Exercise I -教育訓練通知

- 要領：
  - 稽核底稿之陳述應包含人、事、時、地、物。
- 解答：
  - 100/9/7 下午2:00至下午4:00於I210會議室，舉辦內部稽核教育訓練，邀請NII產業發展協進會吳昭儀資深經理蒞臨本中心講授，請本中心今年度內稽人員及有興趣之同仁參加，爲響應環保，本訓練恕不提供紙本教材，謝謝。

Exercise III 解答

資安稽核情境模擬演練

項目	ISO/CNS27001 對應內容
1 風險評鑑及管理	本文4.2.1
2 安全政策	附錄A.5
3 資訊安全組織	附錄A.6
4 資產管理	附錄A.7
5 人力資源安全	附錄A.8

啓始會議

啟始會議

稽核目的、範圍、方式、流程介紹

資產管理稽核

資產管理稽核

2. 適用範圍 1
3. 權責 1
4. 參考資料 2
5. 定義 2
6. 作業程序 4
6.1 流程圖 4
6.2 控制程序 5
6.2.1 資訊資產識別 5
6.2.2 資訊資產分類 5
6.2.3 資訊資產價值識別 6
6.2.4 資訊資產清冊及價值確認 8
6.2.5 資訊資產編號及標示 8
6.2.6 資訊資產管理作業 9
6.2.7 稽核 10
6.2.8 資訊資產之報廢 10
6.2.9 資訊資產之處理規範 10
7. 相關表單 11

首先要取得資訊資產管理程序書

資產管理稽核

6.2.5 資訊資產編號及標示

6.2.5.1 除「文件」類之資訊資產外，資訊資產編號之編碼方式如下圖所示，第 1~4 碼為權責單位別，第 5、6 碼為資產類別，第 7~10 碼為資訊資產編號。

6.2.5.2 已列入機密等級分類的資訊資產及系統之輸出資料，應明確標示其機密等級，避免其機密性遭破壞。

6.2.5.3 實體設備之重要等級標示方式：

6.2.5.3.1 實體設備之重要等級應以不同顏色標籤區分，並註明財產編號與財產名稱。

XXX – XX – XXXX

- 項次編號：
- 類別：
  - CN：通訊
  - DA：資料
  - DC：文件
  - EV：環境
  - HW：硬體
  - PE：人員

- 參照相關的作業程序書
- 訪談相關人員實際作法
- 參考相關執行紀錄

➔ 確認 說、寫、作 一致

資產管理稽核

6.9 資訊資產之處理規範

6.9.1 資訊資產之報廢（或銷毀）應依「WI3-S13-01資訊資產異動管理作業規範」之相關規定，採取適當之方式進行銷毀。

6.9.2 等級屬3或以上之資產，應加強安全保護及存取控制管控措施，以防止洩漏或不法及不當的使用。

6.9.3 等級屬3或以上文件類資訊資產之安全處理應符合以下作業要求：

(1) 紙類文件不再使用時，應銷毀處理。

(2) 系統流程、作業流程、資料結構及授權程序等系統相關文件，應予適當保護，以防止不當利用。

(3) 系統文件應指定專人管理，並鎖在安全的儲櫃或其他安全場所，且發送對象應以最低必要的人員為限。

資產管理稽核

臺北縣政府資訊中心

資訊資產清單

機密等級：□公開□一般■限閱□敏感

文件編號：FM4-S13-01　　版　　次：1.1

紀錄編號：　　填表日期：98 年 03 月 05 日

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
TPC-SW-00010	軟體	應用系統_戶政資訊查詢系統	戶政資訊查詢系統／戶政資訊查詢系統維護	王麗貞	資訊中心	資訊中心	3	3	3	3
TPC-SW-00011	軟體	應用系統_殯葬管理資訊系統	殯葬管理資訊系統／臺北縣殯葬管理資訊系統維護	王麗貞	資訊中心	資訊中心	3	2	3	3
TPC-SW-00026	軟體	應用系統_流程管理平台	流程管理平台／臺北縣政府流程管理平台委外服務	王麗貞	資訊中心	北縣府	3	2	4	4
TPC-SW-00012	軟體	應用系統_差勤管理系統	差勤系統／臺北縣政府差勤管理系統增修、維護及維運服務	周瑞真	資訊中心	北縣府	3	2	3	3
TPC-SW-00013	軟體	應用系統_資產整合管理資訊系統	財產管理系統／臺北縣政府財產管理系統維護	周瑞真	資訊中心	北縣府	3	2	3	3

資產是否詳列（抽幾筆資產，觀察是否列入）？資產分類是否恰當？

資產權責、保管及使用單位

資產重要性（業務衝擊）評估

資產管理稽核

風險評鑑及管理稽核

風險評鑑及管理稽核

目　錄

1. 目的 4
2. 範圍 4
3. 權責 4
3.1 資訊安全委員會 4
3.2 資訊安全小組 4
3.3 權責單位主管 4
3.4 資訊資產權責單位 4
4. 名詞定義 4
4.1 機密性 (Confidentiality) 4
4.2 完整性 (Integrity) 4
4.3 可用性 (Availability) 5
4.4 可接受風險值 5
4.5 殘餘風險 (Residual Risk) 5
4.6 威脅 (Threat) 5
4.7 弱點 (Vulnerability) 5
4.8 風險 (Risk) 5
5. 參考資料 5
5.1 PO2-S13-01 資訊資產管理程序 5
6. 作業說明 5
6.1 鑑別資產 5
6.2 資產評值 5
6.3 鑑別風險 6
6.4 確認風險評估結果 7
6.5 風險管理 7

確認程序書之架構是否完整

流程產出之風險評鑑結果是否可重複及可比較（不同人做可得到類似的評鑑結果）

風險評鑑及管理稽核

6.2.1 鑑別資產

6.2.1.1 資訊資產之鑑別應依據「資訊資產管理程序書」進行...及分類。

6.2.2 鑑別風險

6.2.2.1 威脅暨弱點評估

6.2.2.1.1 將各類資訊資產可能面臨之事件（威脅-弱點）含6類，並建立「威脅弱點評估表」：

A. 人為：包含因人員有意或無意行為、人力資源等所產生之風險。

B. 文件/資料：包含資料、文件之建立、維護...之不當所產生之風險。

C. 軟體：包含系統設計、維護、操作之不當所產生之風險。

D. 硬體：包含所有硬體設施之失效、損毀等可能風險。

E. 通訊：包含資料、影像、聲音傳輸媒介失效等所可能產生之風險。

F. 環境：包含天災、供水、用電、空調等，整體資訊環境，可能發生之風險。

6.2.2.2 事件發生機率及衝擊的評估

事件發生機率及衝擊的評估可依以下步驟進行：

6.2.2.2.1 依依各資訊資產之分類，進行選擇所需評估的事件（威脅-弱點）類別。

6.2.2.2.2 依以下之標準評估各事件發生機率及衝擊程度：

6.2.2.2.3 事件發生機率的評估：事件（威脅-弱點）發生機率值可參考下表得出。

- 風險評鑑的程序是否符合組織文化及業務目標
- 程序內容有沒有弱點威脅及衝擊評估的描述

風險評鑑及管理稽核

6.3.2 事件發生機率與影響程度評估

6.3.2.1 依威脅的等級對應表（表1）評估各事件之威脅等級

表1 威脅的等級對應表

評估標準	等級	評估值
每季發生一次之可能性	低	1
每月發生一次之可能性	中	2
每週發生一次之可能性	高	3

6.3.2.2 依弱點的等級對應表（表2）評估各事件之弱點等級

表2 弱點的等級對應表

評估標準	等級	評估值
該弱點不容易被威脅利用	低	1
該弱點容易被威脅利用	中	2
該弱點非常容易被威脅利用	高	3

6.3.3 風險值的計算

(1) 評估事件發生機率及影響程度後，計算出風險值。

(2) 風險值=（資訊資產價值 x 威脅等級 x 弱點等級）

6.3.5 風險評鑑彙整表

將上述評估資料彙整後產生「FM4-S13-04-風險評鑑彙整表」，並將「FM4-S13-04-風險評鑑彙整表」提交資訊安全小組開會審議。

6.4 確認風險評估結果

資訊安全小組依據「FM4-S13-04-風險評鑑彙整表」產出「FM4-S13-05-風險評鑑報告」，作為風險管理之用。

6.5 風險管理

6.5.1 可接受風險值的決定

(1) 資訊資產之可接受風險值，需經資訊安全委員會開會決議，並記載於會議紀錄中。

(2) 資訊安全委員會每年至少召開一次會議檢討可接受風險值。可接受風險必須考量組織環境及作業之安全需求，並進行適當地調整。

6.5.2 選擇控制措施

(1) 超出可接受風險值之資訊資產，應參考 ISO27001/CNS27001 選擇適當之控管措施，並產出「FM4-S13-06-風險改善計畫表」說明風險控管措施之執行辦法。

(2)「FM4-S13-06-風險改善計畫表」應陳報資訊安全委員會開會審核，並列入追蹤管理程序。

16

風險評鑑及管理稽核

風險評鑑及管理稽核

依評鑑程序計算出威脅值

是否完整列出資產之威脅、弱點

資產編號	資產類	資產名稱	資產說明	權責單位	風險事件		風險評鑑			
					威脅	弱點	資產價	威脅等	弱點等	風險
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP04/I-	楊啟得	不當維護	不正確的使用軟體和硬體	4	1	1	4
TPC-HW-036	硬體	伺服主機_I-	IMC	楊啟得	不當維護	文件化管理之缺乏或不足	4	1	1	4
TPC-HW-036	硬體			楊啟得	不當維護	缺乏有效的變更控制	4	1	1	4
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP07/I-	楊啟得	不當維護	缺乏監督機制	4	1	1	4
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP08/I-	楊啟得	不當維護	專業訓練不足	4	1	1	4
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP09/I-	楊啟得	不當維護	複雜的使用者介面	4	1	1	4

風險評鑑及管理稽核

資產編號	資產類	資產名稱	資產說明	權責單位	風險事件		風險評鑑			
					威脅	弱點	資產價	威脅等	弱點等	風險
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP04/I-	楊敏得	不當維護	不正確的使用軟體和硬體	4	1	1	4
TPC-HW-036	硬體					文件化管理之缺乏或不足	4	1	1	4
TPC-HW-036	硬體					缺乏有效的變更控制	4	1	1	4
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP07/I-	楊敏得	不當維護	缺乏監管機制	4	1	1	4
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP08/I-	楊敏得	不當維護	專業訓練不足	4	1	1	4
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP09/I-	楊敏得	不當維護	複雜的使用者介面	4	1	1	4
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP09/I-	楊敏得	硬體失效	不正確的使用軟體和硬體	4	2	1	8
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP09/I-	楊敏得	硬體失效	沒有作好維護的工作	4	2	1	8
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP09/I-	楊敏得	硬體失效	缺乏有效變更控制	4	2	1	8
TPC-HW-036	硬體	伺服主機_I-Chain	IMC-ICH-AP09/I-	楊敏得	硬體失效	缺乏硬體耗損控管	4	2	2	16

上線資料庫風險值超過組織可接受的風險值16，請問有沒有規劃對應的改善措施？

風險評鑑及管理稽核

臺北縣政府資訊中心 Information Management Center of Taipei County

風險改善計畫

機密等級：□公開 □一般 ■限閱 □敏感

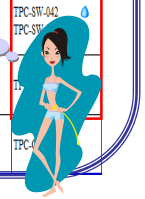
文件編號：FM4-S13-06　　版　次：1.0

紀錄編號：　　填表日期：98 年 3 月 5 日

ISO 27001控制目標	現況說明	風險改善建議措施	ISO 27001條文	建議權責單位	預計改善時間	實際改善時間	預計經費	與高風險資產之風險評估彙整表對照
	造成服務中斷	臨前加強定期進行巡檢維護工作	A.9.2.4設備維護	楊敏得	98年4月30日		無	TPC-HW-036
A.10.1 作業之程序與責任	可能造成設備超負荷問題	建立變更管理流程，依變更依程序進行	A.10.1.2變更管理				無	TPC-SW-042 TPC-SW-043
A.10.5 備份	測試環境無備NB，AP未備份，如NB失效，可能導致最新版程式無法使用	備份於異地備援場所	A.10.5.1資訊備份				無	TPC-SW-042 TPC-SW
A.10.1 作業之程序與責任	防火牆政策修改有一定之程序，若因不熟悉相關變更流程，故無法及時滿足其要求	建立變更管理流程，要求使用者依據變更依程序提出申請	A.10.1.2變更管理	張元泰	98年4月30日		無	T
A.9.2 設備安全	因機房停電，供電後突然造成元件損毀，惟服務未中斷	1.臨前加強定期進行巡檢維護工作 2.要求於兩小時內排除	A.9.2.2支援的公用設施 A.9.2.4設備維護	張元泰	98年4月30日		無	TPC

針對風險評鑑高於組織可接受風險之項目是否訂定改善計畫

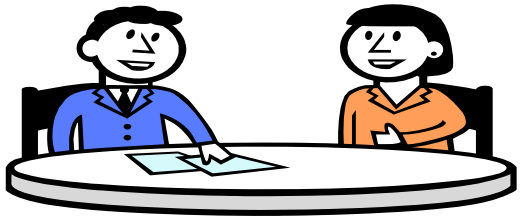
應該有訂風險改善計畫的....



風險評鑑及管理稽核

這是很重要的稽核點，我會先記錄下來，您可以在查核後會議中澄清。

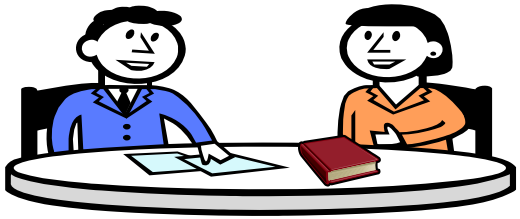
嗯~文件裏面沒有，但我記得之前有擬定改善建議措施的，....我需要再找找看..。



安全政策稽核

有正式公告嗎？

嗯...好像沒有正式公告..。



安全政策稽核

目　　錄

壹、 說明 1
貳、 目的 1
參、 適用範圍 1
肆、 定義 .....
伍、 權責說明 .....
陸、 資訊安全政策 2
柒、 資訊安全管理指標 2
捌、 資訊安全責任 3
玖、 資訊安全政策之修訂及公告 3

安全政策稽核

政策內容包含： 資訊安全之目標、範圍、實施內容、執行組織、權責分工、員工責任、事件通報處理流程及違反安全政策的後果等。

二、 本單位高階主管應積極參與資訊安全管理活動，提供對資訊安全之支持及承諾。
三、 本單位應定期提供全體同仁資訊安全訓練課程，提昇人員資訊安全認知。
四、 本單位全體同仁皆須應遵守本單位資安事件通報機制，通報所發現之資訊安全事件或資訊安全弱點。
五、 本單位全體同仁若未遵守本政策或發生任何違反本政策之行為，將依相關規定處理。
六、 本單位所有委外廠商皆須簽署保密協議書，並遵守本政策，以及相關程序之規定，不得未經授權使用或濫用本會之各類資訊資產。

政策由專人定期檢討與維護

玖、 資訊安全政策之修訂及公告

本政策應由資訊安全管理小組每年定期或因組織、業務、法令或環境等因素之變動，予以適當修訂，並呈 XXX 核准後公告實施。

安全政策稽核

正式公告通知員工遵循

公　告

○○○字第097001號

主旨：請全體同仁依資通安全管理制度辦理各項資訊作業事宜，特此公告。

說明：
一、為提升本單位資通安全防護作業，減少資通安 全事件之傷害，並確保重要資料的機密性、完整性以及可用性，依CNS 27001設計資通安全管理制度。
二、資通安全管理制度請參閱(網路芳鄰→Fileserver→資通安全管理制度資料夾)，請同仁確實遵守。
三、本公告自民國98年5月31日起生效。
四、 以上特此公告。

告知員工瞭解制度的管道

資訊安全組織稽核

資訊安全組織稽核

1 目的

1.1 確保本單位資訊安全管理制度之資訊安全責任，以落實本單位資訊安全政策之推動。

1.2 符合 CNS/ISO 27001 標準下列控制目標：

為確保組織內部資訊安全管理事項之推動，應建立適當管理架構，以審核資訊安全政策、分配安全責任，並協調組織範圍之安全政策實施。建立與組織外部安全專家之聯繫，並在處理安全事故時諮詢專家之意見。

2 適用範圍

2.1 本單位資訊安全管理制度之建立、實施與控制等

3 權責

3.1 資訊安全管理小組：

負責本單位資訊安全之維護與落實，權責範圍包括下列各項：

3.1.1 資訊安全管理制度之管理審查。

3.1.2 資訊安全政策之研擬。

3.1.3 各組資訊安全事項權責分工之協調。

3.1.4 資訊資產面臨之風險監督。

3.1.5 應採用之資訊安全技術、方法及程序之協調研議。

3.1.6 資訊安全事件之檢討及監督。

3.1.7 矯正預防措施之核准與監督。

3.1.8 其他重要資訊安全事項之協調研議。

4 參考資料

成立資訊安全管理小組，並釐清權責

資訊安全組織稽核

5. 作業說明

5.1 資訊安全組織架構與工作執掌

5.1.1 資訊安全組織架構

本中心資訊安全組織參照下圖，由資訊安全小組定期或不定期更新「FM4-S12-01-資訊安全組織成員表」。

資訊安全管理小組組織圖及權責分工

定期召開管理審查會議

5.1.2 資訊安全委員會

由本中心主任、副主任及各科科長組成，負責資訊安全管理制度相關事項之決議。

(1) 每年定期或視需要召開會議，審查資訊安全管理相關事宜。

(2) 視需要召開跨部門之資源協調會議，負責協調資訊安全管理制度執行所需之相關資源分配。

資訊安全組織稽核

6.2 定性化指標

6.2.1 資訊安全政策應定期審查，以確保資訊安全管理制度是否落實。

6.2.2 應定期審查資訊安全組織人員執掌，以確保資訊安全工作之推展。

6.2.3 應符合主管機關要求，依員工之職務及責任提供適當之資訊安全[illegible]

6.2.4 加強內部控制，防止未經授權之不當存取，以確保資訊資產受適當的保護。

6.2.5 應採取適當之保護措施及權限控管機制，以保障資訊處理設施之環境安全。

6.2.6 應確保資訊不因傳遞過程，或無意間之行為，透漏給未經授權之第三者。

6.2.7 系統開發應考量安全需求，並定期稽核安全弱點。

6.2.8 確保所有資訊安全事件或可疑之安全弱點，都應依循適當之通報機制向上反應，並予以適當調查及處理。

存取權限、委外相關規定

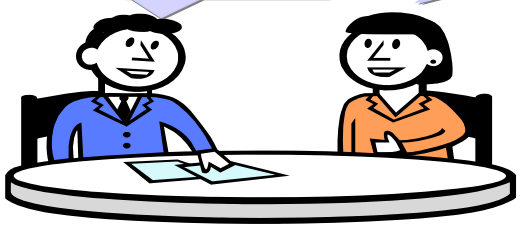
7. 資訊安全政策之審查及實施

本政策應每年定期審查，遇組織、業務、法令或環境等因素之更迭，予以適當修訂，經「資訊安全委員會」核定後公告施行，以確保資訊安全運作之有效性。

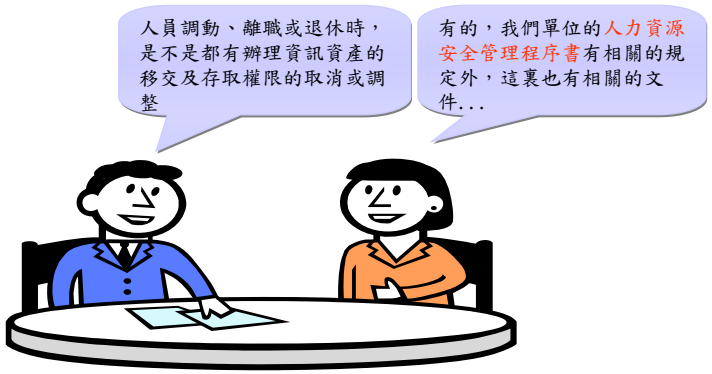
資訊安全組織稽核

其實不是只有資訊室或系統管理人員才需要簽保密協議，只要有機會接觸重要資訊的人員都需要納入管理，窗口服務人員常常需要執行客戶資料的處理，也應該簽署保密協議。

是，這是我們沒有注意到的…..



人力資源安全稽核



人力資源安全稽核

目　錄

1. 目的
2. 範圍
3. 權責
3.1 資訊安全委員會
3.2 資訊安全小組
3.3 單位主管
3.4 人事單位
3.5 專案承辦人
4. 名詞定義
4.1 內部人員
4.2 外部人員
5. 參考資料
5.1 勞動基準法
5.2 QM1-S01-01 資訊安全政策
5.3 行政院暨所屬機關約僱人員僱用辦法
5.4 WI3-S13-01 資訊資產異動管理作業規範
5.5 PO2-S13-02 風險評鑑與管理程序書
5.6 PO2-S15-01 實體安全管理程序書
5.7 機房管理手冊
5.8 公務人員服務法
5.9 公務員懲戒法
5.10 電腦處理個人資料保護法
5.11 PO2-S17-01 存取控制程序書
5.12 WI3-S17-01 帳號管理作業規範
5.13 PO2-S13-01 資訊資產管理程序書
6. 作業說明
6.1 人員角色與責任界定
6.2 人員報到適用權責簽清與安全事項說明
6.3 任用條款與條件
6.4 管理階層責任
6.5 資訊安全認知、教育及訓練
6.6 懲處過程
6.7 終止責任
6.8 資產的歸還
6.9 存取權限的移除

- 檢視文件是否齊備
- 詢問人員是否瞭解相關規定

人力資源安全稽核

6. 作業說明

6.1 人員角色與責任界定

6.1.1 人員角色與責任界定，請參考本文件之“權責”說明。

6.1.2 本中心之各項業務，必須指定專責之負責人及代理人，於業務負責執行期間或代理執行業務之管理工作，並配合「QM1-S01-01資訊安全政策」之要求，進行安全管理。本中心資訊安全職責詳「臺北縣政府資訊中心職務分配表」。

6.2 人員報到適用權責簽清與安全事項說明

(1) 本中心內部人員之任用，應建立適當的安全評估。

(2) 員工之進用，除依據「勞動基準法」及「行政院暨所屬機關約僱人員僱用辦法等相關法規」等相關法規辦理之外，應詳查員工身分證明文件，確保該員工之身分真實性。

(3) 委託駐府、廠商人員處理本中心業務前，應施以適當之風險評鑑，以鑑別可能發生之風險。資訊資產異動及風險評鑑方式分別依據「WI3-S13-01 資訊資產異動管理作業規範」及「PO2-S13-02 風險評鑑與管理程序書」辦理。

6.3 任用條款與條件

(1) 本中心內部人員應使其了解相關之工作責任、安全要求與本中心「QM1-S01-01 資訊安全政策」，並簽署「FM4-S14-01-員工保密暨使用合法電腦軟體切結書」。

(2) 駐府及廠商人員於本中心服務時應使其了解相關之工作責任安全要求與本中心「QM1-S01-01 資訊安全政策」，並簽署「資訊安全保密切結書」。

- 取得員工名單，抽核是否簽具保密切結書
- 訪談瞭解組織離職、調職作業流程，抽驗是否確實辦理相關程序
- 例如：查證離職員工的e-mail帳號是否已刪除

人力資源安全稽核

6.5 資訊安全認知、教育及訓練

(1) 資訊安全小組應訂定每年之「資訊安全教育訓練計畫」，並駐府及廠商人員，進行資訊安全教育訓練(如資訊安全注意事宣導)。

(2) 資訊安全教育訓練內容至少應包含法律相關規範及正確使用備等安全注意事項。

(3) 為確保教育訓練執行之成效，應辦理測驗或其它方式進行

(4) 承辦本中心之資訊安全教育訓練之負責人，應備妥簽到表紀錄留存備查。

6.6 懲處過程

(1) 本中心內部人員執行工作，若違反資訊安全或相關法規規定（例「公務人員服務法」、「公務員懲戒法」與「電腦處理個人資料保護法」等）時，如涉及人為過失並經單位主管或政風單位協同相關單位查證屬實後，經陳報機關首長後執行相關懲處。

(2) 駐府及廠商人員執行業務時，應遵守政府資訊安全相關法令及本中心資訊安全相關規定，若違反時(如電腦洩密、盜取個人資料…等)，將依合約或相關法令規定辦理。

- 確認相關單位是否依規定辦理人員資訊安全認知教育訓練
- 查核相關教育訓練的記錄例如：課程時間、課程講義、人員簽到或學習記錄、評量成績、上課照片

人力資源安全稽核

人力資源安全稽核

臺北縣政府資訊中心

調（離）職人員資訊資產移交列表

紀錄編號：　　填表日期：　年　月　日

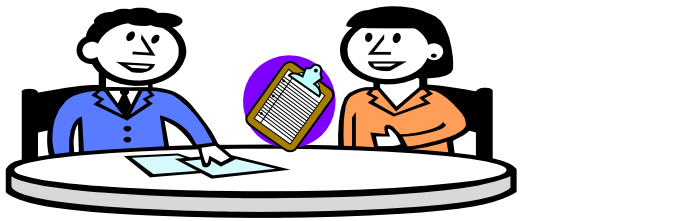
申請人：			聯絡電話：	
單位：			調(離)職日期：　年　月　日	
資訊資產編號	資訊資產名稱	接收人員	接收單位	備註

附件：資訊資產異動申請表

申請人	科長	主任

確認人員離職時是否收回保管的資產並將帳號權限移除，例如e-mail帳號

人力資源安全稽核



人力資源安全稽核

資訊安全推動計畫

資訊安全教育訓練簽到表

時間：　98年5月14日

地點：會議室A

單位	姓名/職稱	簽名
		吳 XX
		羅 OO
資訊科	黃 XX	黃 XX
資訊科	李 OO	李 OO
	王 XX	王 XX

資訊安全認知教育訓練要依職務層級進行，像是資訊業務人員若僅上初階的「網路安全管理」是不足夠的，教育訓練的部分需要再加強。

瞭解

Exercise IV 解答

Exercise IV稽核結束之口頭報告

- 缺失：
  - 經99.06.11 15:30與機房管理員(王小姐)一同至A機房進行實地抽查發現，硬體(HW-00119)未依分級標示硬體(未貼標籤)。(Clause A.7.2.2)
- 觀察：
  - 經99.06.11 10:00與ISMS文管人員(林先生)於會議室A進行文件審查發現，未有足夠證據或紀錄顯示殘餘風險已經管理階層之核准(因尚未進行風險再評鑑)。[Clause 本文4.2.1(h)]
- 建議：
  - 經99.06.11 10:00與ISMS文管人員(林先生)於會議室A進行文件審查發現，目前使用之威脅弱點評估表自首次建立後，從未進行檢視或修訂，建議組織宜於風險評鑑前檢視/修訂威脅及弱點項目。[Clause 本文4.2.1(d)]