教育機構99年度C、D級機關學校

資訊安全稽核報告書

教育部98年度提升校園資訊安全服務計畫

執行團隊：安侯企業管理股份有限公司

中　華　民　國　99　年　12　月　31　日

目　　錄

壹、 依據

行政院國家資通安全會報「政府機關(構)資訊安全責任等級分級作業施行計畫」。

貳、 目的

為強化教育體系各級單位資訊安全管理制度及業務之落實，教育部乃針對部屬館所、學院、專科及高中職等類別擇定 25 個單位，委由安侯企業管理股份有限公司（以下簡稱 KPMG）辦理資訊安全管理制度外部稽核服務。

參、 稽核作業準備

一、教育訓練

（一）針對 C、D 級機關學校(共約 550 所學校、750 人)辦理外部稽核活動說明，並進行「教育部 99 年度 C、D 級機關學校資訊安全稽核計畫」說明暨「資訊安全內部稽核技巧」教育訓練。

（二）教育訓練內容

1、 資訊安全稽核理論與實務。
2、 教育體系常見之資安稽核發現。
3、 修正後「個人資料保護法」對教育機構之衝擊。
4、 99 年 C、D 級機關學校資訊安全稽核計畫說明。

（三）「教育部 99 年度 C、D 級機關學校資訊安全稽核計畫」說明暨「資訊安全內部稽核技巧」教育訓練場次如下：

課程時間安排	課程時數	上課地點
99/06/03（四） 14:00~16:00	2 小時	集思台大會議中心柏拉圖廳(台北市羅斯福路四段 85 號 B1)
99/06/04（五） 14:00~16:00	2 小時	高雄大學綜合一演講廳(高雄市楠梓區高雄大學路 700 號)
99/06/07（一） 14:00~16:00	2 小時	中興大學農學院國際會議廳(台中市南區國光路 250 號)
99/06/10（四） 14:00~16:00	2 小時	寶桑國小 401 大研習教室（臺東市四維路二段 23 號）

二、工作說明會

（一）「教育部 99 年度 C、D 級機關學校資訊安全稽核計畫」說明會：

1、99 年 6 月 18 日(五) 上午於教育部電算中心舉行。

2、協助受稽核學校了解稽核依據、稽核流程、稽核前準備工作、稽核時間安排方式等相關事宜。

3、邀請本部 98 年遴選之 15 所資訊安全管理制度導入種子學校人員，擔任受稽核學校 ISMS 導入輔導，協助受稽核學校完成稽核準備事宜。

4、協助配對輔導單位與受稽核單位結果如下：

受稽核單位	縣市	輔導單位	縣市
北區			
私立南亞技術學院	桃園縣	N/A<已導入 ISO27001>	
華夏技術學院	臺北縣		
大華技術學院	新竹縣	國立新竹教育大學	新竹市
私立德霖技術學院	臺北縣		
中華科技大學（原私立中華技術學院）	台北市	明新科技大學	新竹縣
臺北市立內湖高級工業職業學校	台北市		
私立亞東技術學院	臺北縣	中華大學	新竹市
國立新竹高級中學	新竹市		
臺北市私立滬江高級中學	台北市	玄奘大學	新竹市
國立新莊高級中學	臺北縣		
私立崇右技術學院	基隆市	國立宜蘭大學	宜蘭縣
國立基隆女子高級中學	基隆市		
國立頭城高級家事商業職業學校	宜蘭縣		
中區			
私立環球技術學院	雲林縣	N/A <已導入教版 ISMS>	
國立金門技術學院（8 月改制科大）	金門縣	國立中興大學	台中市
國立金門高級農工職業學校	金門縣		
國立清水高級中學	台中縣	亞洲大學	台中縣
國立臺中女子高級中學	台中市	國立嘉義大學	嘉義市
南區			
私立南榮技術學院（8 月改制科大）	台南縣	南臺科技大學	台南縣
私立興國管理學院	台南縣		
國立中山大學附屬國光高級中學	高雄市	國立高雄大學	高雄市

國立內埔高級農工職業學校	屏東縣	國立高雄第一科技大學	高雄縣
國立臺南大學附屬高級中學	台南縣	高苑科技大學	高雄縣
國立臺南護理專科學校	台南縣	遠東科技大學	台南縣
東區			
私立慈濟技術學院	花蓮縣	慈濟大學	花蓮縣
國立臺東專科學校	台東縣		

（二）個人資料保護工作事項說明會

1、99 年 08 月 05 日（四）於教育部電算中心舉行。

2、協助各受稽核學校與種子學校，瞭解「個人資料保護工作事項」執行重點與稽核目標。

3、種子學校於個人資料保護作業輔導問題與討論。

（三）資安稽核輔導種子學校分區聯席會議

1、由參與「教育部 99 年度 C、D 級機關學校資訊安全稽核計畫」之資安稽核輔導種子學校，對於輔導經驗及常見問題進行討論分享。並交流輔導心得，以順利完成本計畫對於資安等級 C、D 級學校之輔導。

2、資安稽核輔導種子學校分區聯席會議場次如下：

分區	會議時間	會議地點	出席學校
北區	99/08/23（一） 10:00 – 12:00	KPMG 6801 會議室 （臺北市信義路五段 7 號 68 樓—台北 101 大樓）	明新科技大學 國立新竹教育大學 中華大學 玄奘大學 國立宜蘭大學 慈濟大學
中區	99/08/25（三） 14:00 – 16:00	國立中興大學 資訊科學大樓一樓會議室 （台中市國光路 250 號）	國立中興大學 國立嘉義大學 國立雲林科技大學 亞洲大學
南區	99/08/30（一） 14:00 – 16:00	國立高雄第一科技大學 行政大樓五樓 527 室 （高雄市楠梓區卓越路 2 號）	南臺科技大學 國立高雄大學 國立高雄第一科技大學 高苑科技大學 遠東科技大學

肆、 辦理 C、D 級單位資安稽核輔導訪視

一、稽核時程

稽核服務自 99 年 09 月 23 日至 99 年 12 月 03 日止。

二、稽核標準

（一）教育體系資訊安全管理規範

（二）教育機構個人資料保護工作事項

三、稽核對象

如下表：

類別	技術學院/專科學校	高中職學校
家數	13	12
學校名稱	■ 華夏技術學院 ■ 環球科技大學(原環球技術學院) ■ 大華技術學院 ■ 德霖技術學院 ■ 南亞技術學院 ■ 慈濟技術學院 ■ 興國管理學院 ■ 崇右技術學院 ■ 亞東技術學院 ■ 南榮技術學院 ■ 國立台南護理專科學校 ■ 國立金門大學 ■ 國立臺東專科學校	■ 台北市私立滬江高級中學 ■ 國立內埔高級農工職業學校 ■ 國立清水高級中學 ■ 國立新竹高級中學 ■ 國立新莊高級中學 ■ 國立臺南大學附屬高級中學 ■ 國立金門高級農工職業學校 ■ 台北市立內湖高級工業職業學校 ■ 國立基隆女子高級中學 ■ 國立頭城高級家事商業職業學校 ■ 國立中山大學附屬國光高級中學 ■ 國立臺中女子高級中學

四、各校稽核日期及稽核小組人員

如下表：

稽核日期	受稽學校名稱	稽核顧問	教育部代表
09 月 23 日（四）	華夏技術學院	謝昀澤 梁文典	黃專員淑薰 莊科員佳玲
09 月 29 日（三）	環球科技大學(原環球技術學院)	陳信榮 林姿華	徐科長連城
09 月 30 日（四）	大華技術學院	張祚豪 黃嬿儒	黃專員淑薰 莊科員佳玲
10 月 05 日（二）	私立德霖技術學院	謝昀澤 楊家豪	黃專員淑薰 莊科員佳玲
10 月 07 日（四）	私立南亞技術學院	張祚豪 黃嬿儒	林組長瑞龍
10 月 11 日（一）	臺北市私立滬江高級中學	張祚豪 洪敏峰	趙偉傑
10 月 15 日（五）	國立內埔高級農工職業學校	陳信榮 黃嬿儒	塗正良
10 月 19 日（二）	國立清水高級中學	陳信榮 楊家豪	徐科長連城
10 月 21 日（四）	國立新竹高級中學	謝昀澤 張祚豪	趙偉傑
10 月 25 日（一）	國立新莊高級中學	陳信榮 梁文典	林組長瑞龍
10 月 27 日（三）	私立慈濟技術學院	林姿華 梁文典	黃專員淑薰 莊科員佳玲
11 月 02 日（二）	私立興國管理學院	張祚豪 林茹玉	塗正良
11 月 03 日（三）	私立崇右技術學院	陳信榮 洪敏峰	黃專員淑薰 莊科員佳玲
11 月 04 日（四）	國立臺南大學附屬高級中學	楊家豪 梁文典	林組長瑞龍
11 月 11 日（四）	私立亞東技術學院	林姿華 楊家豪	林組長瑞龍

稽核日期	受稽學校名稱	稽核顧問	教育部代表
11 月 15 日（一）	私立南榮技術學院	林茹玉 梁文典	林組長瑞龍
11 月 16 日（二）	國立臺南護理專科學校	林姿華 梁文典	塗正良
11 月 17 日（三）	國立金門高級農工職業學校	王吉祥	黃專員淑薰 莊科員佳玲
11 月 18 日（四）	國立金門技術學院（已改制為國立金門大學）	王吉祥	黃專員淑薰 莊科員佳玲
11 月 22 日（一）	臺北市立內湖高級工業職業學校	謝昀澤 林姿華	林組長瑞龍
11 月 25 日（四）	國立臺東專科學校	梁文典 洪敏峰	趙偉傑
11 月 29 日（一）	國立基隆女子高級中學	梁文典 呂易儒	趙偉傑
11 月 30 日（二）	國立頭城高級家事商業職業學校	黃嬿儒 呂易儒	林組長瑞龍
12 月 02 日（四）	國立中山大學附屬國光高級中學	楊家豪 梁文典	塗正良
12 月 03 日（五）	國立臺中女子高級中學	楊家豪 梁文典	徐科長連城

五、稽核方式

（一）資訊安全文件制度查核

1、 檢視書面制度之完整性、可行性與一致性。

2、 表單與相關紀錄填寫之落實性。

（二）資訊安全控制作業程序查核

1、 檢視現行資訊安全控制作業是否與文件要求一致。

2、 測試控制作業是否有效（如：系統設定、權限管理）。

（三）實體環境訪視。以實地訪視方式，確認下列項目之管理情形

1、 機房進出門禁管理

2、 機房環境管理

3、 消防管理

4、 實體安全管理

（四）作業系統查核，視需要檢視下列項目

1、 存取權限控制

2、 使用者帳號授權程序

3、 帳戶與通行碼原則

4、 稽核與監控功能

5、 系統服務

（五）應用系統查核，視需要檢視下列項目

1、 應用系統程式開發、維護測試與上線程序

2、 應用系統帳戶與通行碼原則

3、 使用者帳號授權程序

4、 存取權限授權程序

5、 稽核與監控功能

（六）資料庫系統查核，視需要檢視下列項目

1、 帳戶與通行碼原則

2、 使用者帳號授權程序

3、 存取權限授權程序

4、 稽核與監控功能

（七）網路與連線作業查核。

（八）資訊安全事件管理查核。

六、稽核項目

1、適用性聲明書之確認

2、ISMS 建置步驟

3、ISMS 建置需求

4、資訊安全政策訂定與評估

5、資訊安全組織

6、資訊資產分類與管制

7、人員安全管理與教育訓練

8、實體與環境安全

9、通訊與作業安全管理

10、存取控制安全

11、系統開發與維護之安全

12、資訊安全事件之反應及處理

13、業務永續運作管理

14、相關法規與施行單位政策之符合性

15、個人資料保護

伍、稽核成果彙整

一、稽核評估方式

依學校落實辦理教育體系資訊安全管理規範與教育機構個人資料保護工作事項的控制措施之完整性進行評估，並分為「非常完整」、「尚屬完整」、「不盡完整」及「不適用」等四種評等。

二、稽核評等

接受稽核輔導服務之 25 所學校中，整體資訊安全管理制度導如情形及個人資料保護工作事項施行完整度，總評為非常完整者共有 6 家（佔 24%），尚屬完整者共有 19 家（佔 76%）。若依「技術學院／專科學校」及「高中職學校」進行區分分析如下：

（一）技術學院／專科學校類別共13所，其中評等為非常完整者佔 23%，尚屬完整者占77%。

（二）高中職學校類別共12所，其中非常完整佔25%，尚屬完整者占75%。

彙整如下表：

類別	非常完整		尚屬完整		不盡完整		合計	
	家數	%	家數	%	家數	%	家數	%
技術學院／專科學校	3	23%	10	77%	0	0	13	100%
高中職學校	3	25%	9	75%	0	0	12	100%
合計	6	24%	19	76%	0	0	25	100%

三、資安稽核作業績優單位

本年度 C、D 級機關學校資訊安全稽核作業經評等為『非

常完整』之績優單位共 6 所學校，C 級單位(技術學院／專科學校)有 3 所學校，D 級單位(高中職學校)有 3 所學校，績優學校與協助導入之輔導種子學校如下表：

類別	學校名稱	輔導種子學校
技術學院／專科學校	私立大華技術學院	國立新竹教育大學
技術學院／專科學校	私立南亞技術學院	N/A<已導入 ISO27001>
技術學院／專科學校	私立亞東技術學院	中華大學
高中職學校	國立內埔高級農工職業學校	國立高雄第一科技大學
高中職學校	國立新竹高級中學	中華大學
高中職學校	國立臺中女子高級中學	國立嘉義大學

四、常見缺失

依據本次稽核之結果，提出資訊安全常見缺失與個人資料保護常見缺失摘要如下：

（一）資訊安全常見缺失

1、內部或委外人員未簽署資訊安全保密切結書。

2、委外合約未有資安規定之條款，例如保密條款、智慧財產權保護等。

3、設備攜出或攜入安全區域未落實登記留有記錄。

4、防毒軟體病毒碼未即時更新。

5、未定期審查資訊系統或資料庫之管理者帳號與權限。

6、共用帳號與通行碼

7、使用者通行碼為符合複雜度要求，或未定期變更。

8、電腦內發現未經授權之軟體。

9、未落實文件管理程序。

（二）個人資料保護常見缺失

1、電腦內儲存之學生個人資料，未有適當之加密措施。

2、學生個人資料紙本資料儲存場所之資料儲存櫥櫃，未有適當控管措施。

3、學生個人資料之調閱未留有相關調閱記錄。

4、處理個人資料相關人員未依規定簽訂保密切結書。

5、未控管委外廠商存取學生個人資料。

五、綜合建議

（一）資訊安全建議

1、建議落實資安工作執行表單記錄之填寫，並進行抽查以確認執行狀況。

2、建議清查內部與委外人員資安保密切結書之簽署，並核對相關資料之正確性。

3、建議參考教育部相關合約範本條款內容，針對委外合約增修資訊安全相關條款。

4、建議落實資訊資產清冊之更新與維護。

5、建議落實資訊機房設備攜出入管制。

6、建議設定防毒軟體即時自動更新病毒碼，並定期檢查更新是否成功。

7、建議確認已啟動以通行碼保護之螢幕保護程式。

8、建議確認重要校務系統資訊與資料庫之備份。

9、建議落實使用者帳號與通行碼之管制，不共用帳號，並依規定設定通行碼複雜度且定期變更。

10、建議定期查核並移除電腦中未有合法版權之軟體。

（二）個人資料保護建議

1、建議宣導個人資料保護認知，並提供文件基本加密方法之教育訓練供同仁參考，針對電腦中個人資料檔案進行加密。

2、建議應以具備上鎖功能之安全櫥櫃，存放教職員生個人資料紙本，過期資料並應予確實銷毀。

3、建議重要學生個人資料之調閱與存放場所之進出，應予以紀錄。

4、建議處理個資相關人員簽訂保密切結書，並告知相關人員個資保護之責任。

5、建議區隔重要校務系統之程式與資料管理，避免委外廠商接觸學生個人資料。

陸、結論

一、教育體系資訊安全管理制度之推動

綜觀教育體系資訊安全管理制度之推動情形如下：

類別	內　　容	資訊安全管理制度（ISMS）推動情形
A 級 重要核心	‧教育政策主管機關（教育部） ‧教學醫院（台大醫院、成大醫院）	已通過 ISMS 第三方驗證。
B 級 核心	‧6 所入學考試常設機構 ‧105 所大學 ‧13 個 TANet 區網中心 ‧25 個縣/市網中心 ‧陽明大學附設醫院	約 80%單位已通過 ISMS 第三方驗證。
C 級 重要	‧44 所技術學院及 15 所專科學校 ‧24 個部屬館所	辦理 C、D 級機關學校資訊安全稽核計畫，98 年度挑選 20 校/99 年度挑選 25 校進行稽核輔導。
D 級 一般	‧486 所高中職學校 ‧3,398 所國中小學	

對照資安等級 A、B 級單位經過多年宣導推廣，C、D 級學校相對缺乏資源及人力施行資訊安全管理制度，其中普通高中因缺乏專業資訊科系教師，施行資訊安全管理制度尤其需要協助及輔導。

建議持續辦理「C、D 級機關學校資訊安全稽核計畫」，藉由相關教育訓練加強學校資訊管理人員的資安觀念，並透過資安稽核輔導活動，強化學校管理階層對於資訊安全的重視。

二、教育體系資訊安全管理制度（ISMS）稽核輔導

99 年度「C、D 級機關學校資訊安全稽核計畫」為強化已通

過資訊安全管理制度（ISMS）第三方驗證機制之種子學校，對於資訊安全輔導之能量，除了在數次工作說明會中對於輔導技巧及溝通進行說明，並特別針對種子學校召開「資安稽核輔導種子學校分區聯席會議」。

故而此次資安稽核輔導成果較 98 年度「C、D 級機關學校資訊安全稽核計畫」成效更佳，受稽核學校大多接受充足的輔導並充分準備相關稽核事項。

建議持續增加或推動資安等級 B 級學校共同輔導 C、D 級學校，並可運用與相關會議及教育訓練，加以宣導推廣資訊安全區域性聯合防護的觀念。