政府機關（構）資訊安全責任等級分級作業施行計畫

壹、 依據：

依據「國家資通訊安全發展方案（98 年至 101 年）」第 6、7 項行動方案「推動資安治理」及「推動資訊與資訊系統分類分級」辦理。

貳、 目的：

「國家資通安全會報」（以下簡稱本會報）為明確規範政府機關（構）資訊安全責任等級分級作業流程，特訂定「政府機關（構）資訊安全責任等級分級作業施行計畫」，透過資訊安全管理，以防範潛在資安威脅，進而提升國家資通安全防護水準。

參、施行對象：

（一）中央各政府機關（構）（含五院所屬機關（構））。

（二）行政院國家資通安全會報核定納管資通安全重要資訊系統。

（三）各主責機關業管機構涉及民眾權益之重要資訊系統。

肆、具體作法：

一、 各政府機關（構）資通安全作業權責：

各政府機關（構）之資通安全作業權責之相關事項，請參考行政院 93 年 10 月 21 日院台科字第 0930090197 號函送「各政府機關（構）落實資安事件危機處理具體執行方案」；各政府機關（構）首長應負該管單位全盤資安成敗之責，以期落實執行成效。

二、 資安等級區分方式：

(一) 政府機關

1. A 級（重要核心）：

(1) 處理具國家安全機密性或敏感性之數位資料之中央一、二級公務機關（如總統府、行政院、考試院、審計部等）。

(2) 凡涉及國家安全之外交、情報、國境安全、財稅、經濟、金融、醫療及重要民生基礎設施等重要機敏系統。

2. B 級（核心）：

(1) 各政府機關（構）具有影響社會秩序、民眾隱私之機敏資料或維運機關（如部分之中央一、二級機關、各部會之署局單位、各縣市政府、警察局、地方稅捐單位）。

(2) 全國或地方凡涉及社會秩序民生體系運作及民眾隱私等機敏系統。

3. C 級（重要）：

(1) 部分中央一、二級機關（如蒙藏委員會、消保會、體委會等）。

(2) 涉及地方縣市社會秩序、人民財產安全之重要資訊維運單位。

(3) 各部會之地方性作業單位（如各地區行政執行處）。

(4) 氣象作業中心、管理處（如氣象預報中心、地震、海象測報中心）。

(5) 各縣市議會、衛生局、文化局等。

4. D 級（一般）：

(1) 地方鄉、鎮、區公所、代表會、衛生服務中心、鄉村里民代表會等。

(2) 地區性氣象站（如台北、新竹、台中、高雄、宜蘭、花蓮及台東氣象站）。

(二) 學研機關（構）：

1. A 級（重要核心）：

(1) 負責教育政策審定單位（如教育部等）。

(2) 凡涉及各相關部會委託研究具國家安全機密性或敏感性之數位資料之執行單位。

(3) 教學醫院。

2. B 級（核心）：

(1) 凡涉及社會秩序運作及民眾隱私等機敏系統之學研機構。

(2) 各大學（含科技大學）。

(3) 台灣學術網路各區域網路中心暨各縣市教育網路中心。

3. C 級（重要）：

(1) 各技術學院及專科學校。

4. D 級（一般）：

(1) 各高中職（含）以下學校。

(三) 各事業分組：

1. A 級（重要核心）：

(1) 電力部份之核能發電廠、電力調度處、資訊系統處；自來水部份之省、市級自來水單位其資訊人員 40 人以上；石油部份之總公司、油品行銷事業部、天然氣事業部等其資訊人員 40 人以上。

(2) 通信部份之中華電信數據分公司；郵政部份之中華郵政公司其資訊人員 100 人以上。

(3) 財政部份之政策單位、總行其資訊人員 100 人以上。

(4) 金管部份之政策單位、總行其資訊人員 100 人以上。

(5) 醫院部份之醫學中心其資訊人員 30 人以上。

2. B 級（核心）：

(1) 電力部份之火力發電廠、資料處理中心、PC400 部及伺服器 30 部以上；自來水部份之管理處、營運所、水廠其資訊人員 20 人以上；石油部份之探勘事業部、煉油廠、天然氣；糖業部份之總公司資訊人員 30 人（含）以上；綜合部份之資訊人員 20 人（含）以上。

(2) 通信部份之中華電信公司分公司、所其資訊人員 10 人（含）以上；鐵路管理局；船舶部份之各港務局、工程處；郵政部份之中華郵政各地郵局、投遞中心。

(3) 財政部份之事業機構其資訊人員 50 人（含）以上。

(4) 金管部份之事業機構其資訊人員 50 人（含）以上。

(5) 醫院部份之區域醫院其資訊人員 5 人（含）以上。

3. C 級（重要）：

(1) 電力部份之火、水力發電廠、區營業處、總處、工程單位、PC100 部及伺服器 5 部以上；自來水部份之管理處、營運所、

水廠資訊人員 10 人以上；石油部份之事業部、儲運處、營業處、管理處；糖業部份之各糖廠資訊人員 10 人（含）以上；綜合部份之委員會、公司、局、廠處及中船公司。

(2) 通信部份之中華電信各營運處、研究所-分所。

(3) 財政部份之事業機構其資訊人員 20 人（含）以上。

(4) 金管部份之政策單位、總行其資訊人員 20 人（含）以上。

(5) 醫院部份之各地區醫院。

4. D 級（一般）：

(1) 電力部份之火水力發電廠、區營業處、總處、工程單位；自來水部份之管理處、營運所、水廠；石油部份之事業部、儲運處、營業處、管理處；糖業部份之營業處、所、訓練中心、服務處、工程處；綜合部份之分廠。

(2) 通信部份之中華電信各地區服務中心；鐵路局部份之各地收費站、機務段、票務中心。

(3) 財政部份之政策單位、總行其資訊人員 10 人（含）以上。

(4) 金管部份之政策單位、總行其資訊人員 10 人（含）以上。

(5) 醫院部份之其他醫院。

(四) 其他：在資訊資產價值分類內容之區分

1. A 級（重要核心）：違反資訊安全保護政策，會對國家安全之重要機敏資訊或系統等造成工作營運停頓或嚴重之損害，影響業務推動持續一個月（含）以上之損害，有極高度潛在影響等級。

2. B 級（核心）：違反資訊安全保護政策，會對社會秩序、民生體系運作及民眾隱私之機敏資訊或系統，影響業務推動持續一星期（含）以上之損害，有高度潛在影響等級。

3. C 級（重要）：違反資訊安全保護政策，會對地方縣市級之社會秩序、人民生命財產之重要資訊或系統，影響業務推動持續一天（含）以上之損害，有中度潛在影響等級。

4. D 級（一般）：違反資訊安全保護政策，造成意外的事件不影響業務工作或營運，為低度潛在影響等級。

三、 各單位所屬資安等級由主責機關（本會報各分組）、中央部會及各縣市政府等單位核定後，報本會報備查。

四、 除遵行政院及所屬各機關資訊安全管理規範外，各機關（構）依其資安等級應執行之工作事項如下：

作業名稱 / 等級	防護縱深	ISMS 推動作業(註一)	稽核方式	資安教育訓練(一般主管、資訊人員、資安人員、一般使用者(註二))	專業證照(註四)	檢測機關網站安全弱點
A 級	NSOC 直接防護/SOC 自建或委外、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少 2 次內稽	1. 每年至少(3、6、18、3 小時) 2. 資訊人員、資安人員需通過資安職能鑑定(註三)	維持至少 2 張資安專業證照	每年 2 次
B 級	SOC(選項)、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少 1 次內稽	1. 每年至少(3、6、16、3 小時) 2. 資訊人員、資安人員需通過資安職能鑑定(註三)	維持至少 1 張資安專業證照	每年 1 次
C 級	防火牆、防毒、郵件過濾裝置	自行成立推動小組規劃作業	自我檢視	每年至少(2、6、12、3 小時)	資安專業訓練	每年 1 次
D 級	防火牆、防毒、郵件過濾裝置	推動 ISMS 觀念宣導	自我檢視	每年至少(1、4、8、2 小時)	資安專業訓練	每年 1 次

註一：驗證範圍應涵蓋機關（構）之核心業務資訊系統，並逐步擴大至全單位。

註二：1、一般主管：擔任主管職務相關人員，如機關(副)首長、部門主管(含資訊主管)等。

2、資訊人員：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：負責資通安全業務相關人員，如資安管理人員、資安稽核人員等。

4、一般使用者：一般業務、行政、會計、總務人員等單位內資訊系統的使用者。

註三：資安職能鑑定科目包括：資通安全管理制度、資訊系統風險評鑑、資通安全稽核、政府資訊作業委外安全、資安事件應變作業、電子資料保護、電子郵件安全及 WEB 應用程式安全等，A、B 級機關(構)之資訊人員、資安人員需參加行政院研考會規劃辦理之資安訓練並通過鑑定。

註四：由國內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）、資訊安全經理人（Certified Information Security Manager, CISM）、系統安全從業人員（Systems Security Certified Practitioner, SSCP）、資訊安全管理師（Certification for Information System Security Professional, CISSP）等及資安技術類之道德駭客（Certified Ethical Hacker, CEH）、全方位資訊安全專家（Global Information Assurance Certification, GIAC）等。

五、 各類資安系統等級應執行工作事項之推動時程如下：

(一) 100 年前完成郵件過濾裝置。

(二) A 級機關（構）於 98 年前通過 ISMS 第三者驗證，B 級機關（構）於 100 年前通過 ISMS 第三者驗證。

(三) 其餘工作事項自即日起實施。