100年度雲嘉區域網路中心營運持續計畫演練成果報告

情境一

日期：100.09.16

CCU Computer Center

情境內容

- 區網中心演練情境：本次演練情境設定為發生第三級弱震（房屋搖動，門窗格格作響，懸物搖擺，盛水動蕩）。
- 情境：模擬因第三級弱震造成供電短暫中斷，導致TANet 骨幹網路及核心業務系統暫時無法提供服務。

CCU Computer Center

演練前會議

- 演練前演練召集人邀集區網維護TANet網路骨幹維運及學籍系統相關人員召開演練前說明會議。
- 演練召集人說明此次營運持續計畫演練內容及目的。

CCU Computer Center

會議進行狀況

- 參與演練人員熱烈討論演練內容及細節。
- 由演練召集人說明其角色扮演及執行程序。

CCU Computer Center

宣佈演練開始

- 會議中負 責人員核對演練開始時間。
- 會議討論完畢後，主席正式宣佈演練開始，並請參與演練之人員就定位。

CCU Computer Center

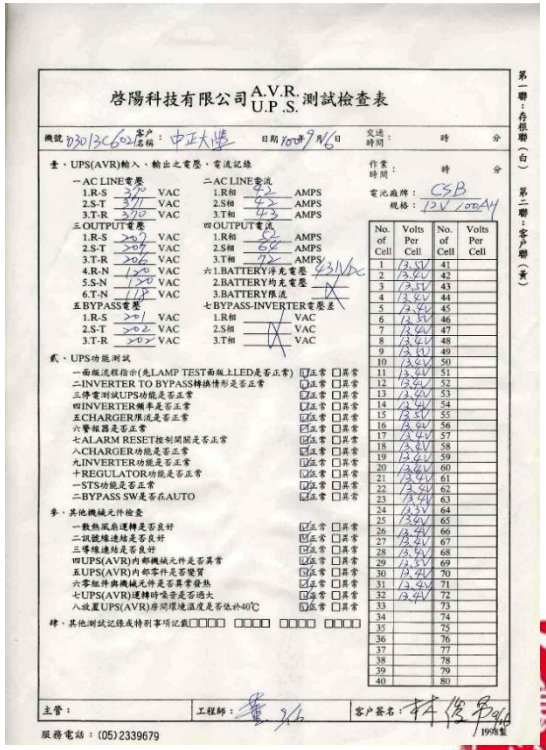
電力維護人員接獲UPS供電異常通知(1/2)

- 電力維護人員進入UPS檢查供電狀況，經發現UPS保護裝置跳脫並進行保護裝置重新復歸。
- 資訊安全官李副校長親自視查檢修狀況。

CCU Computer Center

電力維護人員接獲UPS供電異常通知(2/2)

- 通知UPS維護廠商啟陽科技到點檢測電力供電狀況。
- 維護廠商提供檢測報告單。



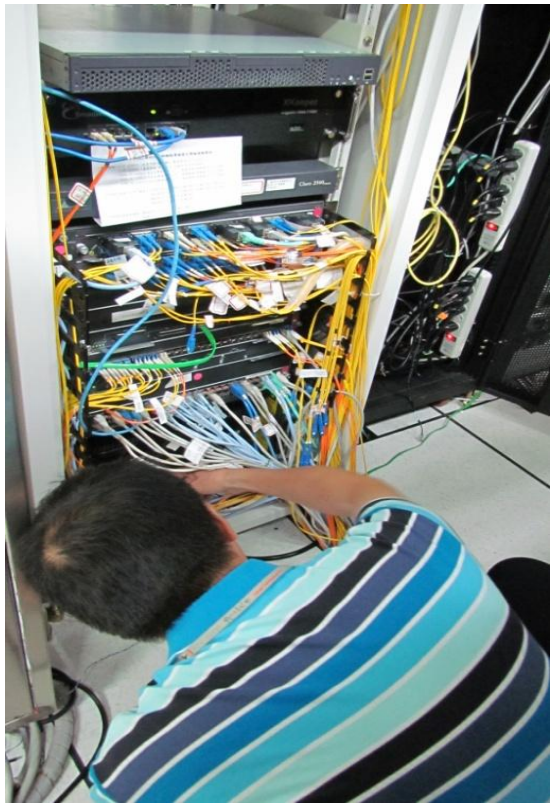
啓陽科技有限公司 A.V.R. U.P.S. 測試檢查表

網路監控人員發現TANet網路中斷情況

- 回復供電後，區網骨幹網路發生無法對外連線情況。
- 負責人開始啓動應變機制進行問題處理。

網路通訊設備檢查

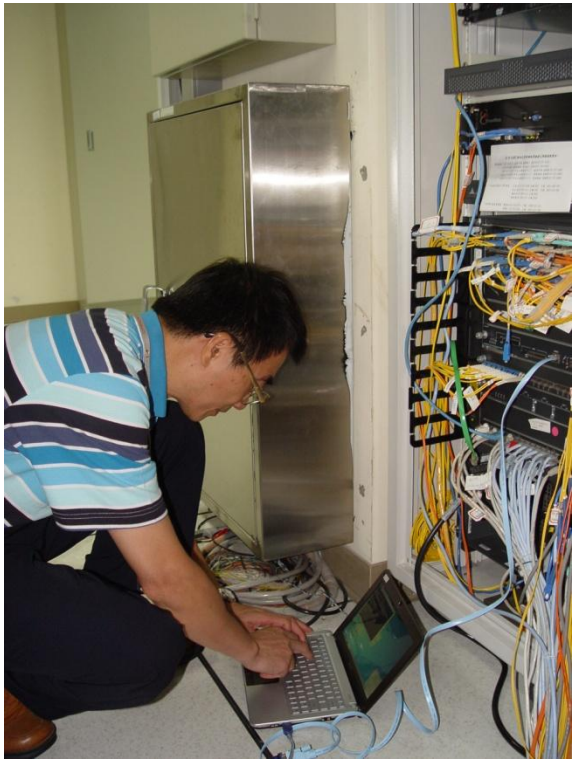
- 區網維運人員進入機房檢查路由器等實體設備。
- 詳細檢查面版電源指示燈、運作燈號、風扇、網路模組狀況及光纖線路等是否正常運作或脫落？



CCU Computer Center

路由器網路狀況檢查

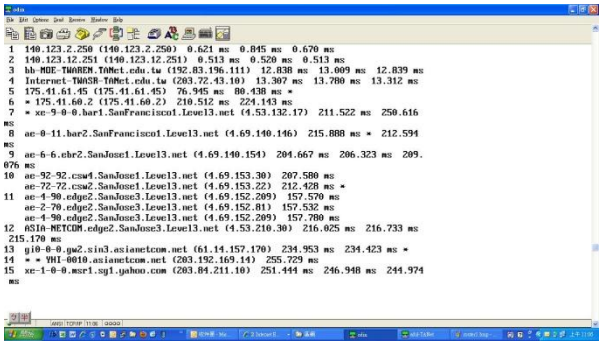
- 區網維運人員重新起動路由器。
- 透過筆記型電腦連接6509路由器，檢測路由相關設定。

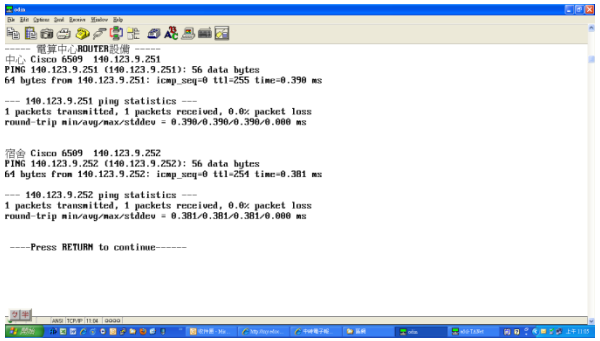


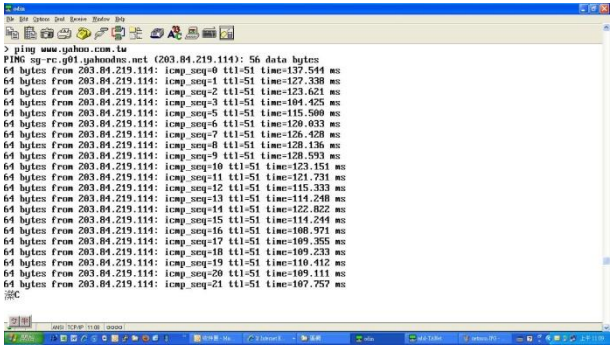
CCU Computer Center

TANet網路骨幹檢測

- 依【學術網路系統障礙偵測與復原作業程序】進行網路檢測。
- 執行netmon指令(內含數拾個tracert及ping之shell script)檢查內外部網路連線狀況。

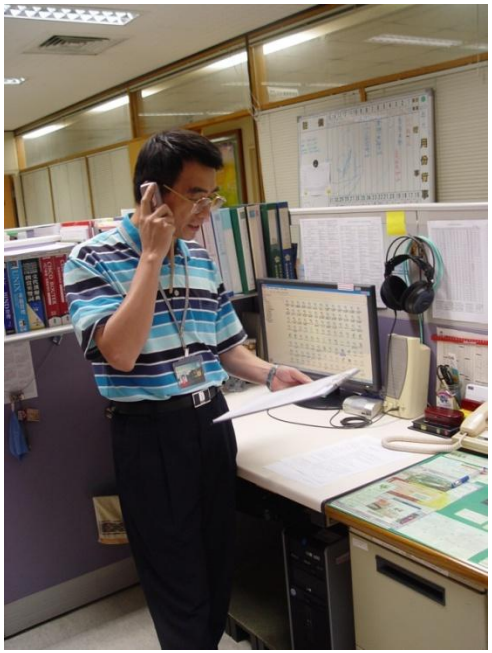






通報TANet設備維護廠商

- 以電話通知TANet維護廠商(麟瑞科技)，請其儘速進行修復。
- 廠商並透過ADSL專線及Cisco2900遠端連接路由設備進行設備檢測。



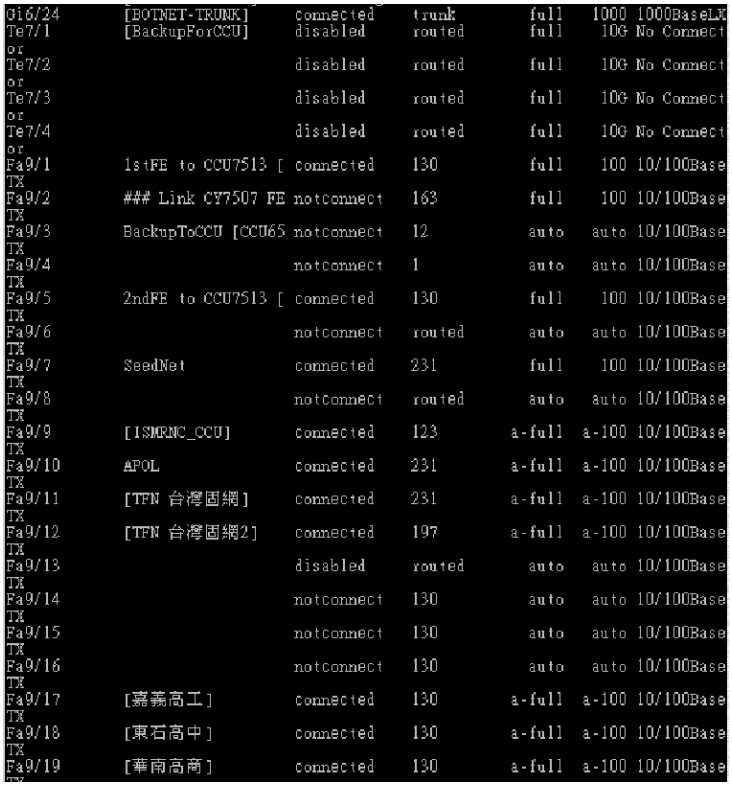
CCU Computer Center

進行資安通報

- 負責人員判定為資訊安全事件，並以電話通知資訊安全官及單位主管。

TANet維護廠商回報修復記錄

- 廠商將系統修復後，同時也以電話報告修復狀況，並E-Mail修復紀錄表。



Gi6/24	[BOTNET-TRUNK]	connected	trunk	full	1000	1000BaseLX
Te7/1	[BackupForCCU]	disabled	routed	full	10G	No Connect
or						
Te7/2		disabled	routed	full	10G	No Connect
or						
Te7/3		disabled	routed	full	10G	No Connect
or						
Te7/4		disabled	routed	full	10G	No Connect
or						
Fa9/1	1stFE to CCU7513 [	connected	130	full	100	10/100Base
TX						
Fa9/2	### Link CY7507 FE	notconnect	163	full	100	10/100Base
TX						
Fa9/3	BackupToCCU [CCU65	notconnect	12	auto	auto	10/100Base
TX						
Fa9/4		notconnect	1	auto	auto	10/100Base
TX						
Fa9/5	2ndFE to CCU7513 [	connected	130	full	100	10/100Base
TX						
Fa9/6		notconnect	routed	auto	auto	10/100Base
TX						
Fa9/7	SeedNet	connected	231	full	100	10/100Base
TX						
Fa9/8		notconnect	routed	auto	auto	10/100Base
TX						
Fa9/9	[ISMRNC_CCU]	connected	123	a-full	a-100	10/100Base
TX						
Fa9/10	APOL	connected	231	a-full	a-100	10/100Base
TX						
Fa9/11	[TFN 台灣固網]	connected	231	a-full	a-100	10/100Base
TX						
Fa9/12	[TFN 台灣固網2]	connected	197	a-full	a-100	10/100Base
TX						
Fa9/13		disabled	routed	auto	auto	10/100Base
TX						
Fa9/14		notconnect	130	auto	auto	10/100Base
TX						
Fa9/15		notconnect	130	auto	auto	10/100Base
TX						
Fa9/16		notconnect	130	auto	auto	10/100Base
TX						
Fa9/17	[嘉義高工]	connected	130	a-full	a-100	10/100Base
TX						
Fa9/18	[東石高中]	connected	130	a-full	a-100	10/100Base
TX						
Fa9/19	[華南高商]	connected	130	a-full	a-100	10/100Base
TX						

麟瑞科技股份有限公司

□台北:台北市南港路二段99-1號 TEL:(02)2651-2340 FAX:(02)2788-0815
□新竹:新竹市寶山路150巷1號7F TEL:(03)561-1522 FAX:(03)561-1540
□台中:台中市忠明南路449號1.5F-3 TEL:(04)2375-3973 FAX:(04)2375-3917
□台南:台南縣永康市中華路1.48號10F TEL:(06)312-6762 FAX:(06)312-6761
□高雄:高雄市博愛二路420號3F-2 TEL:(07)556-9402 FAX:(07)557-9401

維護服務記錄表　表單編號：107236

客戶專線: 0800-863-888　傳真: (02)2651-6891　客服信箱: services@ringline.com.tw

客戶名稱:　連絡人:　電話:　分機:
服務類別: □裝機 □維護 □保固 □測試　合約/接單機號:
服務項目: □系統設定 □設備安裝 □設備維修 □技術諮詢 □其他:

服務紀錄單內容

客服編號	CS11090104	客戶名稱	國立中正大學
聯絡人	張永榴	電話	05-2720411#14103
電子郵件		服務等級	P3
問題來源	SE電話(含手機)	服務項目	技術諮詢
服務類別1	測試	服務類別2	HARDWARE ONSITE SUPPORT
接單編號		保固期限	
報修時間	2011/09/16 10:52	負責工程師	郭璨棠
* 問題概述	配合雲嘉區網資安演練 區網路由器檢測		

作業說明:

2011/09/16 11:06 郭璨棠　服務等級: P3　狀態: 服務紀錄單已登錄
服務紀錄單登錄成功!!
2011/09/16 11:10 郭璨棠　服務等級: P3　狀態: 工程師處理中
回應客戶登記:
10:52 接獲通知演練開始.
10:58 以遠端透過out-of-band 線路(ADSL) 連線進TANET 6509檢查.
11:00 回報CPU / 界面 / 路由正常.

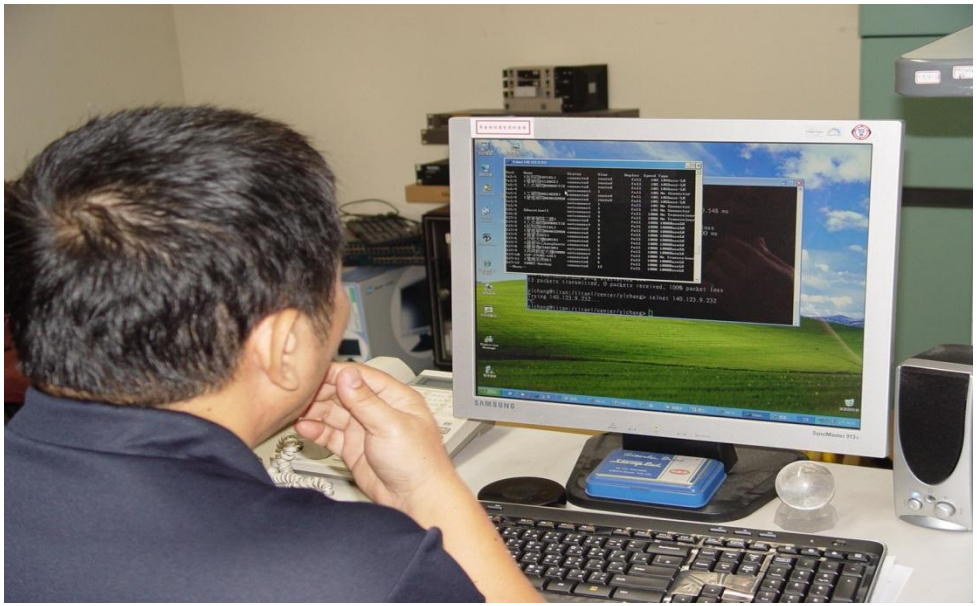
故障品	廠牌	品名/規格	數量	序號	故障原因

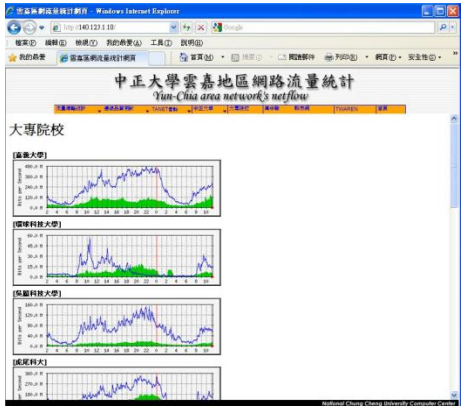
客戶簽名:　工程師簽名:　主管簽名:

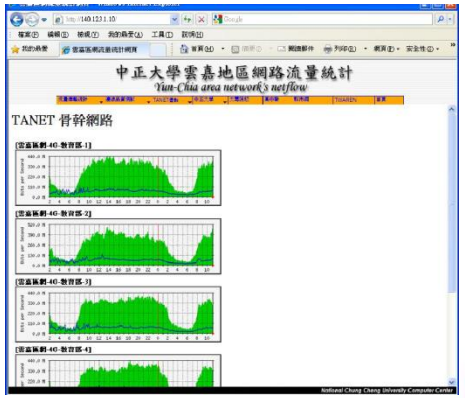
CCU Computer Center

網路復原測試

- 區網負責人員進行網路復原測試，確認連線狀況。







CCU Computer Center

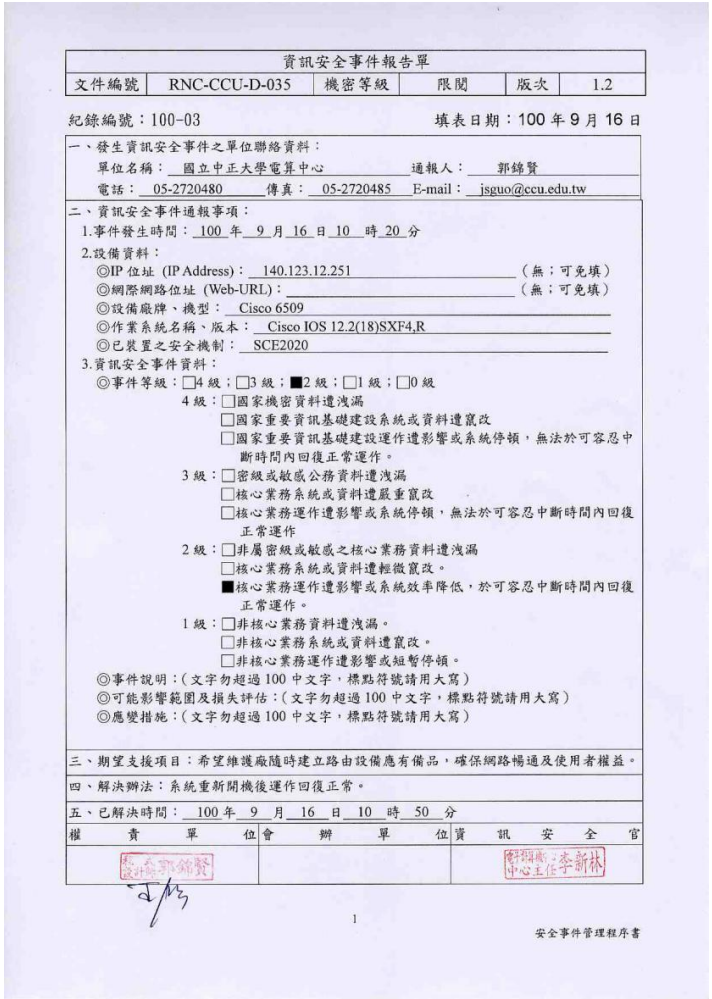
學籍系統連線檢測

- 執行ping指令檢查網路連線狀況。
- 經檢測學籍系統發現，網路線品質不良，負責人更換網路線。
- 負責人登錄連線測試，確認系統功能正常。

CCU Computer Center

資訊安全事件報告單(1/2)

- 由區網網路維運人員依現況填報資安訊安全事件報告單並由資訊安全官簽核確認。



資訊安全事件報告單

文件編號	RNC-CCU-D-035	機密等級	限閱	版次	1.2

紀錄編號：100-03　　填表日期：100 年 9 月 16 日

一、發生資訊安全事件之單位聯絡資料：

單位名稱：國立中正大學電算中心　通報人：郭錦賢

電話：05-2720480　傳真：05-2720485　E-mail：jsguo@ccu.edu.tw

二、資訊安全事件通報事項：

1.事件發生時間：100 年 9 月 16 日 10 時 20 分

2.設備資料：

◎IP 位址 (IP Address)：140.123.12.251　（無：可免填）

◎網際網路位址 (Web-URL)：　（無：可免填）

◎設備廠牌、機型：Cisco 6509

◎作業系統名稱、版本：Cisco IOS 12.2(18)SXF4,R

◎已裝置之安全機制：SCE2020

3.資訊安全事件資料：

◎事件等級：□4 級；□3 級；■2 級；□1 級；□0 級

4 級：□國家機密資料遭洩漏
□國家重要資訊基礎建設系統或資料遭竄改
□國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

3 級：□密級或敏感公務資料遭洩漏
□核心業務系統或資料遭嚴重竄改
□核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作

2 級：□非屬密級或敏感之核心業務資料遭洩漏
□核心業務系統或資料遭輕微竄改。
■核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

1 級：□非核心業務資料遭洩漏。
□非核心業務系統或資料遭竄改。
□非核心業務運作遭影響或短暫停頓。

◎事件說明：(文字勿超過 100 中文字，標點符號請用大寫)

◎可能影響範圍及損失評估：(文字勿超過 100 中文字，標點符號請用大寫)

◎應變措施：(文字勿超過 100 中文字，標點符號請用大寫)

三、期望支援項目：希望維護廠隨時建立路由設備應有備品，確保網路暢通及使用者權益。

四、解決辦法：系統重新開機後運作回復正常。

五、已解決時間：100 年 9 月 16 日 10 時 50 分

權責單位	會辦單位	資訊安全官
郭錦賢		李新林

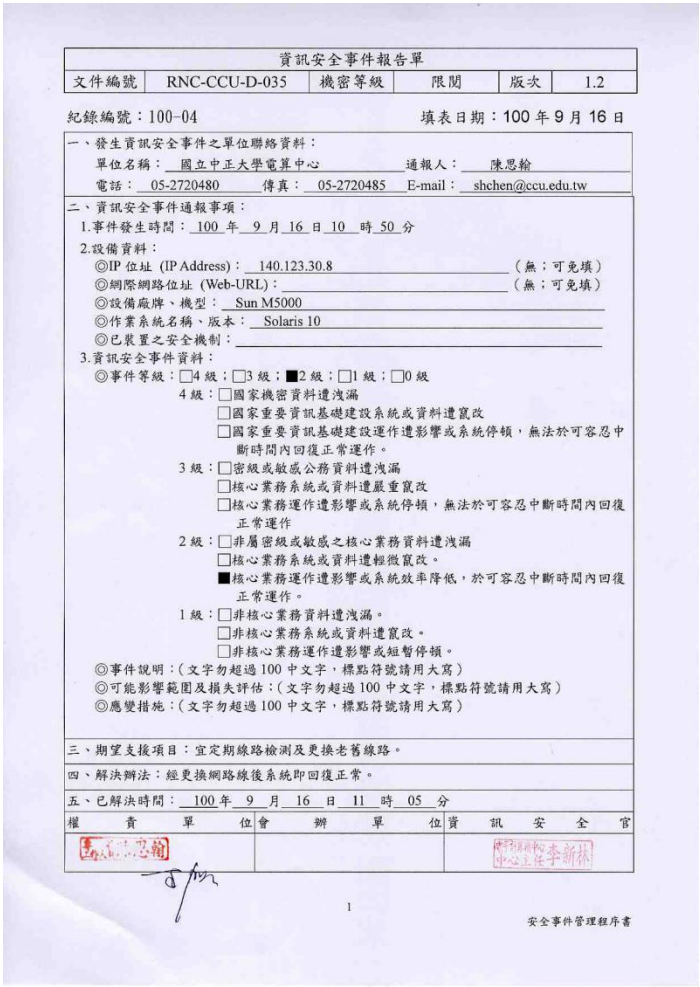
1

安全事件管理程序書

CCU Computer Center

資訊安全事件報告單(2/2)

- 由學籍系統負責人依現況填報資安訊安全事件報告單並由資訊安全官簽核確認。



資訊安全事件報告單

文件編號	RNC-CCU-D-035	機密等級	限閱	版次	1.2

紀錄編號：100-04　　填表日期：100 年 9 月 16 日

一、發生資訊安全事件之單位聯絡資料：
單位名稱：國立中正大學電算中心　通報人：陳恩翰
電話：05-2720480　傳真：05-2720485　E-mail：shchen@ccu.edu.tw

二、資訊安全事件通報事項：
1.事件發生時間：100 年 9 月 16 日 10 時 50 分
2.設備資料：
◎IP 位址 (IP Address)：140.123.30.8　（無；可免填）
◎網際網路位址 (Web-URL)：　（無；可免填）
◎設備廠牌、機型：Sun M5000
◎作業系統名稱、版本：Solaris 10
◎已裝置之安全機制：
3.資訊安全事件資料：
◎事件等級：□4 級；□3 級；■2 級；□1 級；□0 級
4 級：□國家機密資料遭洩漏
□國家重要資訊基礎建設系統或資料遭竄改
□國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。
3 級：□密級或敏感公務資料遭洩漏
□核心業務系統或資料遭嚴重竄改
□核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作
2 級：□非屬密級或敏感之核心業務資料遭洩漏
□核心業務系統或資料遭輕微竄改。
■核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。
1 級：□非核心業務資料遭洩漏。
□非核心業務系統或資料遭竄改。
□非核心業務運作遭影響或短暫停頓。
◎事件說明：(文字勿超過 100 中文字，標點符號請用大寫)
◎可能影響範圍及損失評估：(文字勿超過 100 中文字，標點符號請用大寫)
◎應變措施：(文字勿超過 100 中文字，標點符號請用大寫)

三、期望支援項目：定定期線路檢測及更換老舊線路。

四、解決辦法：經更換網路線後系統即回復正常。

五、已解決時間：100 年 9 月 16 日 11 時 05 分

權責單位	會辦單位	資訊安全官
[redacted]		[redacted]

1

安全事件管理程序書

CCU Computer Center

事件處理回報

- 各系統負責人向資訊安全官(李副校長)回報事件處理狀況。

CCU Computer Center