# 「政府機關（構）資通安全責任等級分級作業規定」

壹、目的

為明確規範政府機關（構）資通安全責任等級分級作業流程，透過資通安全（以下簡稱資安）管理，以防範潛在資安威脅，進而提升國家資安防護水準，特訂定「政府機關（構）資通安全責任等級分級作業規定」（以下簡稱本規定）。

貳、適用對象

一、中央及地方政府機關（含行政法人）。

二、國（公）營事業、醫療及學術機構。

三、由政府委託民間興建營運後轉移（Build-Operate-Transfer, BOT）之關鍵資訊基礎設施(Critical Information Infrastructure，CII)之營運單位。關鍵資訊基礎設施，指涉及核心業務運作，為支持關鍵基礎設施持續營運所需之重要資訊系統或調度、控制系統(Supervisory Control and Data Acquisition, SCADA)，亦屬關鍵基礎設施之重要元件，應配合對應之關鍵基礎設施統一納管。

參、分級原則

一、政府機關層級。

二、涉及外交、國防、國土安全、財政、經濟、警政等重要業務。

三、涉及能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、高科技園區等關鍵資訊基礎設施業務或營運。

四、涉及全國、區域性或地區性個人資料檔案。

肆、具體作法

一、政府機關（構）資安責任等級

(一) 政府機關

1. A 級

(1) 總統府、國安會、立法院、司法院、考試院、監察院、行政院及直轄市政府。

(2) 立法院、司法院、考試院、監察院及行政院等所屬二級機關、相當二級機關之獨立機關（以下合稱二級機關）。但其業務或組織單純者，得報經其上級機關核准，調整為 B 級或 C 級。

(3) 凡涉及外交、國防、國土安全，及掌理全國財政、經濟、警政等重要業務之機關，如外交部領事事務局、內政部警政署刑事警察局等。

(4) 負責能源、水資源、通訊傳播、交通、金融、緊急救援、高科技園區等關鍵資訊基礎設施之營運機關，如交通部民用航空局飛航服務總臺等。

(5) 保有全國性個人資料檔案之機關，如勞動部勞工保險局、衛生福利部中央健康保險署等。

2. B 級

(1) 縣（市）政府。

(2) 凡涉及社會秩序及人民財產業務之機關，如地方政府警察局、地方政府地政事務所等。

(3) 保有區域性或地區性個人資料檔案之機關，如財政部各地區國稅局、地方政府戶政事務所等。

3. C 級

其他政府機關及地方政府民意機關。

(二) 學術機構

1. A 級

凡涉及各相關機關委託研究具國家安全機密性或敏感性之學校。

2. B 級

(1) 各大學。

(2) 臺灣學術網路各區域網路中心暨各直轄市、縣（市）教育網路中心。

3. C 級

(1) 各學院、專科學校及高級中等以下學校。

(2)教育部所屬研究機構。

(三) 國（公）營事業、醫療機構及其他

1. A 級

(1)國（公）營事業與特許機構，處理涉及能源、水資源、通訊傳播、交通、金融等關鍵資訊基礎設施業務者，如台灣電力公司、臺灣港務股份有限公司、臺灣證券交易所等。

(2)由政府委託民間興建營運後轉移之關鍵資訊基礎設施之營運單位，如遠通電收股份有限公司、台灣高速鐵路股份有限公司、高雄捷運股份有限公司等。

(3)醫學中心，如國立臺灣大學醫學院附設醫院、臺北榮民總醫院等。

(4)保有全國性個人資料檔案之機構，如中華郵政股份有限公司等。

2. B 級

(1)國（公）營事業涉及全國或地方民生資源等業務，如台灣糖業股份有限公司等。

(2)區域醫院，如臺北市立聯合醫院、衛生福利部桃園醫院、國立臺灣大學醫學院附設醫院雲林分院等。

(3)保有區域性或地區性個人資料檔案之機構。

3. C 級

(1)其他國（公）營事業機構，如金門酒廠實業股份有限公司、福建省連江縣馬祖日報社等。

(2)地區醫院，如臺北市立關渡醫院、國立成功大學醫學院附設醫院斗六分院、臺北榮民總醫院新竹分院等。

二、政府機關（構）符合前點所述一個以上之等級者，適用最高等級。

三、行政院所屬二級機關、各直轄市及縣（市）政府，應檢視其所屬機關（構）（含行政法人）資安責任等級之分級及其妥適性，並彙送行政院資通安全辦公室，經該辦公室複核後，提請行政院國家資通安全會報核定資安責任等級，其修正亦同。

四、總統府、國安會、立法院、司法院、考試院、監察院所屬機關（構）之資安責任等級，比照前點規定辦理，並提送行政院國家資通安全會報備查。

五、原為國（公）營已民營化之事業、公辦民營事業、民營公用事業及政府捐助之財團法人，得由其主管（監督）機關參照本規定，自行訂定資安責任等級，並依其訂定之應辦事項監督管理。

六、政府機關（構）除遵循行政院及所屬各機關資安管理規範外，依其資安等級，應辦理之工作事項如附表。

附表

| 作業名稱 / 等級 | 資訊系統分類分級 | ISMS 推動作業 | 資安專責人力 | 稽核方式 | 業務持續運作演練 | 防護縱深 | 監控管理 | 安全性檢測 | 資安教育訓練(一般主管、資訊人員/資安人員、一般使用者 | 專業證照 |
|---|---|---|---|---|---|---|---|---|---|---|
| A 級 | 1.完成資訊系統分級(104 年底前)<br>2.完成資訊系統資安防護基準要求(105 年底前) | 1.全部核心資訊系統完成 ISMS 導入(105 年底前)<br>2.全部核心資訊系統通過第三方驗證(106 年底前) | 指派資安專責人力 2 人 | 每年至少 2 次內稽 | 每年至少辦理 1 次核心資訊系統持續運作演練 | 1.防毒、防火牆、郵件過濾裝置<br>2.IDS/IPS、Web 應用程式防火牆<br>3.APT 攻擊防禦 | SOC 監控(104 年底前) | 1.每年至少辦理 2 次網站安全弱點檢測<br>2.每年至少辦理 1 次系統滲透測試<br>3.每年至少辦理 1 次資安健診 | 1.每年資安人員(資訊人員)至少 2 人次須接受 12 小時以上資安專業課程訓練或資安職能訓練<br>2.每年一般使用者與主管至少須接受 3 小時資安宣導課程並通過課程評量 | 每年維持至少 2 張國際資安專業證照與 2 張資安職能訓練證書之有效性 |
| B 級 | 1.完成資訊系統分級(104 年底前)<br>2.完成資訊系統資安防護基準要求(105 年底前) | 1.至少 2 項核心資訊系統完成 ISMS 導入(106 年底前)<br>2.至少 2 項核心資訊系統通過第三方驗 | 指派資安專責人力 1 人 | 每年至少 1 次內稽 | 每 2 年至少辦理 1 次核心資訊系統持續運作演練 | 1.防毒、防火牆、郵件過濾裝置<br>2. IDS/IPS<br>3. Web 應用程式防火牆(機關具有對外服務之核心資訊系統) | SOC 監控(105 年底前) | 1.每年至少辦理 1 次網站安全弱點檢測<br>2.每 2 年至少辦理 1 次系統滲透測試<br>3.每 2 年至少辦理 1 次 | 1.每年資安人員(資訊人員)至少 1 人次須接受 12 小時以上資安專業課程訓練或資安職能訓練<br>2.每年一般使用者與主管至少須接受 3 小時 | 每年維持至少 1 張國際資安專業證照與 1 張資安職能訓練證書之有效性 |

附表

| 作業名稱 / 等級 | 資訊系統分類分級 | ISMS 推動作業 | 資安專責人力 | 稽核方式 | 業務持續運作演練 | 防護縱深 | 監控管理 | 安全性檢測 | 資安教育訓練(一般主管、資訊人員/資安人員、一般使用者 | 專業證照 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 證(107 年底前) | | | | | | 資安健診 | 資安宣導課程並通過課程評量 | |
| C 級 | 依各主管機關規定 | 自行成立推動小組規劃作業 | 依各主管機關規定 | 依各主管機關規定 | 依各主管機關規定 | 1.防毒<br>2.防火牆<br>3.郵件過濾裝置(機關具有郵件伺服器) | 依各主管機關規定 | 依各主管機關規定 | 1.依各主管機關規定資安人員(資訊人員)資安專業課程訓練或資安職能訓練要求<br>2.每年一般使用者與主管至少須接受 3 小時資安宣導課程並通過課程評量 | 依各主管機關規定 |

註1. 名詞說明：

（一）ISMS：Information Security Management System，資訊安全管理制度。

（二）IDS：Intrusion Detection System，入侵偵測系統。

（三）IPS：Intrusion Prevention System，入侵防禦系統。

（四）SOC：Security Operation Center，資安監控中心。

（五）APT：Advanced Persistent Threat，進階持續性威脅。

註2. 核心資訊系統：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。

註3. 資安教育訓練之對象說明：

（一）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(含資訊主管)等。

（二）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。

（三）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。

（四）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。

註4. 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。

註5. 資安職能訓練證書：指資訊人員、資安人員需根據機關業務所需，參加資安職能訓練並通過評量取得證書。資安職能訓練科目包括：資訊安全通識、資訊系統風險管理、政府資訊作業委外安全、資安事故處理、電子資料保護、電子郵件安全、WEB 應用程式安全、個人資料保護管理及政府資安管理評鑑等。