檔　　號：
保存年限：

教育部　函

地址：臺北市中山南路5號
傳真：(02)2737-7043
聯絡人：塗正良
聯絡電話：(02)8732-9045

受文者：電算中心
發文日期：中華民國96年12月19日
發文字號：台電字第0960196582號
速別：普通件
密等及解密條件或保密期限：普通
附件：教育部機關學校資通安全工作事項（196582.DOC，共1個電子檔案）

裝

主旨：各機關、學校應編列經費落實資通安全工作事項，資訊安全長(副首長以上)應加強監督執行情形，請 查照。

說明：

一、檢送「教育部所屬機關及各公私立學校資通安全工作事項」。

訂

二、各縣市政府教育局請轉知所屬國中小學，並協助監督考核執行情形。

正本：公私立大專院校、公私立高級中等學校、各縣市政府教育局、部屬機關、國立小學、附設醫院、農林場、臺灣學術網路區域網路中心、各縣市教育網路中心
副本：本部高教司、政風處、技職司、中教司、國教司、中部辦公室、體育司、教研會、電算中心(副本均含附件)

線

部長 杜正勝

教育部所屬機關及各級公私立學校資通安全工作事項

依據教育部中華民國 96 年 12 月 19 日台電字第 0960196582 號函

壹、 資訊安全責任等級分級：

一、 機關學校應參考「資訊安全責任等級分級」及本部相關規定，執行相關資訊安全管理工作，各縣(市)政府應協助所轄中小學執行資訊安全工作。

二、 依據行政院於 94 年 7 月 21 日核定「政府機關（構）資訊安全責任等級分級作業施行計畫」，各資訊安全責任等級分級應執行工作項目如下：

作業 / 內容 / 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/SOC、IDS、防火牆防毒	96 年通過第三者認証	每年至少執行二次內稽	(4,6,18,4 小時)/每年	96 年資安專業鑑定證照二張
B級	強度等級 3	SOC(OP) IDS、防火牆防毒	97 年通過第三者認証	每年至少執行一次內稽	(4,6,18,4 小時)/每年	96 年資安專業鑑定證照一張
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	(2,6,12,4 小時)/每年	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	(1,4,8,2 小時)/每年	資安專業訓練

資訊安全責任分級包含本部所屬機關及各公私立學校區分如下：

A 級：教育部、台大醫院、成大醫院

B 級：大學、區域網路中心、縣(市)教育網路中心

C 級：學院、專科學校、部屬館所

D 級：高中職、國中小學

貳、 資通安全通報應變：

一、 需配合「國家資通安全緊急應變中心」建立緊急通報應變組織，各機關學校應建立資訊安全長(副首長以上)及 2 位資訊安全聯絡人，並列入行政業務交接項目。

二、 2 位資訊安全聯絡人應於「國家資通安全應變網站」登入基本資料：
網址 https://www.ncert.nat.gov.tw 電話：(02)2733-9922

名稱	姓名	職稱	電話	傳真	行動電話	E-MAIL
第 1 聯絡人						
第 2 聯絡人						

三、 機關學校發現資安事件或接獲「國家資通安全會報」、本部等相關主管機關通知發生資安事件時，應於 1 小時內了解資安事件情形進行相關事件應變處理，最晚應於 24 小時內至「國家資通安全應變網站」進行資安事件通報，並於 36 小時內處理完成或完成損害控制後至進行結案通報。

四、 機關學校應配合「國家資通安全會報」及本部每年辦理資通安全攻防演練、

通報演練、社交工程演練等相關演練作業。

參、 資訊安全防護：

一、電腦網路使用安全注意事項：

（一）各機關學校應**酌參**「○○個人電腦使用注意事項(參考)」(如附件)，並考量網路環境狀況**訂定合適之「電腦網路使用安全注意事項」**並確實執行，以有效規範行政人員、教師、學生電腦網路使用安全。

（二）應建立網路使用安全稽核機制，並適當進行內部稽核或自我檢視。

二、網路安全管理：

（一）應設置**防火牆**並適當**阻絕外部**對內之網路連線及通訊埠。

（二）應訂定「網路安全管理作業規範」、建立網路對外服務**申辦作業**及安全檢查。

（三）網路安全**建立檢核機制**，並適當進行安全檢核。

三、電腦系統安全管理：

（一）應訂定「電腦設備安全管理作業規範」，以規範伺服主機及個人電腦作業系統建置安全，系統上線使用前應建立**申辦作業**及安全檢查。

（二）電腦設備作業系統及相關伺服軟體應適時**更新軟體**及進行漏洞修補。

（三）電腦設備作業系統應**安裝防毒軟體**並適時更新病毒資料庫。

（四）作業系統進行遠端維護時，應於**加密管道**進行，並管制維護來源 IP。

（五）電腦系統應建立**檢核機制**，並適當進行安全檢核。

四、應用軟體(網站)安全管理：

（一）應訂定「應用軟體安全管理作業規範」以規範應用軟體、資料庫、程式開發建置及使用安全，系統上線使用應建立**申辦作業**及安全檢查。

（二）**應用程式**所有輸入欄位應進行**字元檢查**，排除不必要特殊字元(如' "!$%^&*_|-><;等)以防止資料庫隱碼攻擊(SQL-injection)。

（三）應用程式進行遠端維護時，應於**加密管道**進行，並管制維護來源 IP。

（四）應用軟體應**建立檢核機制**，並適當進行安全檢核。

肆、 相關文件說明：

一、 教育體系資訊安全管理制度(ISMS)規範：

（一）教育體系資訊安全管理制度規範網址：
http://www.edu.tw/EDU_WEB/EDU_MGT/MOECC/EDU0688001/tanet/fix.htm

（二）教育體系各機關適用對象如下：

1.「教育體系資通安全管理規範」第 1 群：適用教育部電算中心、部屬館所、縣(市)網中心及公私立大專院校。

2. 「教育體系資通安全管理規範」第 2 群：適用公私立高中職學校。

3. 「國中小學資通安全管理系統實施原則」：適用國中小學。

（三）教育體系資訊安全管理制度規範導入試作點範例—國立成功大學
http://www.edu.tw/EDU_WEB/EDU_MGT/MOECC/EDU0688001/tanet/fix.htm

附件

○○個人電腦使用注意事項(參考)

備註：學校應依行政人員、教師、學生各別訂定合適之注意事項

1. 禁止使用未經授權之電腦軟體。
2. 請勿任意拆卸或加裝其他電腦設備。
3. 不可擅自更改系統環境設定。
4. 密碼至少每三個月更換一次，密碼長度應至少 8 碼。
5. 電腦設備不可任意架站或做私人、營利用途。
6. 電腦設備應隨時保持清潔，每週至少擦拭一次。
7. 電腦附近請勿放置茶水、飲料、細小文具用品等物品，以免造成電腦設備損壞。
8. 使用外來檔案，應先掃毒，請勿任意移除或關閉防毒軟體。
9. 下班時，應先行關機始得離去，電腦關機應依正常程序操作。
10. 本○(機關學校)同仁應配合進行軟體更新，修補漏洞，保持更新至最新狀態，勿自行關閉系統自動更新程式。
11. Internet Explorer 等相關瀏覽器安全等級應設定為中級或更高，執行特殊程式如須降低安全性，請通知本中心進行安全檢查及管理。
12. 電子郵件軟體應關閉收信預覽功能,請勿任意開啟不明來源的電子郵件。
13. 電腦應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 10 分鐘以內。
14. 請勿開啟網路芳鄰分享目錄與檔案，並停用 Guest 帳號。
15. 請勿任意下載或安裝來路不明、有違反法令疑慮（如版權、智慧財產權等）或與本○業務無關的電腦軟體。
16. Microsoft Office 軟體(包括 Word、Excel、Powerpoint 等)應將巨集安全性設定為高級或更高，執行特殊程式如須降低安全性，請通知本中心進行安全檢查及管理。
17. **禁止使用點對點互連(P2P)軟體**及 tunnel 相關工具下載或提供分享檔案。
18. 禁止於上班時間使用即時訊息(如 MSN、yahoo Message 等），如業務必須使用，應提出申請，各單位主管應加強監督經許可同仁使用即時訊息情形。
19. 禁止於上班時間閱覽不當之網路(如暴力、色情、賭博、駭客、惡意

網站、釣魚詐欺、傀儡網路等)及瀏覽非公務用途網站，以避免內部頻寬壅塞，各單位主管應加強監督同仁使用網路情形。

20. 禁止使用外部網頁式電子郵件(Webmail)，各單位主管應加強監督同仁使用電子郵件(Webmail)情形，以避免漏洞產生。

21. 禁止於上班時間透過網路資源進行與工作內容無關之串流媒體、MP3、圖片、檔案等網路上的傳輸，非上班時間(中午休息、下班後)的使用，亦不得影響單位內主要系統運作之效率。

22. 同仁上網行為需以不影響各主系統之網路效能為前提，若有資源上的衝突，將以本〇主要系統為主。

23. 電腦內重要資料文件應定期備份，避免資料損毀。

24. 機密性敏感性檔案資料應進行實體隔離(與外部網路隔絕)。

25. 本〇每年不定期進行內部稽核，同仁若查有上開違失事項，依本〇獎懲要點規定議處。