資通安全外部稽核表　單位：＿＿＿＿＿＿＿＿＿＿　稽核人員：＿＿＿＿＿＿＿＿＿＿　單位主管：＿＿＿＿＿＿＿＿

項目	查　　核　　項　　目	檢查方式	良好	尚可	不足
1	軟硬體資產是否列有清冊及專人保管	設備清冊			
2	資訊設備內Default帳號的Password是否變更				
2.1	PC內的Administrator	請使用者輸入密碼(在旁觀察密碼長度，並詢問變更週期)注意：空白密碼與過度簡易密碼			
2.2	防火牆的Administrator				
2.3	資料庫(SQL的SA)				
2.4	無線網路基地台(多User)之Administrator				
3	個人電腦不使用時是否有關機、或登出、或設定螢幕通行碼或其他控制措施進行保護？	螢幕保護程式、密碼保護			
4	是否全面使用防毒軟體並即時更新病毒碼？	檢查是否安裝防毒軟體、防毒軟體是否啓動			
5	是否定期執行各項系統漏洞修補程式？				
5.1	PC的作業系統	Windows Update			
5.2	辦公室自動化軟體(Office、MSN)	Windows Update office update (需要使用office 原版光			
5.3	防火牆作業系統	視設備而定			
5.4	無線網路基地台之作業系統	視設備而定			
6	重要的資料及軟體是否定期作備份處理？	詢問備份方式、週期			
7	是否使用網路防火牆？				
7.1	是否關閉不需使用的Port (如僅開放 上網及mail接收)	視設備而定			
8	是否定期檢測網路運作環境之安全漏洞？	掃描報告已用Emil 通知			
9	對於敏感性資訊之傳送是否採取資料加密等保護措施？	詢問加密方式，如HTTPS、 RAR			
10	PC的安全措施				
10.1	檢查是否有公用資料匣及設定存取權限(建議每六個月檢查一	參考附件1			
10.2	通行碼長度是否超過八個字元？				
10.3	通行碼是否規定需有大小寫字母、數字及符號組成？				
10.4	通行碼輸入錯誤，是否訂有三次以下之限制？				
10.5	是否規定避免使用與個人有關資料（如生日、身份證字號、單位簡稱、電話號碼等）當做通行碼？				
10.6	是否限制登入失敗次數的上限(建議三次)並中斷連線？				

10.7	是否限制登入失敗次數超過上限時需強制延遲一段時間或重新取得授權後才可再登入？				
10.8	是否定期檢查並刪除重覆或閒置的使用者識別碼？	我的電腦(右鍵)【管理】-【本機使用者和群組】【使用者】 建議停用非使用之帳號			
10.9	對於異常登入程序，是否留有紀錄，並有專人定期檢視？	檢查：【開始】-【程式集】-【系統管理工具】-【事件　檢視器】 設定位置：參考附件1			
10.10	機密及敏感性資料的處理是否採用專屬(隔離)的電腦作業環				
10.11	對於異常事件及其他資訊安全事件是否產生稽核日誌？				
10.12	稽核日誌之記錄內容是否包括使用者識別碼、登入登出之日期時間、電腦的識別資料或其網址及事件描述等事項？				
10.13	系統日誌是否保留				
10.14	PC內關閉不需使用的Service	【開始】-【程式集】-【系統管理工具】-【服務】			
10.15	**Terminal Service**	【開始】-【程式集】-【系統管理工具】-【服務】			
10.16	**Telenet Service**	【開始】-【程式集】-【系統管理工具】-【服務】			
10.17	**IIS Service**	【開始】-【控制台】-【新增移除程式】-[新增移除windos元件] IIS(要按下詳細資料查詢)			
10.18	**Ftp Service**				
10.19	**檢查Schedule Task (是否有不明程式被啓動)**	檢查c:\winnt\schedlgu.txt 可寄回國科會分析			
11	**無線網路使用之管控措施 (鎖MAC或WEP)**	視設備而定			