教育部與所屬機關(構)及學校資通安全責任等級分級作業規定

一、依據：行政院一百零四年一月二十日院臺護字第一０四０一二一一一六號函頒之政府機關(構)資通安全責任等級分級作業規定。

二、目的：教育部(以下簡稱本部)為明確規範本部與所屬機關(構)及各級學校資通安全責任等級分級作業，透過資通安全（以下簡稱資安）管理，以防範潛在資安威脅，進而提升本部與所屬機關(構)及各級學校資安防護水準，特訂定本作業規定。

三、適用對象：

(一)本部及所屬機關(構)。

(二)各級學校及其附設醫院(包括醫學中心、區域及地區分院)。

(三)臺灣學術網路各區域網路中心、各直轄市及縣(市)教育網路中心。

(四)辦理各類考試、甄選、招生、評鑑等工作之試務機關(構)及評鑑機構。

四、分級原則

(一)依行政院函頒之政府機關(構)資通安全責任等級分級作業規定，資通安全責任等級區分為A級、B級、C級等三級。

(二)A級機關(構)及學校：

1.本部、臺灣大學醫學院附設醫院、成功大學醫學院附設醫院、國立陽明大學附設醫院。

2.承接具國家安全機密性或敏感性業務或技術研究之學院或系所，其研究領域如下：

(1)涉及國家安全資訊、國家機密資訊之領域：

①國土調查資訊。

②水域調查資訊。

③災害防救資訊。

④大陸及外交情資。

⑤軍事計畫、軍事行動資訊。

(2)涉及國家安全技術、國家機密技術領域：

①國防科技、軍事武器及元件製造技術。

②航太關鍵技術。

③衛星遙測關鍵技術。

④核子工程技術。

⑤資通安全、光電、IC、資通訊及精密機械等自主研發或關鍵技術。

⑥關鍵材料之製造技術。

⑦能源科技之關鍵技術。

⑧農業品種改良、栽培及繁養殖之關鍵技術。

⑨醫學、藥學及生物科技之關鍵技術。

3.辦理大學、技專校院及高級中等學校等入學考試、甄選、招生等工作之常設試務機構(詳如附表一）。

(三)B 級機關(構)及學校：

1.本部所屬機關。

2.本部所屬機構。

3.辦理專科學校、十二年國教入學考試、甄選、招生工作等輪流辦理之試務機構與學校(詳如附表二)、各項評鑑工作之評鑑機構。

4.臺灣學術網路各區域網路中心。

5.各直轄市及縣(市)教育網路中心。

6.各公私立大學。

7.大學附設醫院之區域分院及地區醫院。

(四)C 級學校：

1.第一類：各公私立專科學校、各公私立學院。

2.第二類：各公私立高級中等學校、各公私立國民中學、各公私立國民小學。

五、資訊安全管理及防護具體作法

(一)A 級機關(構)及學校具體作法如下：

1.資訊系統分類分級：

(1)參考行政院國家資通安全會報頒訂之資訊系統分類分級與鑑別機制參考手冊，對核心業務應用資訊系統就機密性、完整性、可用性及法律遵循性等影意構面，進行分類、鑑別及分級，建立相對應之防護基準：

①初期以新建或改版完成之資訊系統為主，採行適當之安全控制措施，後續再推動至各機關(構)及學校全部資訊系統，以確保資訊系統之安全防護水準。

②如已通過資訊安全管理驗證（例如：ISO/IEC 27001、CNS 27001 教育機構資安認證等），準用已採行之風險評鑑方法，轉換為本機制之普、中、高三個安全等級。

(2)承辦大學、技專校院及高級中等學校等入學考試、甄選、招生等工作之常設試務機構，亦應對承接之試務作業相關資訊系統進行分類、鑑別及分級。

2.資訊安全管理制度(ISMS)推動作業：

(1)導入資訊安全管理制度(ISMS)，對機關核心業務應用資訊系統(全部)進行資安風險評鑑、管控等作業，並通過第三方驗證。

(2)承辦大學、技專校院及高級中等學校等入學考試、甄選、招生等工作之常設試務機構，亦應導入資訊安全管理制度，將試務相關資訊系統，納入核心業務應用資訊系統，進行資安風險評鑑、管控等作業，並通過第三方驗證或教育機構資安認證。

3.資安專責人力：

(1)應指派二員具資安專業能力人員，專責執行資訊安全管理相關業務。

(2)承辦大學、技專校院及高級中等學校等入學考試、甄選、招生等工作之常設試務機構，亦須指派人員，對試務相關資訊系統進行資訊安全管理作業。

4.稽核方式：

(1)每年至少辦理二次內部資訊安全稽核作業。

(2)承辦大學、技專校院及高級中等學校等入學考試、甄選、招生等工作之常設試務機構，應於辦理試務前，對試務相關資訊系統及作業進行內部資訊安全稽核作業。

5.業務持續運作演練：

(1)各項核心業務應用資訊系統依實務需要訂定業務持續運作計畫。

(2)每年至少辦理一次核心業務應用資訊系統業務持續運作演練。

(3)承辦大學、技專校院及高級中等學校入學考試、甄選、招生等工作之常設試務機構，對核心試務業務訂定業務持續作計畫，並於辦理試務前進行演練。

6.縱深防護：

(1)對資訊網路環境建立縱深防護架構，包括下列防禦裝置及系統：

①防毒、防火牆、郵件過濾裝置。

②IDS/IPS、Web 應用程式防火牆。

③APT 攻擊防禦設備或系統。

(2)承辦大學、技專校院及高級中等學校等入學考試、甄選、招生等工作之常設試務機構，應將試務相關資訊系統納入學校整體網路環境之資安縱深防護架構中。

7.監控管理：結合臺灣學術網路資安監控系統(北區 SOC、南區 SOC、Mini-SOC、TACERT)或本部資安監控系統機制，進行資安預警情資、事件通報及應變處置。

8.安全性檢測：

(1)每年至少辦理二次安全弱點檢測作業，視資源能力優先選擇核心業務資訊系統(網站)，並對弱點進行修復作業。

(2)每年至少辦理一次滲透測試作業，視資源能力優先選擇核心業務資訊系統，並依測試結果強化網路及系統資安防禦能力。

(3)每年對重要核心資訊網路、設備及系統，至少辦理一次資安健診作業，實施網路架構檢視、有線網路惡意活動檢視、使用者端電腦檢視、伺服主機檢視及安全設定檢視等，並依檢測結果進行修復、調整作業。

(4)承辦大學、技專校院及高級中等學校等入學考試、甄選、招生等工作之常設試務機構，應於辦理試務作業前對資訊網路環境、設備及資訊系統實施資安健診及網站安全弱點檢測作業，並依檢測結果進行修復、調整作業。

9.資安教育訓練：

(1)資安人員或資訊人員應至少二員接受十二小時資安專業課程訓練(包括行政院、教育部、各級教學機構、各區網中心及各直轄市及縣(市)教育網路中心等辦理之資安課程、訓練、講習等)，並獲得研習證明，以增進資安專業知識與能力。

(2)一般使用者及主管至少須接受三小時資安宣導課程(包括機關自辦資安宣導講習、上級機關辦理之資安宣導課程)，並通過課程評量，以提升資安防護認知。

10.專業證照：每年至少維持二張資安專業證照。

11.承接具國家安全機密性或敏感性業務或技術研究之學校(或系所)，對承接之研究相關資訊系統，應依照各委託機關(如國家安全局或國防部等)之資安規定辦理。

(二)B級機關(構)及學校具體作法如下：

1.資訊系統分類分級：

(1)參考行政院國家資通安全會報頒訂之資訊系統分類分級與鑑別機制參考手冊，對核心業務應用資訊系統就機密性、完整性、可用性及法律遵循性等影意構面，進行分類、鑑別及分級，建立相對應之防護基準：

①初期以新建或改版完成之資訊系統為主，採行適當之安全控制措施，後續再推動至各機關全部資訊系統，以確保資訊系統之安全防護水準。

②如已通過資訊安全管理驗證（例如：ISO/IEC 27001、CNS 27001教育機構資安認證等），準用已採行之風險評鑑方法，轉換為本機制之普、中、高三個安全等級。

(2)辦理專科學校及十二年國教入學考試、甄選、招生等工作之試務機構與學校，亦應對承接之試務作業相關資訊系統進行分類、鑑別及分級。

2.ISMS 推動作業：

(1)導入資訊安全管理制度(ISMS)，對機關核心業務之應用資訊系統(至少二項)進行資安風險評鑑、管控等作業，並通過第三方驗證或教育機構資安認證。

(2)辦理專科學校及十二年國教入學考試、甄選、招生等工作之試務機構與學校，亦應導入資訊安全管理制度，將試務相關資訊系統，納入核心業務應用資訊系統，進行資安風險評鑑、管控等作業，並通過第三方驗證或教育機構資安認證。

3.資安專責人力：

(1)應指派一員具資安專業能力人員，專責執行資訊安全管理相關業務。

(2)辦理專科學校及十二年國教入學考試、甄選、招生等工作之試務機構與學校，應指派人員，對試務相關資訊系統進行資訊安全管理作業。

4.稽核方式：

(1)每年至少辦理一次內部資訊安全稽核作業。

(2)辦理專科學校及十二年國教入學考試、甄選、招生等工作之試務機構與學校，應於辦理試務前，對試務相關資訊系統及作業進行內部資訊安全稽核作業。

5. 業務持續運作演練：

(1)各項核心業務應用資訊系統依實務需要訂定業務持續運作計畫。

(2)每二年至少辦理一次核心業務應用資訊系統業務持續運作演練。

(3)辦理專科學校、十二年國教入學考試、甄選、招生等工作之試務機構與學校，對核心試務業務訂定業務持續作計畫，並於辦理試務前進行演練。

6. 縱深防護：對資訊網路環境建立縱深防禦架構，包括下列防禦裝置及系統：

(1)防毒、防火牆、郵件過濾裝置。

(2)IDS/IPS、Web 應用程式防火牆(針對對外服務之核心業務應用系統或網站)。

(3)辦理專科學校及十二年國教入學考試、甄選、招生等工作之試務機構與學校，應將試務相關資訊系統納入學校整體網路環境之資安縱深防護架構中。

7. 監控管理：結合臺灣學術網路資安監控系統(北區 SOC、南區 SOC、Mini-SOC、TACERT)或本部資安監控系統機制，進行資安預警情資、事件通報及應變處置。

8. 安全性檢測：

(1)每年至少辦理一次安全弱點檢測作業，視資源能力優先選擇核心業務資訊系統(網站)，並對弱點進行修復作業。

(2)每二年至少辦理一次滲透測試作業，視資源能力優先選擇核心業務資訊系統，並依測試結果強化網路及系統資安防禦能力。

(3)每二年對重要核心資訊網路、設備及系統，至少辦理一次資安健診作

業，實施網路架構檢視、有線網路惡意活動檢視、使用者端電腦檢視、伺服主機檢視及安全設定檢視等，並依檢測結果進行修復、調整作業。

(4)辦理專科學校及十二年國教入學考試、甄選、招生等工作之試務機構與學校，應於辦理試務作業前對資訊網路環境、設備及資訊系統實施資安健診及網站安全弱點檢測作業，並依檢測結果進行修復、調整作業。

9.資安教育訓練：

(1)資安或資訊人員應至少一員接受十二小時資安專業課程訓練(包括行政院、教育部、各級教學機構、各區網中心及各直轄市及縣(市)教育網路中心等辦理之資安課程、訓練、講習等)，並獲得研習證明，以增進資安專業知識與能力。

(2)一般使用者及主管應至少接受三小時資安宣導課程(包括機關自辦資安宣導講習、上級機關辦理之資安宣導課程)，並通過課程評量，以提升資安防護認知。

10.專業證照：每年至少維持一張資安專業證照。

(三)C 級學校具體作法如下：

1. 資訊系統分類分級：

(1)第一類 C 級學校：應參考行政院國家資通安全會報頒訂之資訊系統分類分級與鑑別機制參考手冊，就機密性、完整性、可用性及法律遵循性等影意構面，進行分類、鑑別及分級，視資源能力，建立相對應之防護基準：

①初期以新建或改版完成之資訊系統為主，採行適當之安全控制措施，後續再推動至其他資訊系統，以確保資訊系統之安全防護水準。

②如已通過資訊安全管理驗證（例如：ISO/IEC 27001、CNS 27001 教育機構資安認證等）之機關，準用已採行之風險評鑑方法，轉換為本機制之普、中、高三個安全等級。

(2)第二類 C 級學校：核心業務如有建置資訊系統，可參考行政院國家資通安全會報頒訂之資訊系統分類分級與鑑別機制參考手冊，視資源能力，建置必要之防護基準。

2.ISMS 推動作業：對核心業務之應用資訊系統進行資訊資產清查，檢視可能之風險，並視資源能力實施適當之管控作為。

3.資安專責人力：應指派一員兼任人員，執行資訊安全管理相關業務。

4.稽核方式：結合機關內部管理機制，每年辦理一次資訊安全自我檢查作業。

5.業務持續運作演練：對核心業務應用資訊系統依實務需要訂定業務持續運作計畫，並每年至少一次定期檢視計畫適用性。

6.縱深防護：

(1)第一類 C 級學校：對資訊網路環境建立縱深防禦架構，包括下列防禦裝置及系統：

①防毒、防火牆裝置。

②如有設置郵件伺服器則須建置郵件過濾裝置。

(2)第二類 C 級學校：由各直轄市及縣(市)教育網路中心於網路收容節點，設置防毒及防火牆設備，集中實施資安防護。

7.監控管理：結合臺灣學術網路資安監控系統(北區 SOC、南區 SOC、Mini-SOC、TACERT)或本部資安監控系統機制，進行資安預警情資、事件通報及應變處置。

8.安全性檢測：核心業務如有運用資訊系統(或網站)，於系統建置或更新時，或每年至少辦理一次資安弱點檢測作業，並對弱點進行修復作業。

9.資安教育訓練：

(1)擔任資安業務人員應接受六小時資安專業課程訓練(包括行政院、教育部、各級教學機構、各區網中心及各直轄市及縣(市)教育網路中心等辦理之資安課程、訓練、講習等)，並獲得研習證明，以增進資

安專業知識與能力。

(2)一般使用者及主管至少應接受三小時資安宣導課程(包括機關自辦資安宣導講習、上級機關辦理之資安宣導課程)，以提升資安防護認知。

10.專業證照：擔任資安業務人員每年至少參加一項資安專業訓練，並取得上課證明。

六、相關配套作法：

(一)資訊安全教育訓練：

1.本部得補助有資安專業師資之大學，分地區對單位或學校辦理資安訓練。

2.由各區域網路中心、各直轄市及縣(市)教育網路中心對所屬學校辦理資安訓練。

3.如為資安專業認證訓練(例如：資安主導稽核員認證訓練)得委請民間資安專業訓練機構辦理。

(二)教育機構資安認證作業：

1.本部得補助具資安專業能力之大學成立教育機構資安驗證中心辦理下列作業：

(1)依照國際資訊安全管理制度標準，研訂教育機構適用之資訊安全管理規範，作為認證標準。

(2)納編具資訊安全稽核認證訓練及實際稽核經驗之稽核員，對申請認證之學校實施資安稽核作業。

2.各機構及學校得向教育機構資安驗證中心申請資安稽核認證。

(三)安全性檢測作業：

1.本部得要求具資安技術檢測能力之大學編成服務團隊，對學校提供網站檢測、資安健診與滲透測試等服務。

2.各單位得向共同供應契約資安服務廠商購置套裝資安檢測服務。

七、資訊安全管理作業相關說明：

(一)名詞：

1.ISMS：Information Security Management System，資訊安全管理制度。

2.IDS：Intrusion Detection System，入侵偵測系統。

3.IPS：Intrusion Prevention System，入侵防禦系統。

4.SOC：Security Operation Center，資安監控中心。

5.APT：Advanced Persistent Threat，進階持續性威脅。

(二)核心業務資訊系統：指經資訊系統分級後，等級為「高」者，另政府機關於通過 ISMS 第三方驗證後，仍應依循標準要求辦理相關作業。

(三)資安教育訓練之對象：

1.一般主管：指擔任主管職務相關人員，如機關首長、副首長、部門主管(包括資訊主管)等。

2.資訊人員：指負責資訊作業相關人員，如系統分析設計人員、系統設計人員、系統管理人員及系統操作人員等。

3.資安人員：指負責資安業務相關人員，如資安管理人員、資安稽核人員等。

4.一般使用者：指一般業務、行政、會計、總務等單位內資訊系統之使用者。

(四)國際資安專業證照：指由國外獨立認驗證機構所核發之資安專業證照（非針對特定廠牌產品之證照），例如資安管理類之 ISO27001 主導稽核員（Lead Auditor, LA）、資安經理人（Certified Information Security Manager, CISM）、系統安全從業人員（Systems Security Certified Practitioner, SSCP）、資安管理師（Certification for Information System Security Professional, CISSP）等，及資安技術類之道德駭客（Certified Ethical Hacker, CEH）、全方位資安專家（Global Information Assurance Certification, GIAC）等。

(五)資安專業訓練證書：指資訊人員、資安人員需根據機關業務所需，參加資訊安全通識、資訊系統風險管理、資安事故處理、電子資料保護、個人資料保護管理及教育體系資安管理訓練等。

(六)資安健診檢測項目：

項目		內容
一、網路架構檢視		針對機關網路架構圖進行安全性弱點檢視，檢視之項目包含設計邏輯是否合宜、主機網路位置是否適當及現有防護程度是否足夠。
二、有線網路惡意活動檢視	(一)封包監聽與分析	在本機關有線網路(內網、外網、DMZ 區或 N 個網段)適當位置架設側錄設備，觀察是否有異常連線或 DNS 查詢，並比對是否連線已知惡意 IP、中繼站或有符合惡意網路行

		為的特徵。
	(二)網路設備紀錄檔分析	檢視防火牆、入侵偵測/防護系統等網路設備紀錄檔，分析過濾異常連線紀錄。
三、使用者端電腦檢視	(一)使用者端電腦惡意程式或檔案檢視	針對個人電腦進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。
	(二)使用者電腦更新檢視	針對個人電腦進行作業系統、Office 應用程式、防毒軟體、Adobe Acrobat 及 Adobe flash player 應用程式更新檢視。
四、伺服器主機檢視	(一)伺服器主機惡意程式或檔案檢視	針對伺服器主機進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。
	(二)伺服器主機更新檢視	針對伺服器主機進行作業系統、Office 應用程式、防毒軟體、 Adobe Acrobat 及 Adobe flash player 應用程式更新檢視。
五、安全設定檢視	(一)目錄伺服器(如 MS AD)中群組的密碼設定與帳號鎖定原則	檢視目錄伺服器中群組的密碼設定與帳號鎖定原則，例如 AD 伺服器有關 Group Policy 中之「密碼設定原則」與「帳號鎖定原則」設定若無 AD 伺服器，可以其他目錄伺服器(如 LDAP)完成「密碼設定原則」與「帳號鎖定原則」安全設定檢視。
	(二)防火牆連線設定	檢視防火牆是否開啟具有安全性風險的通訊埠或非必要通訊埠，連線設定是否有安全性弱點。

附表一：常設之入學試務機構

等　　級	機　　構　　全　　銜
A 級	財團法人大學入學考試中心基金會
A 級	大學甄選入學委員會(國立中正大學)
A 級	大學考試入學分發委員會(國立成功大學)
A 級	身心障礙學生升學大專校院甄試委員會(中央大學)
A 級	技專院校招生委員會聯合會(國立臺北科技大學)
A 級	財團法人技專校院入學測驗中心基金會(國立雲林科技大學)
A 級	國立台灣師範大學心理與教育測驗研究發展中心
A 級	四年制及專科學校二年制聯合甄選委員會(臺北科技大學)
A 級	四年制及專科學校二年制聯合登記分發委員會(臺北科技大學)

附表二：輪流辦理之入學試務機構及學校

等　　級	機　　構　　全　　銜
B 級	全國適性入學委員會
B 級	全國高中高職免試入學委員會
B 級	全國高中高職特色招生試務委員會
B 級	全國高中高職特色招生聯合分發委員會
B 級	全國五專聯合免試入學招生委員會
B 級	五專聯合特色招生考試分發入學招生委員會
B 級	國中教育會考各考區主辦學校
B 級	高中職免試入學各考區主辦學校
B 級	高中高職特色各區主辦學校
B 級	北區五專聯合免試入學招生委員會
B 級	中區五專聯合免試入學招生委員會
B 級	南區五專聯合免試入學招生委員會
B 級	分區四技進修部及二專夜間部聯合登記分發委員會