響）

1.1 補填長期性對策

1.2 補填旭鴻資通及泰鋒電腦

預訂完成日期：110 年 12 月 29 日

追蹤人	追蹤日期	確認結果
[redacted]	110/12/29	OK

長期性對策：（消除不符合事項或潛在風險的根本原因，以防止類似事件再次發生）

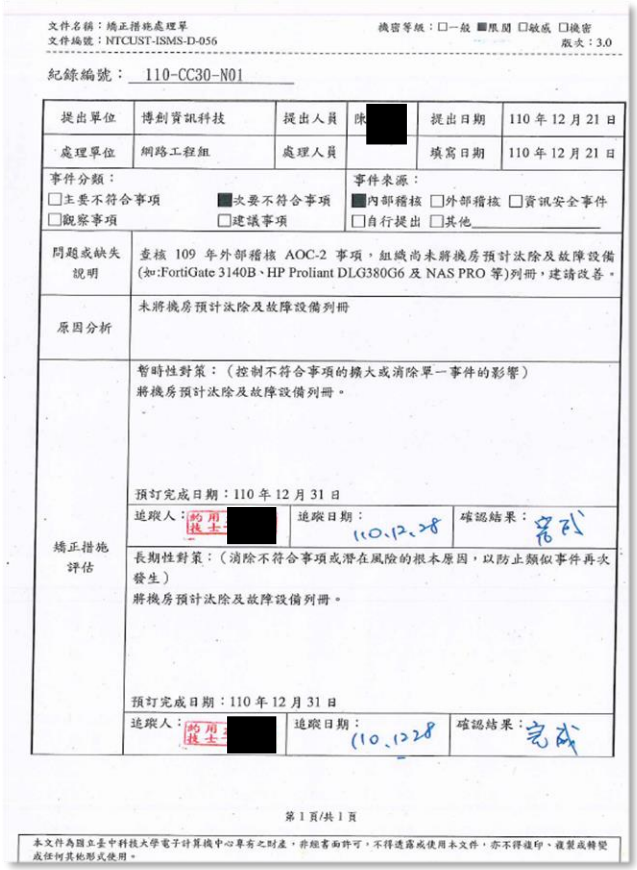
1.1 定期填寫長期性對策

1.2 與[redacted]電腦合作期間皆會填寫至外部聯絡清單

預訂完成日期：110 年 12 月 29 日

追蹤人	追蹤日期	確認結果
[redacted]	110/12/29	OK

第1頁/共1頁



文件名稱：矯正措施處理單　機密等級：□一般 ■限閱 □敏感 □機密
文件編號：NTCUST-ISMS-D-056　版次：3.0

紀錄編號：110-CC30-N01

提出單位	博創資訊科技	提出人員	[redacted]	提出日期	110 年 12 月 21 日
處理單位	網路工程組	處理人員		填寫日期	110 年 12 月 21 日

事件分類：□主要不符合事項 ■次要不符合事項 □觀察事項 □建議事項
事件來源：■內部稽核 □外部稽核 □資訊安全事件 □自行提出 □其他

問題或缺失說明

查核 109 年外部稽核 AOC-2 事項，組織尚未將機房預計汰除及故障設備(如:FortiGate 3140B、HP Proliant DLG380G6 及 NAS PRO 等)列冊，建請改善。

原因分析

未將機房預計汰除及故障設備列冊

矯正措施評估

暫時性對策：（控制不符合事項的擴大或消除單一事件的影響）

將機房預計汰除及故障設備列冊。

預訂完成日期：110 年 12 月 31 日

追蹤人	追蹤日期	確認結果
[redacted]	110.12.28	完成

長期性對策：（消除不符合事項或潛在風險的根本原因，以防止類似事件再次發生）

將機房預計汰除及故障設備列冊。

預訂完成日期：110 年 12 月 31 日

追蹤人	追蹤日期	確認結果
[redacted]	110.12.28	完成

第1頁/共1頁

資安實務需求與省思

- 資安業務實務案例、需求與省思
  - 核心伺服器管理面向
    - SQL injection：課程實驗、資訊揭露與收斂
    - 帳號權限管理：幽靈帳號、廠商臨時帳號、伺服器登入登載不實
    - 代管廠商主機：遠端桌面感染、誤植他校系統
    - 核心系統被內殖服務：挖礦服務、虛擬貨幣
  - 網路資料傳輸面向
    - 國外駭客網路攻擊：協同區網中心共同防禦
    - 明文傳遞機敏性個人資料：全面導入網路傳輸加密保護機制
  - 使用者管理面向
    - 私建NAS系統，病毒流竄
    - 私建無線熱點（Access Point）導致同網段網路問題

實務需求與省思

- 政府與教育部重視資訊安全環節
  - 教育單位應配合稽核政策申請資安計畫補助-資安專章
- 資料散佈在各校務系統需統合及確保安全性
  - 透過單一簽入機制導入一站式服務，後端需資料中心統合各種異質性系統資料，要如何發掘結構化與非結構化數據？
- 資料存取監控
  - 監控各權限正常、異常存取資料程序，是否有數位儀表板(Dashboard)功能提供警示、保護機制？
- 座落於混合雲中的定位
  - 重要個資應留於地端（私有雲），公開資料與去識別化資料上雲（公有雲），是否有整合軟硬體產出的資訊，進行混合雲風險管控與分析資訊，提早更新使用模式的機制？

總結

- IBM是市場上悠久穩健的品牌，在資訊領域的發展脈絡中，這是毋庸置疑的。
- 基於本場次開場講者對IBM Guardium軟體介紹，Guardium提供良好的資料稽核保護與合規性安全。
- 教育單位就實際使用經驗分享，過去國立臺中科技大學電子計算機中心在校務系統伺服器維運，確實在使用IBM Guardium軟體時，其提供穩定好用、完整的在地支援、資料存取類型支援是豐富的。

謝謝來賓聆聽與指教！！

Thank you for your attention!!