NCHU 全機關 ISMS 內稽 一般單位 稽核軌跡

受稽時間：

受稽單位：

受稽人員：

稽核人員：

管理面/制度面			
序	項目	內容	其它說明
1.	訪談問題 與會人員？	Q1. 組織對於全校導入之看法或規劃？ Q2. 單位業務對於代理人員之管理？實質代理？虛位代理？ Q3.	
2.	內部對於資安問題和做為的討論? 是要括必要項之討論與決議記錄? 關注者清單及利害關係者關注議題之討論 外部聯絡清冊		

管理面/制度面			
序	項目	內容	其它說明
3.	矯正 前次次要不符合？		
4.	是否有相關事件故發生		
5.	資產盤點?總數? 風險值區問? 資通系統清冊/系統分級? 資訊資產清冊與風險評鑑工作表的項目要一致		

管理面/制度面			
序	項目	內容	其它說明
6.	個資盤點結果/筆數 盤點時間及風險評鑑記相關錄 是否有境外傳遞個資？ 負責單位？主要交換項目(個資資料)？		
7.	重大組織變革或異動？ 重要設備之加入？		
8.	個資/資安窗口？ 負責人員？ 公用信箱/電話		

管理面/制度面			
序	項目	內容	其它說明
9.	環境安全? 是否有獨立機房? 文件庫房安全性（具個資資料之理）?		
10.	帳號清查 資通系統名稱？OS 版本/DB 版本/Web 工具 （IIS/Apache Tomcat/Nginx/XAMPP）		
11.	年度教育訓練時間及與會者/成效/有效性評估方式 一般人員 系統人員		

管理面/制度面			
序	項目	內容	其它說明
12.	委外合約抽查	安全條款 禁用大陸品牌/人員/設備 雲端服務?	

系統面/技術面-			
序	項目	內容	其它說明
13.	帳號、密碼之長度與強度 初始密碼之變更(抽檢)；定期變更密碼		
14.	帳號申請；權限控管與定期審核權限、 共用帳號(admin)		

系統面/技術面-			
序	項目	內容	其它說明
15.	防毒系統、病毒碼更新、使用期限(合約期滿)		
16.	防火牆規則審查；防火牆 proxy 備份		
17.	螢幕淨空、螢幕保護機制設定		
18.	鐘訊同步：線上、開發、測試、DB、LOG、CCTV、防火牆、環控、流量監控、門禁、刷卡機等主機		

系統面/技術面-			
序	項目	內容	其它說明
19.	系統需求單之審核、傳送、驗收紀錄→簡易變更管理		
20.	程式修改：版本如何控管、如何下載(有無帳密控管、存取紀錄)、修改前的核准程序		
21.	原始碼的管理：儲存、負責人、備份		
22.	AP 安全：測防呆、輸入錯誤、錯誤訊息顯示、逾時設定、帳密設定、連續錯誤登入測試		

系統面/技術面-			
序	項目	內容	其它說明
23.	申請單上最好有：申請日期、地點等欄位		
24.	資安政策、規定：如何讓委外供應商知悉、遵守		
25.	SQL injection 測試： 1.使用者帳號 ‘or 1=1-- ,密碼任意輸入 2.使用者帳號 abcdefg (任意輸入)， 密碼 asdf (任意輸入) ' or 1=1 – 密碼' or 'a'='a 3.取用客戶端送進來的資料前，先刪除所有可能造成問題的特殊字元，這些字元包括單引號（'）、雙引號（"）、問號（?）、星號（*）、底線（_）、百分比（%）、Ampersand（&）等，這些特殊字元都不應該出現在使用者輸入資料中		

系統面/技術面-			
序	項目	內容	其它說明
	-- 符號後的任何敘述都會被當作註解 「/*」 MySQL 「--」 MsSQL		
26.	應用程式是否擁有 db_owner 權限：攻擊者有可能讀取或寫入在被攻陷的資料庫裡的所有資料，攻擊者也有可能移除表格，建立新物件，並掌控被攻陷的資料庫		
27.	避免直接將「sa」帳號(管理所有資料庫權限)用於應用程式中：搜尋測試 資料庫管制方面： 1.Sa 管理帳號的密碼管控 2.所有範例表格以及不需使用的 stored procedure 加以移除 3.測試資料之模糊或虛擬化		
28.	網頁程式撰寫安全： 1.過濾輸入條件中可能隱含的 sql 指令，如 INSERT、SELECT、UPDATE		

系統面/技術面-			
序	項目	內容	其它說明
	等 2.針對輸入條件進行規範，如無必要，應規範為僅可接受大小寫英文字母與數字等 3.針對特殊的查詢參數進行過濾，如--、 ' 等可利用 replace(xx, "'", "''") 進行替換 4.使用參數化的查詢並避免使用動態式的查詢 5.避免使用 GET 的方式傳遞資料盡量採用使用 POST 方式傳遞資料，可以減少資料洩漏的機會。透過 GET 傳遞的資料會顯示在網址列，使用者無意瀏覽到惡意網頁時，透過 GET 傳遞的資料容易發生被截走的風險（Hijacking）。 6.進行程式寫作時，應時常檢查程式是否存在有非預期輸入資料的漏洞。		
29.	網站伺服器： 1.定期修補作業系統與網站伺服器的		

系統面/技術面-			
序	項目	內容	其它說明
	漏洞 2.避免 ASP、PHP 與 JSP 程式源碼洩漏，造成使用者可以 直接瀏覽 3.更改預設的網站虛擬路徑，如 IIS 系統不要使用預設的 C:\Inetpub\WWWRoot\的目錄 4.不提供錯誤訊息給使用者 (1)攻擊者可藉由回報的錯誤訊息得知資料庫的結構 (2)建議將錯誤輸入重導到適當網頁 (3)修改 C:\WINNT\Help\iisHelp\common\500-100.asp 的預設錯誤網頁		
30.	檢查電腦有無更改密碼： cmd > net user (看有多少帳號) cmd > net user username linux lastlog 每個帳號最近的登入時間 w 目前誰在系統上面 chang –l 帳號名		

系統面/技術面-			
序	項目	內容	其它說明
31.	日誌的留存 1. 作業系統日誌(OS event log) 2. 網站日誌(web log) 3. 應用程式日誌(AP log) 4. 登入日誌(logon log)		
32.	備份管理		
33.	系統弱點掃描修補情形？ 滲透測試？ 資安健診？ VNAS 的導入		