檔　　號:
保存年限:

行政院 函

地址：100009 臺北市中正區忠孝東路1段1號
聯絡人：蘇煒哲
電話：(02)23808804
電子郵件：wcsu7589@acs.gov.tw

受文者：教育部

發文日期：中華民國112年8月29日
發文字號：院授數資安字第11250001503號
速別：普通件
密等及解密條件或保密期限：
附件：如說明三（50001503_4_教育部及所屬公務機關、所管特定非公務機關之資通安全責任等級核定表.ods）

主旨：貴部及所屬公務機關、所管特定非公務機關之資通安全責任等級業經核定，請查照。

說明：

一、復112年4月7日臺教資(四)字第1122701210號函暨同年5月18日臺教資通字第1122701918號函。

二、請貴部依核定之資通安全責任等級，積極辦理資通安全管理法各項規定事項，並持續督導機關辦理資通安全相關作業，以強化政府整體資安防禦能量。

三、檢附資通安全責任等級核定表1份。

正本：教育部
副本：電子公文交換章 2023/08/30 09:12:11

1120085579 收文日期:112/08/30

59	國立臺灣海洋大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
60	國立彰化師範大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
61	國立高雄師範大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
62	國立東華大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
63	國立暨南國際大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
64	國立屏東科技大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
65	國立臺灣科技大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
66	國立臺北科技大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
67	國立雲林科技大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
68	國立臺北護理健康大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
69	國立臺北大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
70	國立嘉義大學	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
71	國立臺南護理專科學校	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
72	國立臺東專科學校	大專校院	C	依據資通安全責任等級分級辦法第6條辦理
73	國立陽明交通大學	大專校院	B	依據資通安全責任等級分級辦法第6條辦理，並考量機關業務涉中山科學研究院及國防相關重要計畫，依同法第10條第2款調升等級。
74	國立臺灣大學生物資源暨農學院實驗林管理處	附設機構	C	依據資通安全責任等級分級辦法第6條辦理
75	國立臺灣大學生物資源暨農學院附設山地實驗農場	附設機構	D	依據資通安全責任等級分級辦法第7條辦理
76	國立臺灣大學生物資源暨農學院附設農業試驗場	附設機構	D	依據資通安全責任等級分級辦法第7條辦理
77	國立臺灣大學生物資源暨農學院附設動物醫院	附設機構	D	依據資通安全責任等級分級辦法第7條辦理
78	國立中興大學農業暨自然資源學院實驗林管理處	附設機構	C	依據資通安全責任等級分級辦法第6條辦理

附表五　資通安全責任等級C級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性；並應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		一、初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。

	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		初次受核定或等級變更後之一年內，至少一名資通安全專職人員，分別持有證照及證書各一張以上，並持續維持證照及證書之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、資通安全專職人員，指應全職執行資通安全業務者。

三、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

四、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

五、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。