教育部所屬機關及各級公私立學校資通安全工作事項

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「立法院審議96年度中央政府總預算—通案附帶決議事項」，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

立法院審議96年度中央政府總預算案所作決議事項

一、決議事項二、通案附帶決議事項第1點：

針對有關國家資訊安全會報所頒訂「各政府機關(構)資訊安全責任等級分級作業施行計劃」之內容，已將各級機關資安等級區分為A、B、C、D四個等級，定義各類資安系統等級應執行之工作事項，然網路威脅不僅僅只從外面侵入或系統的防護即可，組織內部同仁使用之個人電腦常在上網過程中，不知不覺遭入侵，成為危害資訊安全的漏洞。政府部門如何有效規範管理公務人員網際網路個人行為，特以此決議文之內容說明為基礎，做為各機關(構)人員網路安全管理之依據，以維護各機關(構)電腦資訊網路系統安全與使用者自身權益之相關事宜。

說明：

1. 各機關(構)需制定員工上網行為管理使用準則，禁止員工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)。
2. 非禁止之不當網站，需建立稽核管理機制，以避免員工過度使用導致內部頻寬壅塞及降低員工工作效率。
3. 禁止員工使用網頁式電子郵件(Webmail)，並建立管理機制，以避免漏洞產生。
4. 對於惡意行為的網站，需要有及時更新機制，以避免員工在因空窗期而感染必傳播惡意程式。
5. 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。
6. 非上班時間(中午休息、下班後)的使用，需建立稽核管理機制，不得影響單位內主要系統運作之效率。
7. 非經申請，禁止於上班時間使用即時訊息(Instant Message)、點對點檔案共享(P2P)及tunnel相關工具。
8. 經許可後使用之即時訊息及點對點檔案共享工作，需建立稽核管理機制，以避免資安漏洞產生。
9. 使用者不得於網際網路上下載及安裝非經許可之應用程式，以避免資安上的風險(木馬，Tunnel軟體，間諜程式，傀儡程式等)及違反法令之疑慮(著作權、版權)。
10. 員工上網行為所佔之單位內部頻寬，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，將以各主系統為主。
11 各機關(構)之機密文件，非經許可，不得透過網際網路工具(IM、P2P、WebMail)來進行傳輸及檔案交換。
12. 各機關(構)需建立稽核管理制度，以避免漏洞產生。
13. 各機關(構)需確實掌握時效，於資安問題發生時，在最短時間之內，彈性調整相關管理機制，以縮短資安空窗期。