

who what
where 資通 why
when 安全 How



各級公私立學校資通安全工作事項-1

- ◆ 資通安全為確保各政府機關（構）之資訊及網路系統遭受入侵或不當使用時，能迅速作必要之應變處置並在最短時間內回復正常運作，以降低該事故可能帶來之損害。

各級公私立學校資通安全工作事項-2

- ◆ 行政院於2004年10月21日頒布「各政府機關(構)落實資安事件危機處理具體執行方案」中提出幾項具體的作法,簡述如下:

(一)組織管理

(二)安全控管

(三)通報機制

(四)稽核管考

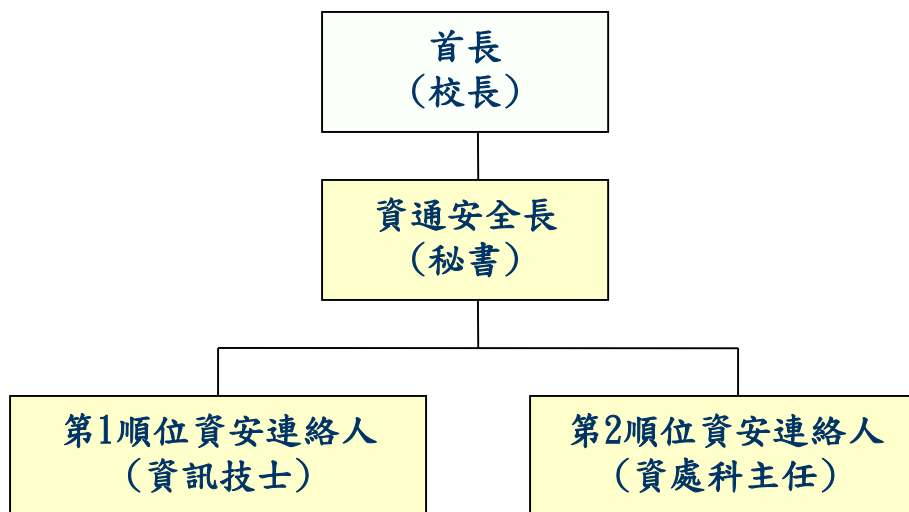
(五)教育認知

各級公私立學校資通安全工作事項-3

(一)組織管理

設立資通安全長（CISO）、建立資安專業制度、

資安預算應採一定比例分配以確保資訊系統運作安全無虞。



各級公私立學校資通安全工作事項-4

(二)安全控管

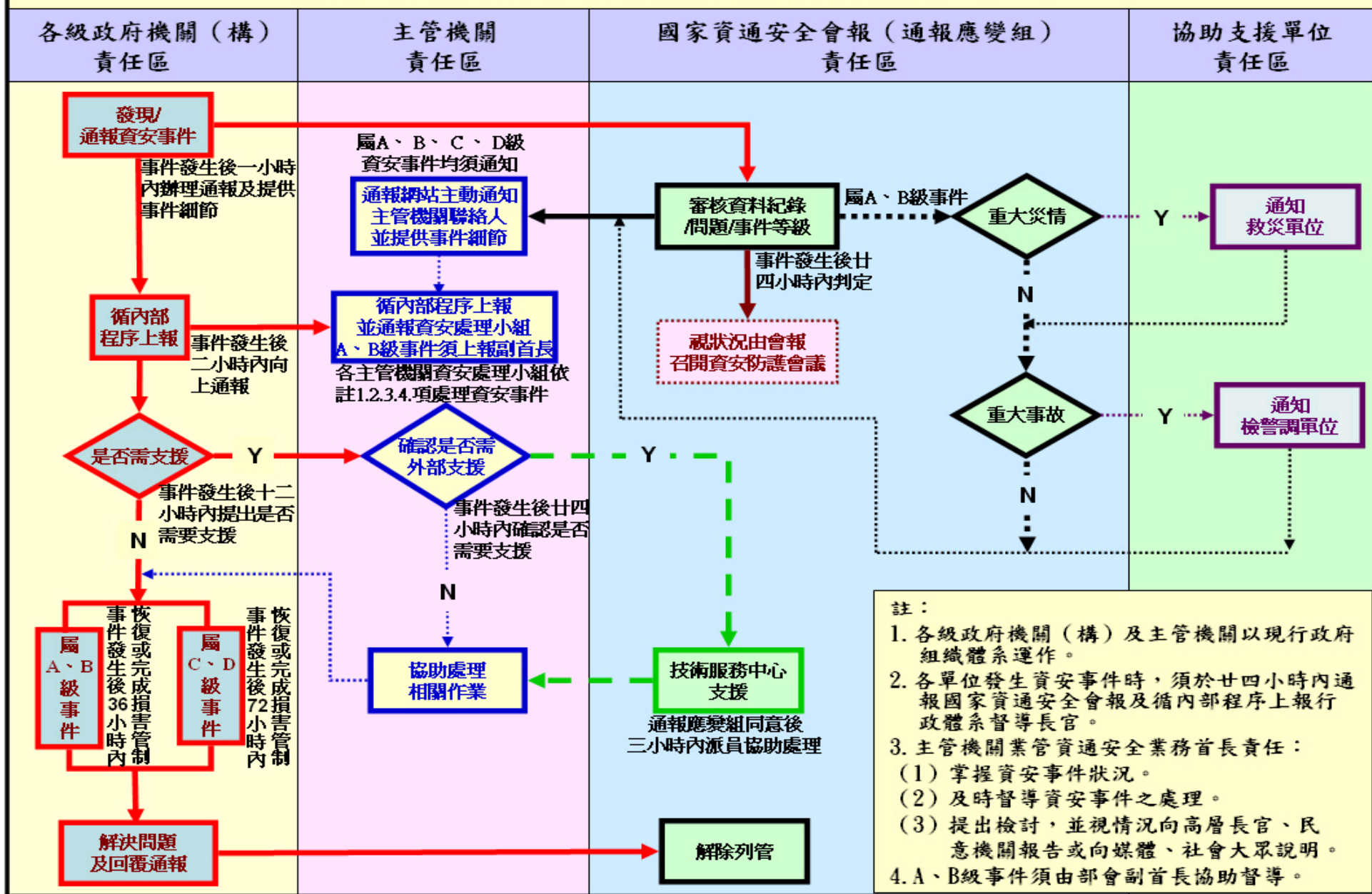
- ◆ 專人負責資安管控。
- ◆ 資訊委外時應要求廠商提供提供資通安全相關服務（包括電腦主機弱點掃描、漏洞修補、防毒軟體等）。
- ◆ 對極重要、重要之敏感文件、資料、檔案等之處理，應採取檔案加密方式儲存，並除非常必要之連網外，均兼採實體隔離等防護措施。

各級公私立學校資通安全工作事項-5

(三)通報機制：

- ◆ 發生資安事件時務必通報，絕對不能有「不需要協助就不必通報」的錯誤心態
- ◆ 依循「通報與應變作業流程」落實資通安全事件之危機通報及緊急應變作業

國家資通安全會報通報與應變作業流程（一）



各級公私立學校資通安全工作事項-6

(四)稽核管考：

- ◆ 健全資訊安全管理制度（ISMS）、確實執行資安檢核作業。

各級公私立學校資通安全工作事項-7

(五)教育認知：

- ◆ 辦理資安教育訓練、加強資安宣導、專業證照取得。
- ◆ 資安事件等級：

事件等級	說 明
A 級	影響公共安全、社會秩序、人員生命財產
B 級	系統停頓，業務無法運作
C 級	業務中斷，影響系統效率
D 級	業務短暫停頓，可立即修復

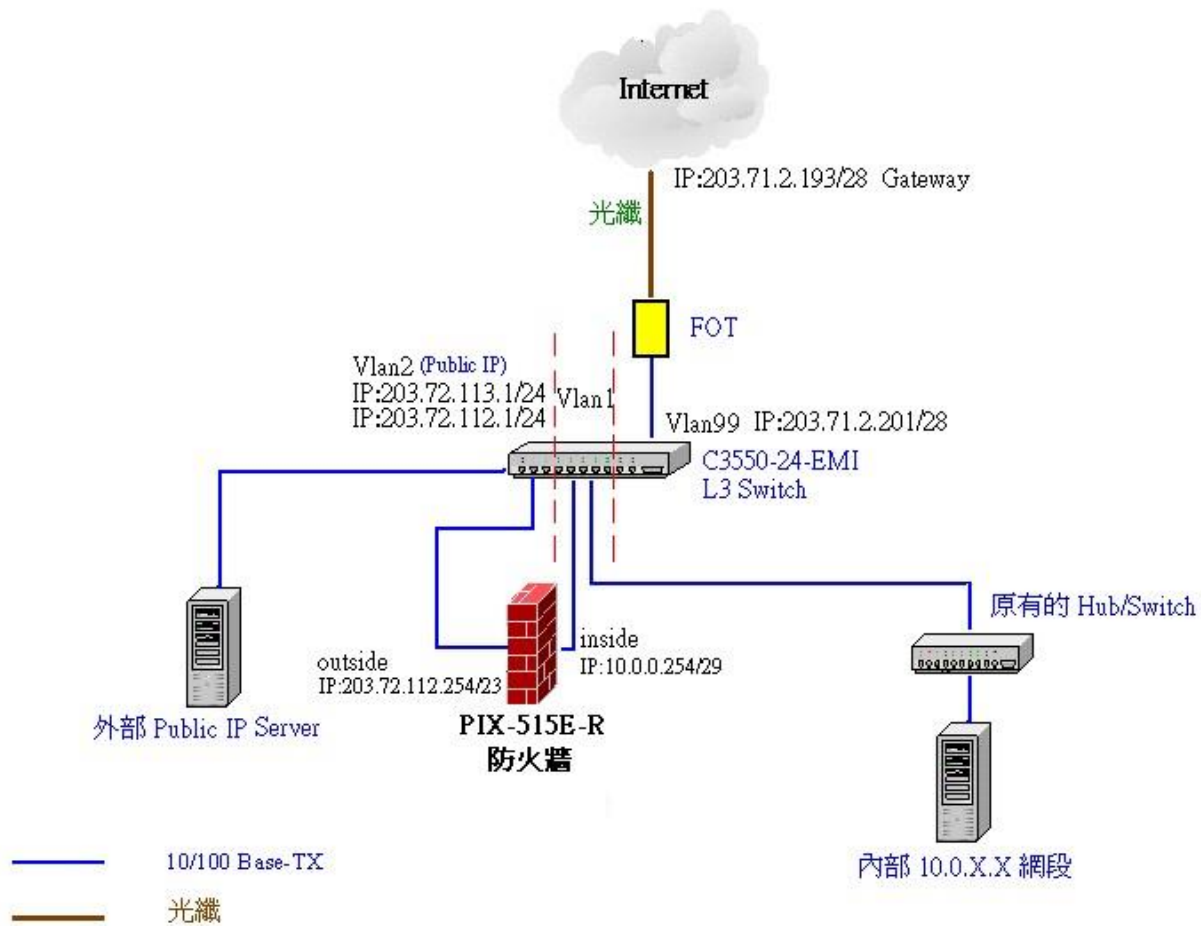
- ◆ 各類資安系統等級應執行之工作事項

內容作業名稱 等級	防禦機制強度	防護縱深	ISMS推動作業	稽核方式	資安教育訓練 (主官、主管、技術、一般)	專業證照
A級	強度等級4	NSOC直接防護/自建SOC、IDS、防火牆、防毒	96年通過第三者認證(註二)	每年至少執行二次內稽	每年至少(4, 6, 18, 4小時)	96年資安專業鑑定二張(註三)
B級	強度等級3	SOC (Optional)、IDS、防火牆、防毒	97年通過第三者認證	每年至少執行一次內稽	每年至少(4, 6, 16, 4小時)	96年資安專業鑑定一張
C級	強度等級2	IDS, 防火牆、防毒	各單位自行成立推動小組規劃作業	自我檢視	每年至少(2, 6, 12, 4小時)	資安專業訓練
D級	強度等級1	防火牆、防毒	推動ISMS觀念宣導	自我檢視	每年至少(1, 4, 8, 2小時)	資安專業訓練

本校資通安全防護措施-1

- ◆ 92年底完成本校防火牆建置，內部使用虛擬IP
- ◆ 防火牆設定(完全限制,必要開放)
- ◆ 垃圾郵件及病毒郵件過濾系統
- ◆ 網路流量偵測系統
- ◆ 伺服器及個人電腦安裝趨勢officescan防毒軟體
- ◆ 電腦教室及班級教室電腦安裝再生卡還原系統確保機器正常使用
- ◆ 可攜式媒體(如隨身碟、隨身硬碟、SD記憶卡等)之使用管制

網路連線架構圖



中壢家商網路架構圖

本校資通安全防護措施-2

防火牆(PIX515E)

Cisco PIX Device Manager 2.1 - 10.0.0.254

File Rules Search Options Tools Wizards Help

Access Rules Translation Rules VPN Hosts/Networks System Properties Monitoring

Use the Rules menu, the toolbar, or the right mouse button to add, edit or delete access, AAA or filter rules.

☒ Access Rules ☐ AAA Rules ☐ Filter Rules [Show Detail](#)

#	Action	Source Host/Network	Destination Host/Network	Interface	Service	Description (Read Only)
1	✗	Group:pcrooml	any	inside	(1-65535)/tcp	
2	✗	Group:pcrooml	any	inside	(512-65535)/tcp	
3	✗	any	any	inside	service grou :Bla	
4	✗	any	any	inside	service grou :Bla	
5	✗	any	any	inside	icmp	
6	✗	any	any	inside	service group:Sasser_TCP	
7	✓	any	any	inside	ip	
1	✓	any	Mail/ 10.0.0.4	outside	service grou :Mail_Server	
2	✓	any	WWW/ 10.0.0.2	outside	http/tcp	
3	✓	any	WWW2/ 10.0.0.7	outside	http/tcp	

✓ Allow traffic ✗ Deny traffic

[Apply](#) [Reset](#)

User: admin Privilege Level: Admin (15) PIX Time: 08:49:59 CST Fri Jul 01 2005

本校資通安全防護措施-3

http://pclhvs.cl.edu.tw - 回收箱/垃圾信攔截明細列表 - Microsoft Internet Explorer

22/39 篇

Mail2000垃圾郵件過濾系統 - MailGates

您有以下垃圾信件或是可疑垃圾信件，被留置於 MailGates 主機上，請協助檢視並處理。若您需要操作進階管理功能，請檢視附檔或直接登入 [MailGates 主機](#)，謝謝。

可疑信件 共 0 封
新信 0 封 / 即將刪除 0 封 (保留期限 120 天)

垃圾信件 共 6812 封
新信 1 封 / 即將刪除 34 封 (保留期限 30 天)

旗標	信件處理	標題	寄件人	日期	預定刪除時間
	送信 送信並加入個人白名單	夢幻天使 女優特選●全台獨家發售片 搶先曝光●	全台獨家七月份發售片 <numxqwqmi.nvspntw@msa.hinet.net>	2008/03/31 13:00	2008/04/30 13:00
	送信 送信並加入個人白名單	提供情趣用品，包括保險套、跳蛋、內衣褲、情趣精品批發零售。情趣用品專業	價格便宜 <notzhk.ajralya@msa.hinet.net>	2008/03/01 16:51	2008/03/31 16:51
	送信 送信並加入個人白名單	Best Sales 2008!	<chlin@pclhvs.cl.edu.tw>	2008/03/01 16:35	2008/03/31 16:35
	送信 送信並加入個人白名單	「家」就是「醫院」！把「專科醫師」帶入您的家庭中！全	世界遺產 <wubfz.kzp@msa.hinet.net>	2008/03/01 16:35	2008/03/31 16:35

http://mg.pclhvs.cl.edu.tw/mg-cgi/mail_read?mg=&suid=CHLIN@pclhvs.cl.edu.tw&MAILBOX=@.spam&MSG=BOSOV358&SORT=DEFAULT&mkey=D(

開始 資安公文 Microsoft Power... 未命名文件 - Mi... Mail2000電子信... http://pclhvs.cl.edu... 下午 02:40

本校資通安全防護措施-4

未命名文件 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

網址(1) http://www.pclhvs.cledu.tw/web/main.htm

Google 開始 書籤 28 已擷取 拼字檢查 翻譯 傳送到 設定

DIVX Y! 網頁搜尋 書籤 設定 迷你筆 知識+ 信箱 拍賣 字典 網頁翻譯

國立中壢高級家事商業職業學校
NATIONAL CHUNG-LI HOME ECONOMIC AND COMMERCIAL VOCATIONAL HIGH SCHOOL

Packet Show

使用者: 管理者
Thu May 22 14:33:24 CST 2008

流量表 統計圖表 查詢 系統管理 支援PS 登出

服務分類 部門分類 排行榜

統計圖表 // 排行榜 [日統計] 選擇觀看員工排名前 30 名 部門排名前 30 名 每頁顯示 30 筆資料 確定 儲存

<< 2008年5月 >>

日 一 二 三 四 五 六
27 28 29 30 1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31

今天是2008年5月22日

管轄部門列表

所屬部門架構

全公司

用戶 10.0.3.44 疑似使用 P2P 軟體(2008-05-22 14:29:57) 用戶 10.0.2.37 疑似使用 P2P 軟體(2008-05-22 09:35:02)

月統計 週統計 日統計 選擇埠號: ALL 總流量

個人排行榜第 1 頁

接收前30名				傳送前30名			
人名/IP	傳輸量(KBytes)	百分比		人名/IP	傳輸量(KBytes)	百分比	
1 10.0.2.16	1076438	6.75%		1 10.0.3.44	1481151	42.34%	
2 10.0.2.187	856579	5.37%		2 10.0.0.53	491815	14.06%	
3 10.0.2.74	776363	4.86%		3 10.0.4.6	101623	2.90%	
4 10.0.2.87	560779	3.51%		4 10.0.0.2	71782	2.05%	
5 10.0.2.78	499291	3.13%		5 10.0.0.27	70790	2.02%	
6 10.0.2.61	398447	2.50%		6 10.0.4.4	59654	1.71%	
7 10.0.2.69	389171	2.44%		7 10.0.2.31	54834	1.57%	

開始 資安公文 Microsoft PowerPoint... 未命名文件 - Micro... Mail2000電子信箱-c... 下午 02:35

推動資安的經驗分享

- ◆ 政策及規範

- ◆ [Goal] 教育體系資通安全管理規範

- ◆ [Jobs] 1.建立資安宣導網

- ◆ 2.訂定相關規範,制度,文件

- ◆ .2-1個人電腦使用注意事項(97.3.20)

- ◆ 依據：教育部96年12月19日台電字第0960196582函訂定之

- ◆ 2-2資訊安全管理要點(88. 8. 1 訂定,98. 7. 23 修正)

- ◆ 依據：「行政院及所屬各機關資訊安全管理要點」

- ◆ 2-3學校網路使用規範(92.5. 30訂定,99.2.2 行政會議修正通過)

- ◆ 依據：99.1.11教育部台電字第0980210235C號令「台灣學術路管理規範」。

推動資安的經驗分享

[Jobs] 3. 資安教育訓練(一般人員每年至少2hr)

97年度第1次資通安全研習 (97.5.28)

98年電腦安全自我檢查(98.7.31, 98.8.3)

99年規畫中...

4. 資安稽核作業

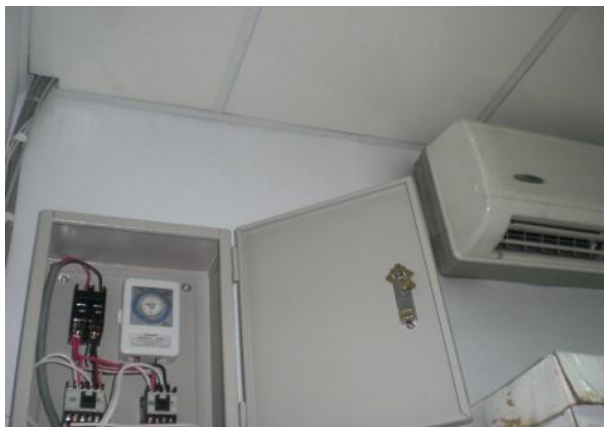
由政風單位會同資訊安全小組及相關單位負責辦理。

每年進行至少1次資訊安全稽核。

98.8.4教育部中辦室至本校資安稽核。

推動資安的經驗分享

◆.實體環境改善



推動資安的經驗分享

- ◆ 資安預算應採一定比例分配以確保資訊系統運作安全無虞。

資安系統維護： packetshow流量管控 15,000元、新世代骨幹 網路36,000元、郵件暨 郵件過濾系統32,000 元、防毒全校授權維護 60,000元	143,000	143,000			
電腦機房設備維護：伺 服器養護30,000元、網 路交換器15,000元冷氣 清洗保養10000	55,000	55,000			
電腦教室設備維護：個 人電腦養護40,000元、 鍵盤滑鼠記憶體等 20,000元、網路交換器 15,000元、冷氣機洗保 養20000	95,000	95,000			
資通安全研習：講座鐘 點4,800元、教材講義 印刷10,200元	15,000	15,000	4,800		

建構中的ISMS...



A主機伺服器管理



B機房門禁



C資安事件通報



D備份作業



E資訊資產管理



T文件管制



E001網路資產



E002軟體資產

