# 資通安全管理法及子法彙編

行政院 中華民國 110 年 9 月

## 目次

壹	•	法	規(	条.	文	••••	••••	••••	••••	•••••	••••	•••••	•••••	•••••	••••	••••	•••••	•••••	1
	_	、資	通	安全	全管	管理	法.	•••••	••••	•••••									1
	二	、資	通	安全	全管	管理	法加	色行	細見	钊									9
	Ξ	、資	通	安全	全責	責任	等系	及分	級美	辦法	<del>.</del>					• • • • •			. 15
	四	、資	通	安全	全事	事件	通幸	设及	應	變辨	法.								. 45
	五	、特	定,	1年2	公系	务機	關	資通	安?	全維	護	計畫	實力	拖情	形和	管核	辨法	<u> </u>	55
	六	、資	通	安全	全情	青資	分子	享辦	法	•••••									.58
	セ	、公	務村	幾層	絹角	斤屬	人	員資	通-	安全	事:	項獎	懲弟	辨法					.61
											•	,,,,							
貮	•	逐	條言	涗!	明	••••	•••••								••••	•••••	•••••	•••••	. 64
貳								••••	••••	•••••	•••••	•••••	•••••	•••••				•••••	
貳	_	、資	通	安全	全管	管理	法.	•••••	••••	•••••	•••••	•••••	•••••		••••	•••••			64
貳	<b>–</b>	、 資、 資	通道	安全	全管 全管	<b>管理</b>	法. 法 <sup>办</sup>	<b></b> 色行	細見	利									64 77
貳	1 1 11	資資資	通通通	安安安	全 全 全 全 章	管理 管理	法法等	<b></b>	細見級発	訓		•••••							64 77 87
貳	一二三四	資資資資	通通通通	安安安安	全 全 全 幸	管理 任 件	法 等 通	·····	細級	則 變辨	·····································								64 77 87 147
貳	一二三四五	資 資 資 等	通通通通 定	安安安安非	全 全 全 全 公	穿 章 章 等 群	法 法 等 通 關	施 及 跟 資	細級應安		**: 養:	計畫	**************************************	施情		稽相	·····································		64 77 87 147

## 壹、 法規條文

## 一、資通安全管理法

總統令 中華民國 107 年 6 月 6 日 華總一義字第 10700060021 號

兹制定資通安全管理法,公布之。

總 統 蔡英文 行政院院長 賴清德

資通安全管理法

中華民國 107 年 6 月 6 日 公布

#### 第一章 總則

第一條 為積極推動國家資通安全政策,加速建構國家 資通安全環境,以保障國家安全,維護社會公共利 益,特制定本法。

第二條 本法之主管機關為行政院。

第三條 本法用詞,定義如下:

- 一、資通系統:指用以蒐集、控制、傳輸、儲存、 流通、刪除資訊或對資訊為其他處理、使用 或分享之系統。
- 二、資通服務:指與資訊之蒐集、控制、傳輸、 儲存、流通、刪除、其他處理、使用或分享 相關之服務。
- 三、資通安全:指防止資通系統或資訊遭受未 經授權之存取、使用、控制、洩漏、破壞、 竄改、銷毀或其他侵害,以確保其機密性、 完整性及可用性。

四、 資通安全事件:指系統、服務或網路狀態經

鑑別而顯示可能有違反資通安全政策或保 護措施失效之狀態發生,影響資通系統機 能運作,構成資通安全政策之威脅。

- 五、公務機關:指依法行使公權力之中央、地方機關(構)或公法人。但不包括軍事機關及情報機關。
- 六、特定非公務機關:指關鍵基礎設施提供者、 公營事業及政府捐助之財團法人。
- 七、關鍵基礎設施:指實體或虛擬資產、系統或 網路,其功能一旦停止運作或效能降低,對 國家安全、社會公共利益、國民生活或經濟 活動有重大影響之虞,經主管機關定期檢 視並公告之領域。
- 八、關鍵基礎設施提供者:指維運或提供關鍵 基礎設施之全部或一部,經中央目的事業 主管機關指定,並報主管機關核定者。
- 九、政府捐助之財團法人:指其營運及資金運 用計畫應依預算法第四十一條第三項規定 送立法院,及其年度預算書應依同條第四 項規定送立法院審議之財團法人。

第四條 為提升資通安全,政府應提供資源,整合民間 及產業力量,提升全民資通安全意識,並推動下列 事項:

- 一、資通安全專業人才之培育。
- 二、資通安全科技之研發、整合、應用、產學 合作及國際交流合作。
- 三、資通安全產業之發展。
- 四、資通安全軟硬體技術規範、相關服務與審

驗機制之發展。

前項相關事項之推動,由主管機關以國家資通 安全發展方案定之。

第五條 主管機關應規劃並推動國家資通安全政策、資 通安全科技發展、國際交流合作及資通安全整體防 護等相關事宜,並應定期公布國家資通安全情勢報 告、對公務機關資通安全維護計畫實施情形稽核概 況報告及資通安全發展方案。

> 前項情勢報告、實施情形稽核概況報告及資通 安全發展方案,應送立法院備查。

第六條 主管機關得委任或委託其他公務機關、法人或 團體,辨理資通安全整體防護、國際交流合作及其 他資通安全相關事務。

> 前項被委託之公務機關、法人或團體或被複委託者,不得洩露在執行或辦理相關事務過程中所獲 悉關鍵基礎設施提供者之秘密。

第七條 主管機關應衡酌公務機關及特定非公務機關業 務之重要性與機敏性、機關層級、保有或處理之資 訊種類、數量、性質、資通系統之規模及性質等條 件,訂定資通安全責任等級之分級;其分級基準、 等級變更申請、義務內容、專責人員之設置及其他 相關事項之辦法,由主管機關定之。

> 主管機關得稽核特定非公務機關之資通安全維 護計畫實施情形;其稽核之頻率、內容與方法及其 他相關事項之辦法,由主管機關定之。

> 特定非公務機關受前項之稽核,經發現其資通 安全維護計畫實施有缺失或待改善者,應向主管機 關提出改善報告,並送中央目的事業主管機關。

第八條 主管機關應建立資通安全情資分享機制。

前項資通安全情資之分析、整合與分享之內 容、程序、方法及其他相關事項之辦法,由主管機 關定之。

第九條 公務機關或特定非公務機關,於本法適用範圍內,委外辦理資通系統之建置、維運或資通服務之提供,應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求,選任適當之受託者,並監督其資通安全維護情形。

第二章 公務機關資通安全管理

- 第十條 公務機關應符合其所屬資通安全責任等級之要求,並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件,訂定、修正及實施資通安全維護計畫。
- 第十一條 公務機關應置資通安全長,由機關首長指派 副首長或適當人員兼任,負責推動及監督機關內 資通安全相關事務。
- 第十二條 公務機關應每年向上級或監督機關提出資通 安全維護計畫實施情形;無上級機關者,其資通 安全維護計畫實施情形應送交主管機關。
- 第十三條 公務機關應稽核其所屬或監督機關之資通安 全維護計畫實施情形。

受稽核機關之資通安全維護計畫實施有缺失 或待改善者,應提出改善報告,送交稽核機關及 上級或監督機關。

第十四條 公務機關為因應資通安全事件,應訂定通報 及應變機制。

公務機關知悉資通安全事件時,除應通報上

級或監督機關外,並應通報主管機關;無上級機關者,應通報主管機關。

公務機關應向上級或監督機關提出資通安全 事件調查、處理及改善報告,並送交主管機關; 無上級機關者,應送交主管機關。

前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法,由主管機關定之。

第十五條 公務機關所屬人員對於機關之資通安全維護 績效優良者,應予獎勵。

前項獎勵事項之辦法,由主管機關定之。

第三章特定非公務機關資通安全管理

第十六條 中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後,指定關鍵基礎設施提供者,報請主管機關核定,並以書面通

知受核定者。

關鍵基礎設施提供者應符合其所屬資通安全 責任等級之要求,並考量其所保有或處理之資訊 種類、數量、性質、資通系統之規模與性質等條 件,訂定、修正及實施資通安全維護計畫。

關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形。

中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。

關鍵基礎設施提供者之資通安全維護計畫實施有缺失或待改善者,應提出改善報告,送交中央目的事業主管機關。

第二項至第五項之資通安全維護計畫必要事

項、實施情形之提出、稽核之頻率、內容與方 法、改善報告之提出及其他應遵行事項之辦法, 由中央目的事業主管機關擬訂,報請主管機關核 定之。

第十七條

關鍵基礎設施提供者以外之特定非公務機關,應符合其所屬資通安全責任等級之要求,並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件,訂定、修正及實施資通安全維護計畫。

中央目的事業主管機關得要求所管前項特定 非公務機關,提出資通安全維護計畫實施情形。

中央目的事業主管機關得稽核所管第一項特 定非公務機關之資通安全維護計畫實施情形,發 現有缺失或待改善者,應限期要求受稽核之特定 非公務機關提出改善報告。

前三項之資通安全維護計畫必要事項、實施 情形之提出、稽核之頻率、內容與方法、改善報 告之提出及其他應遵行事項之辦法,由中央目的 事業主管機關擬訂,報請主管機關核定之。

第十八條

特定非公務機關為因應資通安全事件,應訂 定通報及應變機制。

特定非公務機關於知悉資通安全事件時,應向中央目的事業主管機關通報。

特定非公務機關應向中央目的事業主管機關 提出資通安全事件調查、處理及改善報告;如為 重大資通安全事件者,並應送交主管機關。

前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法,由主 管機關定之。 知悉重大資通安全事件時,主管機關或中央 目的事業主管機關於適當時機得公告與事件相關 之必要內容及因應措施,並得提供相關協助。

#### 第四章 罰則

第十九條 公務機關所屬人員未遵守本法規定者,應按 其情節輕重,依相關規定予以懲戒或懲處。

前項懲處事項之辦法,由主管機關定之。

第二十條 特定非公務機關有下列情形之一者,由中央 目的事業主管機關令限期改正;屆期未改正者, 按次處新臺幣十萬元以上一百萬元以下罰鍰:

- 一、未依第十六條第二項或第十七條第一項 規定,訂定、修正或實施資通安全維護 計畫,或違反第十六條第六項或第十七 條第四項所定辦法中有關資通安全維護 計畫必要事項之規定。
- 二、未依第十六條第三項或第十七條第二項 規定,向中央目的事業主管機關提出資 通安全維護計畫之實施情形,或違反第 十六條第六項或第十七條第四項所定辦 法中有關資通安全維護計畫實施情形提 出之規定。
- 三、未依第七條第三項、第十六條第五項或 第十七條第三項規定,提出改善報告送 交主管機關、中央目的事業主管機關, 或違反第十六條第六項或第十七條第四 項所定辦法中有關改善報告提出之規定。
- 四、未依第十八條第一項規定,訂定資通安 全事件之通報及應變機制,或違反第十 八條第四項所定辦法中有關通報及應變

機制必要事項之規定。

五、未依第十八條第三項規定,向中央目的 事業主管機關或主管機關提出資通安全 事件之調查、處理及改善報告,或違反 第十八條第四項所定辦法中有關報告提 出之規定。

六、違反第十八條第四項所定辦法中有關通 報內容之規定。

第二十一條 特定非公務機關未依第十八條第二項規 定,通報資通安全事件,由中央目的事業主管 機關處新臺幣三十萬元以上五百萬元以下罰 鍰,並令限期改正;屆期未改正者,按次處罰 之。

#### 第五章 附則

第二十二條 本法施行細則,由主管機關定之。 第二十三條 本法施行日期,由主管機關定之。

#### 二、資通安全管理法施行細則

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

- 第一條 本細則依資通安全管理法(以下簡稱本法)第二 十二條規定訂定之。
- 第二條 本法第三條第五款所稱軍事機關,指國防部及其 所屬機關(構)、部隊、學校;所稱情報機關,指國家 情報工作法第三條第一項第一款及第二項規定之機 關。
- 第三條 公務機關或特定非公務機關(以下簡稱各機關) 依本法第七條第三項、第十三條第二項、第十六條第 五項或第十七條第三項提出改善報告,應針對資通安 全維護計畫實施情形之稽核結果提出下列內容,並依 主管機關、上級或監督機關或中央目的事業主管機關 指定之方式及時間,提出改善報告之執行情形:
  - 一、缺失或待改善之項目及內容。
  - 二、發生原因。
  - 三、為改正缺失或補強待改善項目所採取管理、 技術、人力或資源等層面之措施。
  - 四、前款措施之預定完成時程及執行進度之追蹤 方式。
- 第四條 各機關依本法第九條規定委外辦理資通系統之 建置、維運或資通服務之提供(以下簡稱受託業務), 選任及監督受託者時,應注意下列事項:
  - 一、受託者辦理受託業務之相關程序及環境,應 具備完善之資通安全管理措施或通過第三 方驗證。

- 二、受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。
- 三、受託者辦理受託業務得否複委託、得複委託 之範圍與對象,及複委託之受託者應具備之 資通安全維護措施。
- 四、受託業務涉及國家機密者,執行受託業務之 相關人員應接受適任性查核,並依國家機密 保護法之規定,管制其出境。
- 五、受託業務包括客製化資通系統開發者,受託 者應提供該資通系統之安全性檢測證明;該 資通系統屬委託機關之核心資通系統,或委 託金額達新臺幣一千萬元以上者,委託機關 應自行或另行委託第三方進行安全性檢測; 涉及利用非受託者自行開發之系統或資源 者,並應標示非自行開發之內容與其來源及 提供授權證明。
- 六、受託者執行受託業務,違反資通安全相關法令或知悉資通安全事件時,應立即通知委託機關及採行之補救措施。
- 七、委託關係終止或解除時,應確認受託者返還、 移交、刪除或銷毀履行契約而持有之資料。
- 八、受託者應採取之其他資通安全相關維護措施。
- 九、委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時,以稽核或其 他適當方式確認受託業務之執行情形。

委託機關辦理前項第四款之適任性查核,應考量受託業務所涉及國家機密之機密等級及內容,就執行

該業務之受託者所屬人員及可能接觸該國家機密之 其他人員,於必要範圍內查核有無下列事項:

- 一、曾犯洩密罪,或於動員戡亂時期終止後,犯內亂罪、外患罪,經判刑確定,或通緝有案尚未結案。
- 二、曾任公務員,因違反相關安全保密規定受懲 戒或記過以上行政懲處。
- 三、曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫,從事不利國家安全或重大利益情事。

四、其他與國家機密保護相關之具體項目。

第一項第四款情形,應記載於招標公告、招標文件及契約;於辦理適任性查核前,並應經當事人書面 同意。

- 第五條 前條第三項及本法第十六條第一項之書面,依電子簽章法之規定,得以電子文件為之。
- 第六條 本法第十條、第十六條第二項及第十七條第一項 所定資通安全維護計畫,應包括下列事項:
  - 一、核心業務及其重要性。
  - 二、資通安全政策及目標。
  - 三、資通安全推動組織。
  - 四、專責人力及經費之配置。
  - 五、公務機關資通安全長之配置。
  - 六、資通系統及資訊之盤點,並標示核心資通系 統及相關資產。
  - 七、資通安全風險評估。
  - 八、資通安全防護及控制措施。
  - 九、資通安全事件通報、應變及演練相關機制。

- 十、資通安全情資之評估及因應機制。
- 十一、資通系統或服務委外辦理之管理措施。
- 十二、公務機關所屬人員辦理業務涉及資通安全 事項之考核機制。
- 十三、資通安全維護計畫與實施情形之持續精進 及績效管理機制。

各機關依本法第十二條、第十六條第三項或第十 七條第二項規定提出資通安全維護計畫實施情形,應 包括前項各款之執行成果及相關說明。

第一項資通安全維護計畫之訂定、修正、實施及 前項實施情形之提出,公務機關經其上級或監督機關 同意,得由其上級、監督機關或其上級、監督機關所 屬公務機關辦理;特定非公務機關經其中央目的事業 主管機關同意,得由其中央目的事業主管機關、中央 目的事業主管機關所屬公務機關或中央目的事業主 管機關所管特定非公務機關辦理。

第七條 前條第一項第一款所定核心業務,其範圍如下:

- 一、公務機關依其組織法規,足認該業務為機關 核心權責所在。
- 二、公營事業及政府捐助之財團法人之主要服務 或功能。
- 三、各機關維運、提供關鍵基礎設施所必要之業 務。
- 四、各機關依資通安全責任等級分級辦法第四條 第一款至第五款或第五條第一款至第五款 涉及之業務。

前條第一項第六款所稱核心資通系統,指支持核心業務持續運作必要之系統,或依資通安全責任等級

分級辦法附表九資通系統防護需求分級原則之規定, 判定其防護需求等級為高者。

- 第八條 本法第十四條第三項及第十八條第三項所定資 通安全事件調查、處理及改善報告,應包括下列事項:
  - 一、事件發生或知悉其發生、完成損害控制或復 原作業之時間。
  - 二、事件影響之範圍及損害評估。
  - 三、損害控制及復原作業之歷程。
  - 四、事件調查及處理作業之歷程。
  - 五、事件根因分析。
  - 六、為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

七、前款措施之預定完成時程及成效追蹤機制。

- 第九條 中央目的事業主管機關依本法第十六條第一項 規定指定關鍵基礎設施提供者前,應給予其陳述意見 之機會。
- 第十條 本法第十八條第三項及第五項所稱重大資通安 全事件,指資通安全事件通報及應變辦法第二條第四 項及第五項規定之第三級及第四級資通安全事件。
- 第十一條 主管機關或中央目的事業主管機關知悉重大 資通安全事件,依本法第十八條第五項規定公告與 事件相關之必要內容及因應措施時,應載明事件之 發生或知悉其發生之時間、原因、影響程度、控制 情形及後續改善措施。

前項與事件相關之必要內容及因應措施,有下 列情形之一者,不予公告:

一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊,或公開有侵害公務機關、

個人、法人或團體之權利或其他正當利益。 但法規另有規定,或對公益有必要,或為 保護人民生命、身體、健康有必要,或經 當事人同意者,不在此限。

二、其他依法規規定應秘密、限制或禁止公開 之情形。

第一項與事件相關之必要內容及因應措施含 有前項不予公告之情形者,得僅就其他部分公告之。 第十二條 特定非公務機關之業務涉及數中央目的事業 主管機關之權責者,主管機關得協調指定一個以上 之中央目的事業主管機關,單獨或共同辦理本法所 定中央目的事業主管機關應辦理之事項。

第十三條 本細則之施行日期,由主管機關定之。 本細則修正條文自發布日施行。

## 三、資通安全責任等級分級辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 108 年 8 月 26 日行政院院臺護字第 1080184606 號令修正 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

- 第一條 本辦法依資通安全管理法(以下簡稱本法)第七條第 一項規定訂定之。
- 第二條 公務機關及特定非公務機關(以下簡稱各機關)之資 通安全責任等級,由高至低,分為A級、B級、C級、D級及 E級。
- 第三條 主管機關應每二年核定自身資通安全責任等級。

行政院直屬機關應每二年提交自身、所屬或監督之公 務機關及所管之特定非公務機關之資通安全責任等級,報 主管機關核定。

直轄市、縣(市)政府應每二年提交自身、所屬或監督之公務機關,與所轄鄉(鎮、市)、直轄市山地原住民區公所及其所屬或監督之公務機關之資通安全責任等級,報主管機關核定。

直轄市及縣(市)議會、鄉(鎮、市)民代表會及直轄市山地原住民區民代表會應每二年提交自身資通安全責任等級,由其所在區域之直轄市、縣(市)政府彙送主管機關核定。

總統府、國家安全會議、立法院、司法院、考試院及監察院應每二年核定自身、所屬或監督之公務機關及所管之 特定非公務機關之資通安全責任等級,送主管機關備查。

各機關因組織或業務調整,致須變更原資通安全責任 等級時,應即依前五項規定程序辦理等級變更;有新設機 關時,亦同。 第一項至第五項公務機關辦理資通安全責任等級之提 交或核定,就公務機關或特定非公務機關內之單位,認有 另列與該機關不同等級之必要者,得考量其業務性質,依 第四條至第十條規定認定之。

第四條 各機關有下列情形之一者,其資通安全責任等級為A級:

- 一、業務涉及國家機密。
- 二、業務涉及外交、國防或國土安全事項。
- 三、業務涉及全國性民眾服務或跨公務機關共用性 資通系統之維運。
- 四、業務涉及全國性民眾或公務員個人資料檔案之 持有。
- 五、屬公務機關,且業務涉及全國性之關鍵基礎設施 事項。
- 六、屬關鍵基礎設施提供者,且業務經中央目的事業 主管機關考量其提供或維運關鍵基礎設施服務之 用戶數、市場占有率、區域、可替代性,認其資 通系統失效或受影響,對社會公共利益、民心士 氣或民眾生命、身體、財產安全將產生災難性或 非常嚴重之影響。

七、屬公立醫學中心。

第五條 各機關有下列情形之一者,其資通安全責任等級為B級:

- 一、業務涉及公務機關捐助、資助或研發之國家核心 科技資訊之安全維護及管理。
- 二、業務涉及區域性、地區性民眾服務或跨公務機關 共用性資通系統之維運。
- 三、業務涉及區域性或地區性民眾個人資料檔案之 持有。
- 四、 業務涉及中央二級機關及所屬各級機關(構)共

用性資通系統之維運。

- 五、屬公務機關,且業務涉及區域性或地區性之關鍵 基礎設施事項。
- 六、屬關鍵基礎設施提供者,且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性,認其資通系統失效或受影響,對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重影響。

七、屬公立區域醫院或地區醫院。

第六條 各機關維運自行或委外設置、開發之資通系統者,其 資通安全責任等級為 C 級。

> 前項所定自行或委外設置之資通系統,指具權限區分 及管理功能之資通系統。

- 第七條 各機關自行辦理資通業務,未維運自行或委外設置、 開發之資通系統者,其資通安全責任等級為 D 級。
- 第八條 各機關有下列情形之一者,其資通安全責任等級為E級:
  - 一、無資通系統且未提供資通服務。
  - 二、屬公務機關,且其全部資通業務由其上級機關、 監督機關或上開機關指定之公務機關兼辦或代管。
  - 三、屬特定非公務機關,且其全部資通業務由其中央 目的事業主管機關、中央目的事業主管機關所屬 公務機關、中央目的事業主管機關所管特定非公 務機關或出資之公務機關兼辦或代管。
- 第九條 各機關依第四條至前條規定,符合二個以上之資通安 全責任等級者,其資通安全責任等級列為其符合之最高等 級。
- 第十條 各機關之資通安全責任等級依前六條規定認定之。但 第三條第一項至第五項之公務機關提交或核定資通安全責

任等級時,得考量下列事項對國家安全、社會公共利益、人 民生命、身體、財產安全或公務機關聲譽之影響程度,調整 各機關之等級:

- 一、業務涉及外交、國防、國土安全、全國性、區域 性或地區性之能源、水資源、通訊傳播、交通、 銀行與金融、緊急救援與醫院業務者,其中斷或 受妨礙。
- 二、業務涉及個人資料、公務機密或其他依法規或契 約應秘密之資訊者,其資料、公務機密或其他資 訊之數量與性質,及遭受未經授權之存取、使用、 控制、洩漏、破壞、竄改、銷毀或其他侵害。
- 三、各機關依層級之不同,其功能受影響、失效或中斷。
- 四、其他與資通系統之提供、維運、規模或性質相關 之具體事項。
- 第十一條 各機關應依其資通安全責任等級,辦理附表一至附表 八之事項。

各機關自行或委外開發之資通系統應依附表九所定 資通系統防護需求分級原則完成資通系統分級,並依附表 十所定資通系統防護基準執行控制措施;特定非公務機關 之中央目的事業主管機關就特定類型資通系統之防護基 準認有另為規定之必要者,得自行擬訂防護基準,報請主 管機關核定後,依其規定辦理。

各機關辦理附表一至附表八所定事項或執行附表十 所定控制措施,因技術限制、個別資通系統之設計、結構 或性質等因素,就特定事項或控制措施之辦理或執行顯有 困難者,得經第三條第二項至第四項所定其等級提交機關 或同條第五項所定其等級核定機關同意,並報請主管機關 備查後,免執行該事項或控制措施;其為主管機關者,經 其同意後,免予執行。

公務機關之資通安全責任等級為 A 級或 B 級者,應依主管機關指定之方式,提報第一項及第二項事項之辦理情形。

中央目的事業主管機關得要求所管特定非公務機關,依其指定之方式提報第一項及第二項事項之辦理情形。

第十二條 本辦法之施行日期,由主管機關定之。

本辦法修正條文自發布日施行。

附表一 資通安全責任等級 A 級之公務機關應辦事項

制度面向	辨理項目	辦理項目細項	辨理內容
		1	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
	資通系統分級	及防護基準	九完成資通系統分級,並完成附表十之
			控制措施;其後應每年至少檢視一次資
			通系統分級妥適性。
			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
	<b>資訊安全管理</b>	系統之導入及通	27001 等資訊安全管理系統標準、其他
管理面	過公正第三方	•	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,於三年內完成公正第三方
			驗證,並持續維持其驗證有效性。
	資通安全專責	人員	初次受核定或等級變更後之一年內,配
			置四人;須以專職人員配置之。
	內部資通安全		每年辦理二次。
	業務持續運作		全部核心資通系統每年辦理一次。
	資安治理成熟	·	每年辦理一次。
	安全性檢測	弱點掃描	全部核心資通系統每年辦理二次。
	3 2 12 13 13	渗透測試	全部核心資通系統每年辦理一次。
		網路架構檢視	
		網路惡意活動	
		檢視	
		使用者端電腦	,
	資通安全健	惡意活動檢視	<b>毎年辦理一次。</b>
	診	伺服器主機惡	
		意活動檢視	
		目錄伺服器設	
ルルナ		定及防火牆連	
技術面		線設定檢視	1.1.4.1.2.1.2.1.2.1.2.1.2.1.2.1.2.1.2.1.
			初次受核定或等級變更後之一年內,完
			成威脅偵測機制建置,並持續維運及依
			主管機關指定之方式提交監控管理資
	資通安全威脅	偵測管理機制	料。其監控範圍應包括本表所定「端點」
			偵測及應變機制」與「資通安全防護」
			之辨理內容、目錄服務系統與機關核心
			資通系統之資通設備紀錄及資訊服務   北座田知七和傑。
			或應用程式紀錄。
	<b>北</b>		初次受核定或等級變更後之一年內,依
	政府組態基準		主管機關公告之項目,完成政府組態基
			準導入作業,並持續維運。

	資通安全弱)	點通報機制	一、初次受核定或等級變更後之一年 內次完成資通安全弱點通報之一 學 學 是 一 一 內,完成資 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一
	端點偵測及	應變機制	一、初次受核定或等級變更後之二年 內、完成 內、完成 一、 內、完成 一、 一、 一、 一、 一、 一、 一、 一、
	資通 <del>安全</del> 防護	防舞 大樓 人機 具核者式 進攻 大時 大樓 人人	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。
認知與訓練	資通安全 教育訓練	資月 資通安全專職人 員 資通安全專職人人 員 一般使用者及主	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。 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。 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

- 一、初次受核定或等級變更後之一年內,至少四名資通安全專職人員,分別各自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。
- 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, 應於修正施行後一年內符合規定。

#### 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構; 第三方核發之驗證證書應有前開委託機構之認證標誌。
- 三、資通安全專職人員,指應全職執行資通安全業務者。
- 四、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。
- 五、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。
- 六、端點偵測及應變機制,指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或 異常活動行為分析及相關威脅程度呈現功能之防護作業。
- 七、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。

附表二 資通安全責任等級 A 級之特定非公務機關應辦事項

制度面向	辨理項目	辨理項目細項	辨理內容
	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,並完成附 表十之控制措施;其後應每年至少檢 視一次資通系統分級妥適性。
管理面	資訊安全管理過公正第三方	系統之導入及通 之驗證	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,於三年內完成公 正第三方驗證,並持續維持其驗證有 效性。
	資通安全專責	人員	初次受核定或等級變更後之一年內, 配置四人。
	內部資通安全	稽核	每年辦理二次。
	業務持續運作	演練	全部核心資通系統每年辦理一次。
	安全性檢測	弱點掃描	全部核心資通系統每年辦理二次。
	Z I I I I I I I	渗透測試	全部核心資通系統每年辦理一次。
		網路架構檢視	
		網路惡意活動	
		檢視	
		使用者端電腦	
	資通安全健	惡意活動檢視	每年辦理一次。
	診	伺服器主機惡	
		意活動檢視	
		目錄伺服器設	
		定及防火牆連	
技術面		線設定檢視	
	資通安全威脅	偵測管理機制	初次受核定或等級變更後之一年內, 完成威脅偵測機制建置, 並持續維運。其監控範圍應包括本表所定「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。
	資通安全弱點	通報機制	一、關鍵基礎設施提供者初次受核定 或等級變更後之一年內,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, 應於修正施行後一年內,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	防網具器子制入禦具之統用進脅施軟防郵,件傾制對心,式持擊體將伺備濾及服通備火性禦勢 外資應防續防續防續 外資應防續 對於資 大性樂學	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。
認知	資通安全 教育訓練	資人 資員 資員 一章 一章 一章 一章 一章 一章 一章 一章 一章 一章	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。 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。 每人每年接受三小時以上之資通安全 通識教育訓練。
與訓練	資通安全專業證照		一、初次受核定或等級變更後之一年 內,至少四名資通安全專責人 員,各自持有證照一張以上,並 持續維持證照之有效性。 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, 應於修正施行後一年內符合規 定。

#### 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構;

第三方核發之驗證證書應有前開委託機構之認證標誌。

- 三、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業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。
- 六、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍 內,另行訂定其所管特定非公務機關之資通安全應辦事項。

附表三 資通安全責任等級 B 級之公務機關應辦事項

制度面向	辨理項目	辦理項目細項	辨理內容
		l	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
	資通系統分級	及防護基準	九完成資通系統分級,並完成附表十之
			控制措施;其後應每年至少檢視一次資
			通系統分級妥適性。
			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
	<b>資訊安全管理</b>	系統之導入及通	27001 等資訊安全管理系統標準、其他
管理面	過公正第三方	•	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,於三年內完成公正第三方
			驗證,並持續維持其驗證有效性。
	資通安全專責	人員	初次受核定或等級變更後之一年內,配
			置二人;須以專職人員配置之。
	內部資通安全		每年辦理一次。
	業務持續運作	,	全部核心資通系統每二年辦理一次。
	資安治理成熟	·	每年辦理一次。
	安全性檢測	弱點掃描	全部核心資通系統每年辦理一次。
		渗透測試	全部核心資通系統每二年辦理一次。
		網路架構檢視	
		網路惡意活動	
		檢視	
	次设的入地	使用者端電腦	
	資通安全健	惡意活動檢視	每二年辦理一次。
	診	伺服器主機惡	
		意活動檢視	
		目錄伺服器設	
技術面		定及防火牆連線設定檢視	
3人7円 四		冰双火烟机	初次受核定或等級變更後之一年內,完
			料。其監控範圍應包括本表所定「端點
	資通安全威脅	偵測管理機制	
			之辦理內容、目錄服務系統與機關核心
			資通系統之資通設備紀錄及資訊服務
			或應用程式紀錄。
			初次受核定或等級變更後之一年內,依
	政府組態基準		主管機關公告之項目,完成政府組態基
	12/11/11/11/11/11		本導入作業,並持續維運。 1
	I		

	資通安全弱)	點通報機制	一、初次受核定或等級變更後之一年 內,完成資通安全弱點通報依主管機關指定之方式提交資訊資產 機關指定之方式提交資訊資產 點資料。 二、本辦法中華民國一百十年內房 應於修正施行後一年內內 應於修正施行後一年內內 通安全弱點通報機制導入作業之 並持續維運及依主管機關指定 方式提交資訊資產盤點資料。
	端點偵測及	應變機制	一、初次受核定或等級變更後之二年 初次受核定或等級變更後之二年 內,完成端頂測及應變機主管機 關指定之方式提交偵測資料。 二、本辦法中華民國一百十年沒 一下, 一下, 一下, 一下, 一下, 一下, 一下, 一下,
	資通安全 防護	防毒軟體 網有所 與有, 過 時 時 時 時 時 時 時 時 時 時 時 時 り り り り り り り	初次受核定或等級變更後之一年內,完 一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。
認知與訓練	資通安全 教育訓練	資月 資通安全專職人 員 資通安全專職人 員以外之資訊人 員 一般使用者及主	通安全專業課程訓練或資通安全職能訓練。 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。

資通安全專業證照及職能訓練 證書

- 一、初次受核定或等級變更後之一年內,至少二名資通安全專職人員,分別各自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。
- 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, 應於修正施行後一年內符合規 定。

#### 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構; 第三方核發之驗證證書應有前開委託機構之認證標誌。
- 三、資通安全專職人員,指應全職執行資通安全業務者。
- 四、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。
- 五、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。
- 六、端點偵測及應變機制,指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或 異常活動行為分析及相關威脅程度呈現功能之防護作業。
- 七、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。

## 附表四 資通安全責任等級 B 級之特定非公務機關應辦事項

制度面向	辨理項目	辦理項目細項	辦理內容
			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
	資通系統分級	及防護基準	九完成資通系統分級,並完成附表十之
			控制措施;其後應每年至少檢視一次資
			通系統分級妥適性。
			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
<b>然</b>	<b>資訊安全管理</b>	系統之導入及通	27001 等資訊安全管理系統標準、其他
管理面	過公正第三方	• • •	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,於三年內完成公正第三方
			驗證,並持續維持其驗證有效性。
	資通安全專責	人員	初次受核定或等級變更後之一年內,配
			置二人。
	內部資通安全	稽核	每年辦理一次。
	業務持續運作	演練	全部核心資通系統每二年辦理一次。
	安全性檢測	弱點掃描	全部核心資通系統每年辦理一次。
	女主任做例	渗透測試	全部核心資通系統每二年辦理一次。
		網路架構檢視	
		網路惡意活動	
		檢視	
		使用者端電腦	
	資通安全健	惡意活動檢視	· 每二年辦理一次。
	診	伺服器主機惡	
		意活動檢視	
		目錄伺服器設	
		定及防火牆連	
技術面		線設定檢視	
			初次受核定或等級變更後之一年內,完
			成威脅偵測機制建置,並持續維運。其
	音诵安全 威脅	偵測管理機制	監控範圍應包括本表所定「資通安全防
	X Z Z Z X X	X (1/1 B - 2 1/2   1/1	護」之辦理內容、目錄服務系統與機關
			核心資通系統之資通設備紀錄及資訊
			服務或應用程式紀錄。
			一、 關鍵基礎設施提供者初次受核定
			或等級變更後之一年內,完成資
	資通安全弱點	通報機制	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。

			_ Labylatton - 14 . n
			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,
			應於修正施行後一年內,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。
		防毒軟體	
		網路防火牆	
		具有郵件伺服器	
		者,應備電子郵	初办马拉宁求签织綫再络之一年内,宁
	次以中入	件過濾機制	初次受核定或等級變更後之一年內,完
	資通安全	入侵偵測及防禦	成各項資通安全防護措施之啟用,並持
	防護	機制	續使用及適時進行軟、硬體之必要更新
		具有對外服務之	- 或升級。
		核心資通系統	
		者,應備應用程	
		式防火牆	
		資通安全專責人 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。
			每人每二年至少接受三小時以上之資
	資通安全	資通安全專責人	
	教育訓練	員以外之資訊人員	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。
認知		一般使用者及主	每人每年接受三小時以上之資通安全
與訓練		管	通識教育訓練。
77 WINK			一、 初次受核定或等級變更後之一年
			內,至少二名資通安全專責人員,
			各自持有證照一張以上,並持續
		세스 ১٠৫ 대학	維持證照之有效性。
	資通安全專:	<b></b>	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,
			應於修正施行後一年內符合規
			定。
			AC -

#### 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構; 第三方核發之驗證證書應有前開委託機構之認證標誌。
- 三、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業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。
- 六、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍 內,另行訂定其所管特定非公務機關之資通安全應辦事項。

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	辨理項目	辦理項目細項	辦理內容
172714	7,1-7,1	1 / 1 - / 3 - 7	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
	資通系統分級	及防護基準	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。
			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
管理面	次却点入然理	久 st → 道 >	27001 等資訊安全管理系統標準、其他
	資訊安全管理	系統之等八	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	1 吕	初次受核定或等級變更後之一年內,配
	貝地女生寺貝	八貝	置一人;須以專職人員配置之。
	內部資通安全		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。
	en A Li IA mi	弱點掃描	全部核心資通系統每二年辦理一次。
	安全性檢測	渗透測試	全部核心資通系統每二年辦理一次。
		網路架構檢視	
		網路惡意活動	
		檢視	
		使用者端電腦	
	資通安全健	惡意活動檢視	   每二年辦理一次。
	診	伺服器主機惡	
		意活動檢視	
		目錄伺服器設	
		定及防火牆連	
技術面		線設定檢視	
			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。
	資通安全弱點	通報機制	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 網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制	· 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。
認知	資通安全 教育訓練	資人 資員 資員 一 資員 一 一 一 会 会 会 会 会 会 会 会 会 の の の の の の の の の の の の の	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。 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。 每人每年接受三小時以上之資通安全
與訓練	資通安全專業證書	主管 證照及職能訓練	通識教育訓練。 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。

附表六 資通安全責任等級 C 級之特定非公務機關應辦事項

制度面向	辨理項目	辦理項目細項	辦理內容	
	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	
	貝迪尔統分級	及防護基华	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。	
			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	
管理面	   資訊安全管理	名はつ道 λ	27001 等資訊安全管理系統標準、其他	
	貝凱女王官庄	示例 <b>之</b> 号八	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	人旨	初次受核定或等級變更後之一年內,配	
	<b>其巡女王</b> 守貝	<b>八</b> 只	置一人。	
	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。	
	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。	
		渗透測試	全部核心資通系統每二年辦理一次。	
		網路架構檢視		
		網路惡意活動		
		檢視		
		使用者端電腦	与一 左 titio rm	
	資通安全健	惡意活動檢視		
	診	伺服器主機惡	<b>  每二年辦理一次。</b>	
		意活動檢視		
		目錄伺服器設		
		定及防火牆連		
技術面		線設定檢視		
			一、 關鍵基礎設施提供者初次受核定	
			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。	
	資通安全弱點	通報機制	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 網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制	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。
認知與訓練	資通安全 教育訓練	資人 資人 資人 資人 資人 資人 一資人 一百 一百 一百 一百 一百 一百 一百 一百 一百 一百	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。 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。
	資通安全專業	一般使用者及 主管 證照	每人每年接受三小時以上之資通安全 通識教育訓練。 初次受核定或等級變更後之一年內,至 少一名資通安全專責人員持有證照一 張以上,並持續維持證照之有效性。

#### 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、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 三、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。
- 四、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。
- 五、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。

附表七 資通安全責任等級 D 級之各機關應辦事項

制度面向	辨理項目	辨理項目細項	辦理內容
技術面	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
4文4号 国	防護	網路防火牆	續使用及適時進行軟、硬體之必要更新 或升級。
認知	資通安全	一般使用者及主	每人每年接受三小時以上之資通安全
與訓練	教育訓練	管	通識教育訓練。

備註:特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之 範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。

### 附表八 資通安全責任等級E級之各機關應辦事項

制度面向	辨理項目	辨理項目細項	辨理內容
認知	資通安全	一般使用者及主	每人每年接受三小時以上之資通安全
與訓練	教育訓練	管	通識教育訓練。

備註:特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範 圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。

附表九 資通系統防護需求分級原則

防護需求 等級	官	中	善
機密性	發生資通安全事件致資通系統受影響時,可能造成未經授權之資運、資惠 數機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資 通系統受影響時,可能 造成未經授權之資訊揭露,對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資 通系統受影響時,可能 造成未經授權之資訊揭露,對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資 通系 受影響時,可能 造成資訊錯誤或之營運 等情事,對機關之營運、資產或信譽等方面將產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資 通系統受影響時,可能 造成資訊錯誤或遭竄改 等情事,對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資 通系統受影響時,可能 造成資訊錯誤或遭竄改 等情事,對機關之營運、 資產或信譽等方面將產 生有限之影響。
可用性	發生資海安全事件致資 選舉 實通 安全事時 資 過 影響 資 過 光 資 過 光 數 資 也 表 數 或 使 用 之 資 產 生 數 信 譽 等 页 重 生 非 常 重 或 类 更 或 类 更 或 或 或 或	發生資子 等件致資 通安全事件致資 通 多響 資 資 數學 資 報 表 數	發生資子 等件致資 通 经 等 等 等 等 等 等 资 。
法律遵循性	如設安實資行。 實實作涉令等 實實不 實達作 實達 實達 實達 實達 實達 實達 實達 實達 實達 實達	如設安資資資化行性人人懲人	其他資通系統設置或運 作於法令有相關規範之 情形。

備註:資通系統之防護需求等級,以與該系統相關之機密性、完整性、可用性及法律遵循性 構面中,任一構面之防護需求等級之最高者定之。

附表十 資通系統防護基準

系統	防護需求			
分級				
控制措施	色	高	中	普
114 —	措施內			
構面	容			
存取控制	帳號管	之閒置時間或可 使用期限時,系 統應自動將使用 者登出。	二、資通系統開系統開系統開系統用核連審 人。 一、資源縣縣 人。 一、 一、 資本 , 一、 等级 , 一、 有级 , 一、 , 一、 , 一、 , 一、 , 一、 , , 一、 , , , ,	建立帳號管理機制, 包含帳號之申請、建 立、修改、啟用、。 用及刪除之程序。
		有控制措施。		6 T. b
	最小權限	採最小權限原則,僅 使用者行為之程序) 能,完成指派任務所	無要求。	
	遠端存取	一、遠端存取之來源 及管理之存取控 二、等級「普」之所	, , ,	一、野之型權制, 文件用作 大人

		1		14 明 → 如 ㎞ ጣ
				機關內部網段
				或資通系統後
				臺之連線。
				四、應採用加密機
				制。
		一、應定期審查機關	<b>剥所保留資通系統產</b>	一、訂定日誌之記錄
		生之日誌。		時間週期及留
		二、等級「普」之所	有控制措施。	存政策,並保留
				日誌至少六個
				月。
				二、確保資通系統有
	記錄事			記錄特定事件
	件			之功能,並決定
				應記錄之特定
				資通系統事件。
				三、應記錄資通系統
				管理者帳號所
				執行之各項功
				能。
		資通系統產生之日誌	應包含事件類型、發生	時間、發生位置及任
	日誌紀	何與事件相關之使用	者身分識別等資訊,拐	《用單一日誌機制,確
	錄內容	保輸出格式之一致性	, 並應依資通安全政	策及法規要求納入其
士以一		他相關資訊。		
事件日	日誌儲	依據日誌儲存需求,	配置所需之儲存容量	0
誌與可	存容量			
歸責性		一、機關規定需要即	資通系統於日誌處理	失效時,應採取適當
		時通報之日誌	之行動。	
		處理失效事件		
		發生時,資通系		
	日誌處	統應於機關規		
	理失效	定之時效內,對		
	之回應	特定人員提出		
		警告。		
		二、等級「中」及「普」		
		之所有控制措		
		施。		
		一、系統內部時鐘應	定期與基準時間源進	資通系統應使用系
		行同步。		統內部時鐘產生日
	時戳及	二、等級「普」之所	有控制措施。	誌所需時戳,並可以
	校時			對應到世界協調時
	,			間(UTC)或格林威治
				標準時間(GMT)。
	日誌資	一、定期備份日誌至	一、應運用雜湊或其	對日誌之存取管理,
	日誌資	一、定期備份日誌至	一、應運用雜湊或其	對日誌之存取管理,

	如五四	<b>万久从从上</b> 井	4 法 4 上 4 、	世四头一站四二十
	訊之保	原系統外之其		僅限於有權限之使
	護	他實體系統。	完整性確保機	用者。
		二、等級「中」之所	制。	
		有控制措施。	二、等級「普」之所	
			有控制措施。	
		一、應將備份還原,	一、應定期測試備份	一、訂定系統可容忍
		作為營運持續	資訊,以驗證備	資料損失之時
		計畫測試之一	份媒體之可靠	間要求。
		部分。	性及資訊之完	二、執行系統源碼與
		二、應在與運作系統	整性。	資料備份。
	系統備	不同地點之獨	二、等級「普」之所	
	分份	立設施或防火	有控制措施。	
	177	櫃中,儲存重要		
營運持		資通系統軟體		
續計畫		與其他安全相		
		關資訊之備份。		
		三、等級「中」之所		
		有控制措施。		
		一、訂定資通系統從	中斷後至重新恢復服	無要求。
		務之可容忍時間.	要求。	
	系統備	二、原服務中斷時,	於可容忍時間內,由	
	援		方式取代並提供服	
		務。		
		一、對資通系統之存	資通系統應具備唯-	一識別及鑑別機關使
	內部使	取採取多重認證		用者行為之程序)之
	用者之	技術。	功能,禁止使用共用	
	識別與	二、等級「中   及「普		· 11 - 12 G
	鑑別	之所有控制措		
		施。		
		一、身分驗證機制應		一、使用預設密碼
		入或密碼更換當		登入系統時,
		二、密碼重設機制對	•	應於登入後要
識別與			及具有時效性符記。	求立即變更。
鑑別		三、等級「普」之所		二、身分驗證相關
		1 1 2	// <b>/</b> =   <b>/</b>   <b>/</b>	資訊不以明文
	身分驗			傳輸。
	證管理			三、具備帳戶鎖定
				機制,帳號登
				入進行身分驗
				證失敗達五次
				後,至少十五
				分鐘内不允許
				該帳號繼續嘗
<u> </u>				<b> </b>

	T	
		試登入或使用
		機關自建之失
		<b></b>
		四、使用密碼進行
		驗證時,應強
		制最低密碼複
		雜度;強制密
		碼最短及最長
		之效期限制。
		五、密碼變更時,至
		少不可以與前
		三次使用過之
		密碼相同。
		六、第四點及第五
		點所定措施,
		對非內部使用
		者,可依機關
		自行規範辦
		理。
	鑑別資	資通系統應遮蔽鑑別過程中之資訊。
	訊回饋	
	加密模	資通系統如以密碼進行鑑別時,該密碼應 無要求。
	組鑑別	加密或經雜湊處理後儲存。
	非內部	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之
	使用者	程序)。
	之識別	
	與鑑別	
	系統發	針對系統安全需求(含機密性、可用性、完整性)進行確認。
	展生命	
	週期需	
	求階段	
	系統發	一、根據系統功能與要求,識別可能影響 無要求。
	展生命	系統之威脅,進行風險分析及評估。
系統與	週期設	二、將風險評估結果回饋需求階段之檢核
服務獲	計階段	項目,並提出安全需求修正。
服		一、執行「源碼掃描」 一、應針對安全需求實作必要控制措
ান্		安全檢測。    施。
	系統發	二、系統應具備發生 二、應注意避免軟體常見漏洞及實作必
	展生命	嚴重錯誤時之通  要控制措施。
	週期開	知機制。
	發階段	三、等級「中」及「普」 短錯誤訊息及代碼,不包含詳細之
		之所有控制措 錯誤訊息。
		施。

		1 1 1 5 6 6 1 1 5	
	系統發	一、執行「滲透測試」 執行「弱點掃描」安	·全檢測。
	展生命	安全檢測。	
	週期測	二、等級「中」及「普」	
	試階段	之所有控制措	
	DOTE 12	施。	
		一、於系統發展生命週期之維運階段,應	一、於部署環境中
		執行版本控制與變更管理。	應針對相關資
	系統發	二、等級「普」之所有控制措施。	通安全威脅,
	展生命		進行更新與修
	週期部		補,並關閉不
	署與維		必要服務及埠
	運階段		口。
			二、資通系統不使
			用預設密碼。
	系統發	資通系統開發如委外辦理,應將系統發展生命	命週期各階段依等級
	展生命	將安全需求(含機密性、可用性、完整性)	•
	週期委		
	外階段		
	獲得程	  開發、測試及正式作業環境應為區隔。	無要求。
	序	<b>州</b> 级	711 X 17
	系統文	應儲存與管理系統發展生命週期之相關文件	- 0
	件		
		一、資通系統應採用 無要求。	無要求。
		加密機制,以防	
		止未授權之資	
		訊揭露或偵測	
		資訊之變更。但	
		傳輸過程中有	
		替代之實體保	
		護措施者,不在	
	<b>壮</b> 从 、	此限。	
系統與	傳輸之	二、使用公開、國際	
通訊保	機密性	機構驗證且未	
護	與完整	遭破解之演算	
	性	法。	
		三、支援演算法最大	
		長度金鑰。	
		四、加密金鑰或憑證	
		應定期更換。	
		五、伺服器端之金鑰	
		保管應訂定管	
		理規範及實施	
		應有之安全防	

		護措施。		
		資通系統重要組態設	無要求。	無要求。
	資料儲	定檔案及其他具保護		
	存之安	需求之資訊應加密或		
	全	以其他適當方式儲		
		存。		
	漏洞修	一、定期確認資通系統	充相關漏洞修復之狀	系統之漏洞修復應
	· 海河沙 復	態。		測試有效性及潛在
	1交	二、等級「普」之所有	<b>肯控制措施</b> 。	影響,並定期更新。
		一、資通系統應採用	一、監控資通系統,	發現資通系統有被
		自動化工具監	以偵測攻擊與	入侵跡象時,應通
		控進出之通信	未授權之連	報機關特定人員。
		流量,並於發現		
	資通系		通系統之未授	
	統監控	權之活動時,針	· ·	
			二、等級「普」之所	
_		分析。	有控制措施。	
系統與		二、等級「中」之所		
資訊完		有控制措施。		
整性		一、應定期執行軟體	一、使用完整性驗證	無要求。
		與資訊完整性	工具,以偵測未	
		檢查。	授權變更特定軟	
		二、等級「中」之所	體及資訊。	
	軟體及	有控制措施。	二、使用者輸入資料	
	資訊完		合法性檢查應置	
	整性		放於應用系統伺	
			服器端。	
			三、發現違反完整性時、容易多姓應	
			時,資通系統應	
			實施機關指定之	
			安全保護措施。	

備註:特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範 圍內,另行訂定其所管特定非公務機關之系統防護基準。

## 四、資通安全事件通報及應變辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

### 第一章 總則

第一條 本辦法依資通安全管理法(以下簡稱本法)第十四條第 四項及第十八條第四項規定訂定之。

第二條 資通安全事件分為四級。

公務機關或特定非公務機關(以下簡稱各機關)發生 資通安全事件,有下列情形之一者,為第一級資通安全事 件:

- 一、非核心業務資訊遭輕微洩漏。
- 二、非核心業務資訊或非核心資通系統遭輕微竄改。
- 三、非核心業務之運作受影響或停頓,於可容忍中斷 時間內回復正常運作,造成機關日常作業影響。

各機關發生資通安全事件,有下列情形之一者,為第 二級資通安全事件:

- 一、非核心業務資訊遭嚴重洩漏,或未涉及關鍵基礎 設施維運之核心業務資訊遭輕微洩漏。
- 二、非核心業務資訊或非核心資通系統遭嚴重竄改, 或未涉及關鍵基礎設施維運之核心業務資訊或核 心資通系統遭輕微竄改。
- 三、非核心業務之運作受影響或停頓,無法於可容忍 中斷時間內回復正常運作,或未涉及關鍵基礎設 施維運之核心業務或核心資通系統之運作受影響 或停頓,於可容忍中斷時間內回復正常運作。

各機關發生資通安全事件,有下列情形之一者,為第 三級資通安全事件:

- 一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重 洩漏,或一般公務機密、敏感資訊或涉及關鍵基 礎設施維運之核心業務資訊遭輕微洩漏。
- 二、未涉及關鍵基礎設施維運之核心業務資訊或核心 資通系統遭嚴重竄改,或一般公務機密、敏感資 訊、涉及關鍵基礎設施維運之核心業務資訊或核 心資通系統遭輕微竄改。
- 三、未涉及關鍵基礎設施維運之核心業務或核心資通 系統之運作受影響或停頓,無法於可容忍中斷時 間內回復正常運作,或涉及關鍵基礎設施維運之 核心業務或核心資通系統之運作受影響或停頓, 於可容忍中斷時間內回復正常運作。

各機關發生資通安全事件,有下列情形之一者,為第 四級資通安全事件:

- 一、一般公務機密、敏感資訊或涉及關鍵基礎設施維 運之核心業務資訊遭嚴重洩漏,或國家機密遭洩 漏。
- 二、一般公務機密、敏感資訊、涉及關鍵基礎設施維 運之核心業務資訊或核心資通系統遭嚴重竄改, 或國家機密遭竄改。
- 三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓,無法於可容忍中斷時間內回復正常運作。

第三條 資通安全事件之通報內容,應包括下列項目:

- 一、發生機關。
- 二、發生或知悉時間。
- 三、狀況之描述。
- 四、等級之評估。

五、因應事件所採取之措施。

六、外部支援需求評估。

七、其他相關事項。

第二章 公務機關資通安全事件之通報及應變

第四條 公務機關知悉資通安全事件後,應於一小時內依主管機關指定之方式及對象,進行資通安全事件之通報。

前項資通安全事件等級變更時,公務機關應依前項規 定,續行通報。

公務機關因故無法依第一項規定方式通報者,應於同項規定之時間內依其他適當方式通報,並註記無法依規定方式通報之事由。

公務機關於無法依第一項規定方式通報之事由解除後, 應依該方式補行通報。

- 第五條 主管機關應於其自身完成資通安全事件之通報後,依 下列規定時間完成該資通安全事件等級之審核,並得依審 核結果變更其等級:
  - 一、通報為第一級或第二級資通安全事件者,於接獲 後八小時內。
  - 二、通報為第三級或第四級資通安全事件者,於接獲 後二小時內。

總統府與中央一級機關之直屬機關及直轄市、縣(市) 政府,應於其自身、所屬、監督之公務機關、所轄鄉(鎮、 市)、直轄市山地原住民區公所與其所屬或監督之公務機關, 及前開鄉(鎮、市)、直轄市山地原住民區民代表會,完成 資通安全事件之通報後,依前項規定時間完成該資通安全 事件等級之審核,並得依審核結果變更其等級。

前項機關依規定完成資通安全事件等級之審核後,應 於一小時內將審核結果通知主管機關,並提供審核依據之 相關資訊。

總統府、國家安全會議、立法院、司法院、考試院、監察院及直轄市、縣(市)議會,應於其自身完成資通安全事件之通報後,依第一項規定時間完成該資通安全事件等級之審核,並依前項規定通知主管機關及提供相關資訊。

主管機關接獲前二項之通知後,應依相關資訊,就資通 安全事件之等級進行覆核,並得依覆核結果變更其等級。但 主管機關認有必要,或第二項及前項之機關未依規定通知 審核結果時,得就該資通安全事件逕為審核,並得為等級之 變更。

- 第六條 公務機關知悉資通安全事件後,應依下列規定時間完成損害控制或復原作業,並依主管機關指定之方式及對象辦理通知事官:
  - 一、第一級或第二級資通安全事件,於知悉該事件後 七十二小時內。
  - 二、第三級或第四級資通安全事件,於知悉該事件後三十六小時內。

公務機關依前項規定完成損害控制或復原作業後,應 持續進行資通安全事件之調查及處理,並於一個月內依主 管機關指定之方式,送交調查、處理及改善報告。

前項調查、處理及改善報告送交之時限,得經上級或監 督機關及主管機關同意後延長之。

上級、監督機關或主管機關就第一項之損害控制或復原作業及第二項送交之報告,認有必要,或認有違反法令、不適當或其他須改善之情事者,得要求公務機關提出說明及調整。

第七條 總統府與中央一級機關之直屬機關及直轄市、縣(市) 政府,就所屬、監督、所轄或業務相關之公務機關執行資通 安全事件之通報及應變作業,應視情形提供必要支援或協助。

主管機關就公務機關執行資通安全事件之應變作業, 得視情形提供必要支援或協助。

公務機關知悉第三級或第四級資通安全事件後,其資 通安全長應召開會議研商相關事宜,並得請相關機關提供 協助。

第八條 總統府與中央一級機關之直屬機關及直轄市、縣(市) 政府,對於其自身、所屬或監督之公務機關、所轄鄉(鎮、 市)、直轄市山地原住民區公所與其所屬或監督之公務機關 及前開鄉(鎮、市)、直轄市山地原住民區民代表會,應規 劃及辦理資通安全演練作業,並於完成後一個月內,將執行 情形及成果報告送交主管機關。

前項演練作業之內容,應至少包括下列項目:

- 一、每半年辦理一次社交工程演練。
- 二、每年辦理一次資通安全事件通報及應變演練。

總統府與中央一級機關及直轄市、縣(市)議會,應依 前項規定規劃及辦理資通安全演練作業。

- 第九條 公務機關應就資通安全事件之通報訂定作業規範,其 內容應包括下列事項:
  - 一、判定事件等級之流程及權責。
  - 二、事件之影響範圍、損害程度及機關因應能力之評 估。
  - 三、資通安全事件之內部通報流程。
  - 四、通知受資通安全事件影響之其他機關之方式。
  - 五、前四款事項之演練。
  - 六、資通安全事件通報窗口及聯繫方式。
  - 七、其他資通安全事件通報相關事項。

- 第十條 公務機關應就資通安全事件之應變訂定作業規範,其 內容應包括下列事項:
  - 一、應變小組之組織。
  - 二、事件發生前之演練作業。
  - 三、事件發生時之損害控制機制。
  - 四、事件發生後之復原、鑑識、調查及改善機制。
  - 五、事件相關紀錄之保全。
  - 六、其他資通安全事件應變相關事項。
- 第三章 特定非公務機關資通安全事件之通報及應變
- 第十一條 特定非公務機關知悉資通安全事件後,應於一小時 內依中央目的事業主管機關指定之方式,進行資通安全 事件之通報。

前項資通安全事件等級變更時,特定非公務機關應依 前項規定,續行通報。

特定非公務機關因故無法依第一項規定方式通報者, 應於同項規定之時間內依其他適當方式通報,並註記無法 依規定方式通報之事由。

特定非公務機關於無法依第一項規定方式通報之事 由解除後,應依該方式補行通報。

- 第十二條 中央目的事業主管機關應於特定非公務機關完成資 通安全事件之通報後,依下列規定時間完成該資通安全 事件等級之審核,並得依審核結果變更其等級:
  - 一、通報為第一級或第二級資通安全事件者,於接獲後八小時內。
  - 二、通報為第三級或第四級資通安全事件者,於接獲後二小時內。

中央目的事業主管機關依前項規定完成資通安全事件之審核後,應依下列規定辦理:

- 一、審核結果為第一級或第二級資通安全事件者,應 定期彙整審核結果、依據及其他必要資訊,依主 管機關指定之方式送交主管機關。
- 二、審核結果為第三級或第四級資通安全事件者,應 於審核完成後一小時內,將審核結果、依據及其 他必要資訊,依主管機關指定之方式送交主管 機關。

主管機關接獲前項資料後,得就資通安全事件之等 級進行覆核,並得為等級之變更。

- 第十三條 特定非公務機關知悉資通安全事件後,應依下列規 定時間完成損害控制或復原作業,並依中央目的事業主 管機關指定之方式辦理通知事宜:
  - 一、第一級或第二級資通安全事件,於知悉該事件後 七十二小時內。
  - 二、第三級或第四級資通安全事件,於知悉該事件後 三十六小時內。

特定非公務機關依前項規定完成損害控制或復原作 業後,應持續進行事件之調查及處理,並於一個月內依中 央目的事業主管機關指定之方式,送交調查、處理及改善 報告。

前項調查、處理及改善報告送交之時限,得經中央目 的事業主管機關同意後延長之。

中央目的事業主管機關就第一項之損害控制或復原作業及第二項送交之報告,認有必要,或認有違反法令、 不適當或其他須改善之情事者,得要求特定非公務機關 提出說明及調整。

特定非公務機關就第三級或第四級資通安全事件送 交之調查、處理及改善報告,中央目的事業主管機關應於

審查後送交主管機關;主管機關就該報告認有必要,或認有違反法令、不適當或其他須改善之情事者,得要求特定非公務機關提出說明及調整。

第十四條 中央目的事業主管機關就所管特定非公務機關執行 資通安全事件之通報及應變作業,應視情形提供必要支 援或協助。

> 主管機關就特定非公務機關執行資通安全事件應變 作業,得視情形提供必要支援或協助。

> 特定非公務機關知悉第三級或第四級資通安全事件 後,應召開會議研商相關事宜。

- 第十五條 特定非公務機關應就資通安全事件之通報訂定作業 規範,其內容應包括下列事項:
  - 一、判定事件等級之流程及權責。
  - 二、事件之影響範圍、損害程度及機關因應能力之評估。
  - 三、資通安全事件之內部通報流程。
  - 四、通知受資通安全事件影響之其他機關之時機及 方式。
  - 五、前四款事項之演練。
  - 六、資通安全事件通報窗口及聯繫方式。
  - 七、其他資通安全事件通報相關事項。
- 第十六條 特定非公務機關應就資通安全事件之應變訂定作業 規範,其內容應包括下列事項:
  - 一、應變小組之組織。
  - 二、事件發生前之演練作業。
  - 三、事件發生時之損害控制,及向中央目的事業主管機關請求技術支援或其他必要協助之機制。
  - 四、事件發生後之復原、鑑識、調查及改善機制。

五、事件相關紀錄之保全。 六、其他資通安全事件應變相關事項。

第四章 附則

- 第十七條 主管機關就各機關之第三級或第四級資通安全事件, 得召開會議,邀請相關機關研商該事件之損害控制、復原 及其他相關事宜。
- 第十八條 公務機關應配合主管機關規劃、辦理之資通安全演 練作業,其內容得包括下列項目:
  - 一、社交工程演練。
  - 二、資通安全事件通報及應變演練。
  - 三、網路攻防演練。
  - 四、情境演練。
  - 五、其他必要之演練。
- 第十九條 特定非公務機關應配合主管機關規劃、辦理之資通 安全演練作業,其內容得包括下列項目:
  - 一、網路攻防演練。
  - 二、情境演練。
  - 三、其他必要之演練。

主管機關規劃、辦理之資通安全演練作業,有侵害 特定非公務機關之權利或正當利益之虞者,應先經其書 面同意,始得為之。

前項書面同意之方式,依電子簽章法之規定,得以電子文件為之。

第二十條 公務機關於本辦法施行前,已針對其自身、所屬或監督之公務機關或所管之特定非公務機關,自行或與其他機關共同訂定資通安全事件通報及應變機制,並實施一年以上者,得經主管機關核定後,與其所屬或監督之公務機關或所管之特定非公務機關繼續依該機制辦理資通安

全事件之通報及應變。

前項通報及應變機制如有變更,應送主管機關重為 核定。

第二十一條 本辦法之施行日期,由主管機關定之。 本辦法修正條文自發布日施行。

## 五、特定非公務機關資通安全維護計畫實施情形稽核 辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

- 第一條 本辦法依資通安全管理法(以下簡稱本法)第七條第二項規定訂定之。
- 第二條 本辦法所定書面,依電子簽章法之規定,得以電子文件 為之。
- 第三條 主管機關除因不可抗力因素外,應每年擇定受稽核之 特定非公務機關(以下簡稱受稽核機關),並以現場實地稽 核之方式,稽核其資通安全維護計畫實施情形。

主管機關擇定前項受稽核機關時,應綜合考量其業務之重要性與機敏性、資通系統之規模與性質、資通安全事件發生之頻率與程度、資通安全演練之成果、歷年受主管機關或中央目的事業主管機關稽核之頻率與結果或其他與資通安全相關之因素。

主管機關為辦理第一項稽核,應訂定稽核計畫,其內容包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及中央目的事業主管機關協助事項。

主管機關決定前項稽核之重點領域與基準及項目時, 應綜合考量我國資通安全政策、國內外資通安全趨勢、過往 稽核計畫之內容與稽核結果,及其他與稽核資源之適當分 配或稽核成效相關之因素。

第四條 主管機關辦理前條第一項之稽核,應將稽核計畫於一個月前以書面通知受稽核機關。

受稽核機關如因業務因素或有其他正當理由,得於收 受前項通知後五日內,以書面敘明理由向主管機關申請調 整稽核日期。 前項申請,除有不可抗力之事由外,以一次為限。

- 第五條 主管機關辦理第三條第一項之稽核,得要求受稽核機關為資通安全維護計畫實施情形之說明、協力或提出相關之文件、證明資料供現場查閱,並執行下列事項,受稽核機關及其所屬人員應予配合:
  - 一、稽核前訪談。
  - 二、現場實地稽核。

受稽核機關依法律有正當理由,未能為前項說明、協力或提出資料供現場查閱者,應以書面敘明理由,向主管機關提出。

主管機關收受前項書面後,應進行審核,依下列規定辦理,並得停止稽核作業之全部或一部:

- 一、認有理由者,應將審核之依據及相關資訊記載於 稽核結果報告。
- 二、認無理由者,應要求受稽核機關依第一項規定辦理;已停止稽核作業者,得擇期續行辦理,並於 十日前以書面通知受稽核機關。
- 第六條 主管機關辦理第三條第一項之稽核,應依同條第二項 所定考量因素,就各受稽核機關分別組成三人以上之稽核 小組。

主管機關組成前項稽核小組時,應考量稽核之需求,邀請具備資通安全政策或該次稽核所需之技術、管理、法律或實務專業知識之公務機關代表或專家學者擔任小組成員, 其中公務機關代表不得少於全體成員人數之四分之一。

主管機關應以書面與稽核小組成員約定利益衝突之迴避及保密義務。

第二項之公務機關代表或專家學者,有下列情形之一者,應主動迴避擔任該次稽核之稽核小組成員:

一、本人、其配偶、三親等內親屬、家屬或上開人員

財產信託之受託人,與受稽核機關或其負責人間有財產上或非財產上之利害關係。

- 二、本人、其配偶、三親等內親屬或家屬,與受稽核機關或其負責人間,目前或過去二年內有僱傭、 承攬、委任、代理或其他類似之關係。
- 三、本人目前或過去二年內任職之機關(構)或單位, 曾為受稽核機關之顧問,其輔導項目與受稽核項 目相關。
- 四、其他情形足認擔任稽核小組成員,將對稽核結果 之公正性造成影響。
- 第七條 主管機關應於每季所定受稽核機關之稽核作業完成後 一個月內,將稽核結果報告交付該季受稽核機關。

前項稽核結果報告之內容,應包括稽核之範圍、缺失或 待改善事項、第五條第二項所定受稽核機關未能為說明、協 力或提出資料供現場查閱之情形、理由與同條第三項所定 主管機關審核結果,及其他與稽核相關之必要內容。

第八條 受稽核機關經發現其資通安全維護計畫實施情形有缺失或待改善者,應於主管機關交付稽核結果報告後一個月內,依主管機關指定之方式提出改善報告,並送交中央目的事業主管機關;主管機關及中央目的事業主管機關認有必要時,得要求該受稽核機關進行說明或調整。

前項受稽核機關提出改善報告後,應依主管機關指定 之方式及時間,提出改善報告之執行情形,並送交中央目的 事業主管機關;主管機關認有必要時,得要求該受稽核機關 進行說明或調整。

- 第九條 主管機關辦理第三條第一項之稽核,得要求受稽核機關之中央目的事業主管機關派員為必要協助。
- 第十條 本辦法之施行日期,由主管機關定之。 本辦法修正條文自發布日施行。

## 六、資通安全情資分享辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

- 第一條 本辦法依資通安全管理法(以下簡稱本法)第八條第二項規定訂定之。
- 第二條 本辦法所稱資通安全情資(以下簡稱情資),指包括下 列任一款內容之資訊:
  - 一、資通系統之惡意偵察或情蒐活動。
  - 二、資通系統之安全漏洞。
  - 三、使資通系統安全控制措施無效或利用安全漏洞之 方法。
  - 四、與惡意程式相關之資訊。
  - 五、資通安全事件造成之實際損害或可能產生之負面 影響。
  - 六、用以偵測、預防或因應前五款情形,或降低其損害之相關措施。

七、其他與資通安全事件相關之技術性資訊。

第三條 主管機關應就情資分享事宜進行國際合作。

主管機關應適時與公務機關進行情資分享。

公務機關應適時與主管機關進行情資分享。但情資已 依前項規定分享或已經公開者,不在此限。

中央目的事業主管機關應適時與其所管之特定非公務機關進行情資分享。

特定非公務機關得與中央目的事業主管機關進行情資 分享。

前項分享之情資,經中央目的事業主管機關認定足以 防止其他機關資通安全事件之發生或降低其損害者,中央 目的事業主管機關得予以獎勵。

第四條 情資有下列情形之一者,不得分享:

- 一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊,其公開或提供有侵害公務機關、個人、 法人或團體之權利或其他正當利益。但法規另有 規定,或對公益有必要,或為保護人民生命、身 體、健康有必要,或經當事人同意者,不在此限。
- 二、其他依法規規定應秘密或應限制、禁止公開之情 形。

情資含有前項不得分享之內容者,得僅就其他部分分享之。

- 第五條 公務機關或特定非公務機關(以下簡稱各機關)進行情 資分享,應就情資進行分析及整合,並規劃適當之安全維護 措施,避免情資內容、個人資料或依法規規定不得分享之資 訊外洩,或遭未經授權之存取或竄改。
- 第六條 各機關應就所接受之情資,辨識其來源之可靠性及時效性,及時進行威脅與弱點分析及研判潛在風險,並採取對應之預防或應變措施。
- 第七條 各機關進行情資整合時,得依情資之來源、接收日期、 可用期間、類別、威脅指標特性及其他適當項目與內部情資 進行關聯分析。

公務機關應就整合後發現之新型威脅情資進行分享。

- 第八條 各機關應就所接收之情資,採取適當之安全維護措施, 避免情資內容、個人資料或依法規規定不得分享之資訊外 洩,或遭未經授權之存取或竄改。
- 第九條 各機關進行情資分享,應分別依主管機關或中央目的 事業主管機關指定之方式為之。

各機關因故無法依前項規定方式進行情資分享者,分

別經主管機關或中央目的事業主管機關同意後,得以下列方式之一為之:

- 一、書面。
- 二、傳真。
- 三、電子郵件。
- 四、資訊系統。
- 五、其他適當方式。
- 第十條 未適用本法之個人、法人或團體,經主管機關或中央目 的事業主管機關同意後,得與其進行情資分享。

主管機關或中央目的事業主管機關同意前項個人、法 人或團體進行情資分享,應以書面與其約定應遵守第四條 至前條之規定。

第十一條 本辦法施行日期,由主管機關定之。 本辦法修正條文自發布日施行。

## 七、公務機關所屬人員資通安全事項獎懲辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

- 第一條 本辦法依資通安全管理法(以下簡稱本法)第十五條第 二項及第十九條第二項規定訂定之。
- 第二條 公務機關就其所屬人員辦理業務涉及資通安全事項之 獎懲,得依本辦法之規定自行訂定獎懲基準。
- 第三條 有下列情形之一者,予以獎勵:
  - 一、依本法、本法授權訂定之法規或機關內部規範, 訂定、修正及實施資通安全維護計畫,績效優良。
  - 二、稽核所屬或監督機關之資通安全維護計畫實施情 形,或辦理資通安全演練作業,績效優良。
  - 三、配合主管機關、上級或監督機關辦理資通安全維 護計畫實施情形之稽核或資通安全演練作業,經 評定績效優良。
  - 四、辦理資通安全業務切合機宜,防止資通安全事件之發生,避免本機關、其他機關或人民遭受損害。
  - 五、主動發現新型態之資通安全弱點或入侵威脅,並 進行資通安全情資分享,防止資通安全事件之發 生或降低其損害。
  - 六、積極查察資通安全維護之異狀,即時發現重大資 通安全事件,並辦理通報及應變,防止其損害擴 大。
  - 七、對資通安全業務提出具體建議或革新方案,並經採行。
  - 八、辦理資通安全人才培育事務,有具體貢獻。
  - 九、辦理資通安全科技之研發、整合、應用、產學合作或產業發展事務,有具體貢獻。

- 十、辦理資通安全軟硬體技術規範、相關服務及審驗機制發展等事務,有具體貢獻。
- 十一、辦理資通安全政策、法制研析或國際合作事務,有具體貢獻。
- 十二、辦理其他資通安全業務有具體功績。
- 第四條 有下列情形之一者,予以懲處:
  - 一、未依本法、本法授權訂定之法規或機關內部規範 辦理下列事項,情節重大:
    - (一)資通安全情資分享作業。
    - (二)訂定、修正及實施資通安全維護計畫。
    - (三)提出資通安全維護計畫實施情形。
    - (四)辦理資通安全維護計畫實施情形之稽核。
    - (五)配合上級或監督機關資通安全維護計畫實施 情形稽核結果,提出改善報告。
    - (六)訂定資通安全事件通報及應變機制。
    - (七)資通安全事件之通報或應變作業。
    - (八)提出資通安全事件調查、處理及改善報告。
  - 二、辦理資通安全業務經主管機關、上級或監督機關 評定績效不良,經疏導無效,情節重大。
  - 三、其他違反本法、本法授權訂定之法規或機關內部 規範之行為,情節重大。
  - 四、對業務督導不力,致其屬員、所屬或所監督機關之人員有前三款情形之一。
- 第五條 公務機關辦理其所屬人員之平時考核,應審酌前二條 所定獎勵及懲處情形,依事實發生之原因、經過、行為之動 機、目的、手段、表現、所生之影響等因素為之;其所屬人 員為聘用人員、約僱人員或其他與機關有僱傭關係之人員 者,其獎勵及懲處之情形並應納入續聘之參考。
- 第六條 公務機關對所屬人員作成第四條各款情形之懲處前,

應給予當事人申辯之機會;必要時,得就所涉資通安全專業事項,徵詢相關專家學者之意見。

第七條 本辦法之施行日期,由主管機關定之。 本辦法修正條文自發布日施行。

## 貳、逐條說明

# 一、資通安全管理法

條文	說 明
第一章 總則	章名。
第一條 為積極推動國家資通安全政策,加速建構國家資通安全環境,以保障國家安全,維護社會公共利益,特制定本法。	一、明定本法之立法目的。 二、隨 著 數 位 及 其 他 資 通 科 技 (Information Communication Technology)應用之普及,資通安全 議題日益受到重視。為有效規劃我 國之資通安全管理政策,落實於公、 私部門,以建構安全之資通環境,進 而保障國家安全,維護社會公共利益,特制定本法。
第二條 本法之主管機關為行政院。	明定本法之主管機關為行政院。
第三條 本法用詞,定義如下:	明定本法用詞定義,說明如下:
一、資通系統:指用以蒐集、控制、傳	一、参考美國國家標準技術研究所
輸、儲存、流通、刪除資訊或對資	( National Institute of
訊為其他處理、使用或分享之系	Standards and Technology)
統。	SP800-60 Volume I: Guild for
二、資通服務:指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。 三、資通安全:指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害,以確保其機密性、完整性及可用性。	Mapping Type of Information and Information System to Security Categories 及經濟部標準檢驗局公布國家標準 CNS 27001「資訊技術一安全技術—資訊安全管理—要求事項」等文件,於第一款至第四款規定資通系統、資通服務、資通安全及資通安全事件之定義。
四、資通安全事件:指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生,影響資通系統機能運作,構成資通安全政策之威脅。 五、公務機關:指依法行使公權力之中央、地方機關(構)或公法人。但不包括軍事機關及情報機關。	二、第五款及第六款規定公務機關及特定非公務機關。公務機關指依法行使公權力之中央、地方機關(構)或公法人,例如總統府、行政院、立法院、司法院、考試院、監察院、直轄市政府、縣(市)政府、公立社會教育機構、公立文化機構、公立醫療機構或行政法人等。另考量軍事機關

- 六、特定非公務機關:指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。
- 七、關鍵基礎設施:指實體或虛擬資產、系統或網路,其功能一旦停止運作或效能降低,對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞,經主管機關定期檢視並公告之領域。
- 八、關鍵基礎設施提供者:指維運或 提供關鍵基礎設施之全部或一 部,經中央目的事業主管機關指 定,並報主管機關核定者。
- 九、政府捐助之財團法人:指其營運 及資金運用計畫應依預算法第四 十一條第三項規定送立法院,及 其年度預算書應依同條第四項規 定送立法院審議之財團法人。

- 全管理宜由該等機關另行規定,故 定明非屬本法所稱公務機關;該等 機關之範圍,將於施行細則中規範。 特定非公務機關則包括關鍵基礎設 施提供者、公營事業及政府捐助之 財團法人。其中政府捐助之財團法 人之定義,則明定於第九款。
- 三、參考美國 31 CFR 800.208 所定關鍵 基 礎 設 施 (critical infrastructure)、日本網路安全基 本法(サイバーセキュリティ基本 法)第三條所定重要社會基礎業者、 韓國情報通信基礎保護法 (정보통신기반보호법)第二條所定 情報通信基礎設施等定義,於第七 款明定關鍵基礎設施之內涵, 並考 量關鍵基礎設施因應環境與時代變 遷,其範圍可能調整,故規定由行政 院公告之。我國現行重要關鍵基礎 設施所涉領域包括能源、水資源、通 訊傳播、交通、金融、高科技園區等; 以通訊傳播領域為例,目前該領域 之一級關鍵基礎設施均為我國第一 類電信業者;又以高科技園區為例, 園區本身為關鍵基礎設施,而提供 該園區正常運作之電力、電信及供 水等設施者,即為關鍵基礎設施提 供者,而位於園區內之廠商則為使 用者,非關鍵基礎設施提供者。行政 院為本款規定之公告時,將僅公告 領域名稱(如通訊傳播、高科技園 區),並將公布該領域內為關鍵基礎 設施提供者之組織名稱,而非公布 該組織內之關鍵基礎設施具體設 備。
- 四、考量關鍵基礎設施對國家安全、社 會公共利益、國民生活及經濟活動 有重大影響,然各維運關鍵基礎設 施之特定非公務機關其屬性及重要 性仍有不同,爰於第八款規定關鍵

基礎設施提供者為由中央目的事業主管機關指定其中具重要性者,適可要性者,適可定關鍵基礎設施提供者範疇,實別的事業主管機關於指定關鍵基礎設施提供者前,應徵詢相關公務機關、民間團體、專家學者之意見,專後並應以書面通知受核定者。

- 五、提供或維運關鍵基礎設施之全部或 一部者,如屬本法所定義之公務機 關,應遵循本法有關公務機關之規 定;至其他關鍵基礎設施之提供者, 則應遵循本法有關關鍵基礎設施提 供者之規定。
- 六、非提供或維運關鍵基礎設施功能或 重要元件設施,而僅提供關鍵基礎 設施所需用之其他設備或服務者, 雖非本法所稱關鍵基礎設施提供 者,但如其係受關鍵基礎提供者委 託辦理資通系統之建置、維運或資 通服務之提供時,仍應依第九條規 定,受委託者之監督。
- 七、本法係以風險管理概念界定規範對 象,即經由風險評估程序,認其資通 安全有相當風險者,始納入本法規 範範疇;目前係以組織為規範對象, 並非以個人為規範對象,且未及於 所有民間企業、團體,須視其是否屬 本法所定特定非公務機關之範疇而 定,併予敘明。
- 第四條 為提升資通安全,政府應提 供資源,整合民間及產業力量,提升 全民資通安全意識,並推動下列事項: 一、資通安全專業人才之培育。
  - 二、 資通安全科技之研發、整合、應 用、產學合作及國際交流合作。
  - 三、 資通安全產業之發展。
  - 四、 資通安全軟硬體技術規範、相關 服務與審驗機制之發展。

前項相關事項之推動,由主管機 關以國家資通安全發展方案定之。 一、鑒於資通安全之提升須以全民重 視為前提,並須佐以先進之資通安 全技術、軟硬體、專業人才等資資 政府應與民間共同提升全安資資 安全意識,以利先進資資資資 安全意識,以利先進資之發展 術、軟硬體、專業人才等之發展 術、軟硬體、專業人才等之發展 大條產業之振興及國際競爭力 化、第二十條研究開發之推動、第 二十一條人才之確保等規定,為本

- 條第一項規範,並於第二項明定本 條相關事事項之推動,由行政院以 國家資通安全發展方案定之。
- 二、關於租稅優惠措施,因事涉國家稅收,且現行已有產業創新條例、科學技術基本法等法律相關規定可資運用,爰不另於本法規範,併予敘明。
- 第五條 主管機關應規劃並推動國家資 通安全政策、資通安全科技發展、國際 交流合作及資通安全整體防護等相關 事宜,並應定期公布國家資通安全情勢 報告、對公務機關資通安全維護計畫實 施情形稽核概況報告及資通安全發展 方案。

前項情勢報告、實施情形稽核概 況報告及資通安全發展方案,應送立法 院備查。

- 二、為使立法院能掌握國家資通安全 情勢、行政院對公務機關資通安全 維護計畫實施情形之稽核概況及 資通安全發展方案,爰於第二項明 定第一項之報告及方案均應送立 法院備查。
- 第六條 主管機關得委任或委託其他公 務機關、法人或團體,辦理資通安全 整體防護、國際交流合作及其他資通 安全相關事務。

前項被委託之公務機關、法人或 團體或被複委託者,不得洩露在執行 或辦理相關事務過程中所獲悉關鍵基 礎設施提供者之秘密。 

- 府採購法等規定辦理。
- 二、行政院依本條規定為委任或委託, 因涉及公權力之移轉,應考量事務 之性質、對象之屬性等事項,先行 評估委任或委託辦理之適當性後, 再行為之。
- 三、為保障關鍵基礎設施提供者之秘密不因主管機關之委託或委任而有洩露的情形,明定被委託者在執行過程中就獲悉之秘密有保密之義務。
- 第七條 主管機關應衡酌公務機關及 特定非公務機關業務之重要性與機敏 性、機關層級、保有或處理之資訊種 類、數量、性質、資通系統之規模及 性質等條件,訂定資通安全責任等級 之分級;其分級基準、等級變更申請、 義務內容、專責人員之設置及其他相 關事項之辦法,由主管機關定之。

主管機關得稽核特定非公務機關 之資通安全維護計畫實施情形;其稽 核之頻率、內容與方法及其他相關事 項之辦法,由主管機關定之。

特定非公務機關受前項之稽核, 經發現其資通安全維護計畫實施有缺 失或待改善者,應向主管機關提出改 善報告,並送中央目的事業主管機關。

- 一、 考量公務機關與特定非公務機關 之規模及業務性質不一,其應遵行 之資通安全責任等級亦應有不同, 此外,資通安全責任等級宜因機關 調整、裁撤、業務變動或運用之資 通系統發生重大變更等事由,而有 所調整,以達到資通安全防護之最 適效果。就此,目前有「政府機關 (構)資通安全責任等級分級作業 規定」可作為遵循之參考;於資通 安全管理法制化後,上述諸事宜亦 應加以規定,爰於第一項明定行政 院應衡酌公務機關及特定非公務 機關業務等事項,訂定資通安全責 任等級之分級,並就其分級基準、 等級變更申請、義務內容及專責人 員之設置及其他相關事項,授權該 院訂定辦法規範。

- 之稽核,則於第十三條規範。
- 三、考量特定非公務機關依第二項規 定接受稽核後,經發現其資通安全 維護計畫實施有缺失或待改善情 形,宜由行政院及相關機關進行監 督,確認改善之狀況,爰為第三項 規定。
- 第八條 主管機關應建立資通安全情資 分享機制。

前項資通安全情資之分析、整合與 分享之內容、程序、方法及其他相關 事項之辦法,由主管機關定之。

- 一、為增進與改善我國境內面對資通安全威脅與風險之應變能力及策略擬定,應建立相關資通安全情資分享機制,爰為第一項規定。
- 二、第二項定明資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法,由行政院定之,以資遵循。
- 第九條 公務機關或特定非公務機關,於本法適用範圍內,委外辦理資 通系統之建置、維運或資通服務之提供,應考量受託者之專業能力與經驗、 委外項目之性質及資通安全需求,選 任適當之受託者,並監督其資通安全 維護情形。

考量公務機關或特定非公務機關於本法 適用範圍內委外辦理資通系統建置 外辦理資通服務之提供時,應依所委外 道里或資通服務之提供時,應依所委會當之性質與資通安全需求 通安全維護為 宣話者,此確保國家安全、社會公共利益或 個人權益,爰為本條規定。相關監督事期 也技術性及細節性內容,將於施行細則中規定。

## 第二章 公務機關資通安全管理

第十條 公務機關應符合其所屬資通安 全責任等級之要求,並考量其所保有 或處理之資訊種類、數量、性質、資 通系統之規模與性質等條件,訂定、 修正及實施資通安全維護計畫。

## 章名。

定。公務機關訂修及實施上開計畫,應衡酌機關資源之合理分配, 並依循上級或監督機關之相關資 通安全規定為之。

二、有關資通安全維護計畫之內容,將 由行政院訂定範本,提供各公務機 關參考,以利執行。

第十一條 公務機關應置資通安全長, 由機關首長指派副首長或適當人員兼 任,負責推動及監督機關內資通安全 相關事務。 為確保有效推動資通安全維護事項,公務機關應置資通安全長,由其成立相關推動組織及督導推動相關工作。考量資通安全於機關中之重要性,並參考美國二〇一四年聯邦資訊安全現代化表(Federal Information Security Modernization Act of 2014)§3554關於資訊長應指定資深資安專責人員負責相應事務規定之意旨,爰為本條規定。

第十二條 公務機關應每年向上級或監 督機關提出資通安全維護計畫實施情 形;無上級機關者,其資通安全維護 計畫實施情形應送交主管機關。 參考日本網路安全基本法第十二條有關 促進地方公共團體確保網路資訊安全相 關事項之規定,及同法第三十條規定相 關行政機關之首長應適時提供與網路資 訊安全相關之資料或資訊,以利執行所 掌事務之精神,明定公務機關應每年向 上級或監督機關提出資通安全維護計畫 實施情形,以確認其實施成效,並使上級 或監督機關得了解及稽核所屬或受監督 機關之年度資通安全維護情形。另因總 統府、立法院、司法院、考試院、監察院、 直轄市政府、縣(市)政府、直轄市議會 及縣(市)議會等公務機關無上級機關, 爰規定無上級機關者應將資通安全維護 計畫實施情形送交行政院。行政院收受 上開計畫實施情形後將予以備查,並得 視情形提供必要協助。

第十三條 公務機關應稽核其所屬或監 督機關之資通安全維護計畫實施情 形。

受稽核機關之資通安全維護計畫 實施有缺失或待改善者,應提出改善 報告,送交稽核機關及上級或監督機 關。 一、第一項規定公務機關應稽核其所 屬或監督機關之資通安全維護計 畫實施情形。各公務機關對於其所 屬或監督之各級公務機關,應依其 機關層級、業務及其他相關情形, 就稽核之基準、頻率、內容與方法 訂定相關行政規則,以利執行。稽 核時,宜考量受稽核者歷來接受行

- 政院、上級或監督機關稽核之頻率 與結果等因素,決定最適之受稽核 者。
- 二、第二項規定受稽核機關之資通安 全維護計畫實施有缺失或待改善 者,應向稽核機關及上級或監督機 關提出改善報告,以確保資通安全 維護計畫之落實及政府資通安全 維護之強度。
- 第十四條 公務機關為因應資通安全事 件,應訂定通報及應變機制。

公務機關知悉資通安全事件時, 除應通報上級或監督機關外,並應通 報主管機關;無上級機關者,應通報 主管機關。

公務機關應向上級或監督機關提 出資通安全事件調查、處理及改善報 告,並送交主管機關;無上級機關者, 應送交主管機關。

前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相 關事項之辦法,由主管機關定之。

- 一、為即時掌控資通安全事件,並有效 降低其所造成之損害,爰於第一項 規定公務機關應建立資通安全事件 之通報及應變機制。資通安全事件 之具體類型將於施行細則及本條第 四項授權訂定之辦法中規範。
- 三、考量公務機關於知悉資通安全事件 後,應進行調查、處理及改善工作, 爰於第三項規定公務機關應向上級 或監督機關提出資通安全事件調 查、處理及改善報告,並送交行政 院,以利上級機關、監督機關或行 政院監督,並得據以提供必要之協 助。
- 四、關於公務機關資通安全事件之通 報及應變,目前有「國家資通安全 通報應變作業綱要」可資遵循參 考,於本法施行後,應檢視原有機 制並依本法要求調整之,故第四項

授權行政院訂定第一項至第三項 通報及應變機制之必要事項、通報 內容、報告之提出及其他相關事項 之辦法,以利公務機關適用。

第十五條 公務機關所屬人員對於 機關之資通安全維護績效優良者,應 予獎勵。

前項獎勵事項之辦法,由主管機 關定之。 為促進公務機關所屬人員對於資通安全工作之重視與投入,該等人員於踐行本法要求事項成果優良或卓越時,應予獎勵,其獎勵辦法由行政院定之,爰為本條規定。

第三章 特定非公務機關資通安全管 理 章名。

第十六條 中央目的事業主管機關應於 徵詢相關公務機關、民間團體、專家學 者之意見後,指定關鍵基礎設施提供 者,報請主管機關核定,並以書面通知 受核定者。

關鍵基礎設施提供者應符合其所 屬資通安全責任等級之要求,並考量其 所保有或處理之資訊種類、數量、性質、 資通系統之規模與性質等條件,訂定、 修正及實施資通安全維護計畫。

關鍵基礎設施提供者應向中央目 的事業主管機關提出資通安全維護計 畫實施情形。

中央目的事業主管機關應稽核所 管關鍵基礎設施提供者之資通安全維 護計畫實施情形。

關鍵基礎設施提供者之資通安全 維護計畫實施有缺失或待改善者,應提 出改善報告,送交中央目的事業主管機 關。

第二項至第五項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法,由中央目的事業主管機關擬訂,報請主管機關核定之。

一、 第一項規定關鍵基礎設施提供者之 指定及其程序。關鍵基礎設施提供 者之資通安全維護, 乃現今國際針 對資通安全保護所重視之議題,爰 參考歐盟二〇一六年「網路與資訊 系統安全指令」(The Directive on security of network and information systems)第五條關於 關鍵服務營運商之清單、第十四條 關於關鍵服務營運商用以提供關鍵 服務之網路與資訊系統,如有影響 其安全之事件,關鍵服務營運商須 採取適當措施及最小化事件之影 響,以確保服務之持續性、美國 6 USC §132 指定關鍵基礎設施保護 計畫(Designation of critical infrastructure protection program)及第一三六三六號行政命 令有關改善關鍵基礎設施網路安全 (Executive Order 13636)、日本 網路安全基本法第六條重要社會基 礎業者之職責、韓國情報通信基礎 保護法第八條中央行政機關長官有 權指定主要資訊通信基礎設施及同 法第五條主要資訊通信基礎設施保 護措施之制定等立法例,將關鍵基 礎設施提供者納入本法之適用範 圍。

二、 因關鍵基礎設施涉及國家安全、社

- 會公共利益、國民生活及經濟活動, 爰於第二項規定關鍵基礎設施提供 者應符合其所屬資通安全責任等級 之要求,並訂定、修正及實施資通 安全維護計畫,以確保其資通安全。
- 三、為使中央目的事業主管機關掌握所 管關鍵基礎設施提供者之資通安全 維護計畫實施狀況,爰於第三項規 定關鍵基礎設施提供者應向中央目 的事業主管機關提出資通安全維護 計畫實施情形,以利中央目的事業 主管機關監督,並適時提供相關建 議或協助。
- 四、為確保資通安全維護計畫之落實, 於第四項規定中央目的事業主管機 關應稽核所管關鍵基礎設施提供者 之資通安全維護計畫實施情形。稽 核時,宜考量受稽核者歷來接受行 政院、中央目的事業主管機關稽核 之頻率與稽核結果等因素,決定最 適之受稽核者名單與頻率。
- 五、第五項規定關鍵基礎設施提供者之 資通安全維護計畫實施情形有缺失 或待改善者,應提出改善報告,送 交中央目的事業主管機關,以確保 資通安全維護計畫之落實。
- 六、考量資通安全維護計畫必要事項、 實施情形之提出、稽核之頻率、內 容與方法、改善報告之提出及其也 應遵行事項之辦法,其內容宜有一 致性,以利關鍵基礎設施提供者適 用與遵循,爰於第六項規定,由中 央目的事業主管機關擬訂,並報請 行政院核定之。
- 七、中央目的事業主管機關宜訂定特定 非公務機關資通安全維護計畫之範 本,以供非公務機關參考;行政院 並得提供必要之協助。
- 第十七條 關鍵基礎設施提供者以 外之特定非公務機關,應符合其所屬
- 一、 考量關鍵基礎設施提供者以外之特 定非公務機關亦應負相當之資通安

資通安全責任等級之要求,並考量其 所保有或處理之資訊種類、數量、性 質、資通系統之規模與性質等條件, 訂定、修正及實施資通安全維護計畫。

中央目的事業主管機關得要求所 管前項特定非公務機關,提出資通安 全維護計畫實施情形。

中央目的事業主管機關得稽核所 管第一項特定非公務機關之資通安全 維護計畫實施情形,發現有缺失或待 改善者,應限期要求受稽核之特定非 公務機關提出改善報告。

前三項之資通安全維護計畫必要 事項、實施情形之提出、稽核之頻率、 內容與方法、改善報告之提出及其他 應遵行事項之辦法,由中央目的事業 主管機關擬訂,報請主管機關核定之。 全責任,仍應訂定安全維護計畫並 提出計畫實施情形,爰參考日本網 路安全基本法第三條賦予重要社會 基礎業者配合政府資通安全政策之 協力義務之規定,於第一項明定該 等非公務機關應符合其所屬資資 全責任等級之要求,並修訂及實施 資通安全維護計畫。

- 二、鑒於資通安全維護事項與事業之經營管理關係密切,對於特定非公務機關資通安全維護之指導、監督、管理及稽核,宜由各特定非公務機關之中央目的事業主管機關執行,爰為第二項及第三項規定。
- 三、考量資通安全維護計畫必要事項、 實施情形之提出、稽核之頻率、內 容與方法、改善報告之提出及其他 應遵行事項之辦法,其內容宜有一 致性,以利第一項之特定非公務機 關適用與遵循,爰於第四項規定, 由中央目的事業主管機關擬訂,並 報請行政院核定之。
- 四、中央目的事業主管機關宜訂定特 定非公務機關資通安全維護計畫 之範本,以供特定非公務機關參 考;行政院並得提供必要之協助。
- 第十八條 特定非公務機關為因應 資通安全事件,應訂定通報及應變機 制。

特定非公務機關於知悉資通安全 事件時,應向中央目的事業主管機關 通報。

特定非公務機關應向中央目的事 業主管機關提出資通安全事件調查、 處理及改善報告;如為重大資通安全 事件者,並應送交主管機關。

前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵 行事項之辦法,由主管機關定之。

知悉重大資通安全事件時,主管 機關或中央目的事業主管機關於適當 時機得公告與事件相關之必要內容及 因應措施,並得提供相關協助。

- 規定,為第一項至第三項規定。重 大資通安全事件之認定,將於施行 細則中規範。
- 二、第四項明定第一項至第三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法,由行政院定之,以利特定非公務機關依循。
- 三、考量重大資通安全事件可能影響多數人民之生命、身體或財產安全, 宜由行政院、中央目的事業主管機關於知悉後,分別或共同公告必要之內容(例如發生原因、影響程度及 目前控制之情形等)及因應措施,並 提供相關協助,以利防範、避免損 害之擴大,爰為第五項規定。

## 第四章 罰則

第十九條 公務機關所屬人員未遵守本 法規定者,應按其情節輕重,依相關 規定予以懲戒或懲處。

前項懲處事項之辦法,由主管機 關定之。

- 第二十條 特定非公務機關有下列情形 之一者,由中央目的事業主管機關令 限期改正;屆期未改正者,按次處新 臺幣十萬元以上一百萬元以下罰鍰:
  - 一、未依第十六條第二項或第十七條 第一項規定,訂定、修正或實施 資通安全維護計畫,或違反第十 六條第六項或第十七條第四項 所定辦法中有關資通安全維護 計畫必要事項之規定。
  - 二、未依第十六條第三項或第十七條 第二項規定,向中央目的事業主 管機關提出資通安全維護計畫 之實施情形,或違反第十六條第 六項或第十七條第四項所定辦 法中有關資通安全維護計畫實 施情形提出之規定。

三、未依第七條第三項、第十六條第

章名。

對於公務機關所屬人員之懲戒、懲處本 有公務人員考績法、公務員懲戒法等規 定加以規範,惟為促進該等人員對於資 通安全工作之重視與投入,爰於本條規 定行政院應訂定懲處事項之辦法,對公 務機關所屬人員未遵守本法規定者,按 情節輕重予以懲處。

五項或第十七條第三項規定,提	
出改善報告送交主管機關、中央	
目的事業主管機關,或違反第十	
六條第六項或第十七條第四項	
所定辦法中有關改善報告提出	
之規定。	
四、未依第十八條第一項規定,訂定	
資通安全事件之通報及應變機	
制,或違反第十八條第四項所定	
辦法中有關通報及應變機制必	
要事項之規定。	
五、未依第十八條第三項規定,向中	
央目的事業主管機關或主管機	
關提出資通安全事件之調查、處	
理及改善報告,或違反第十八條	
第四項所定辦法中有關報告提	
出之規定。	
六、違反第十八條第四項所定辦法中	
有關通報內容之規定。	
第二十一條 特定非公務機關未依第十	參考歐盟二〇一六年「網路與資訊系統
八條第二項規定,通報資通安全事件,	安全指令」第二十一條要求會員國必須
由中央目的事業主管機關處新臺幣三	針對違反相關國家法規之行為,制定有
十萬元以上五百萬元以下罰鍰,並令	效罰則之意旨,並考量違反本法所定行
限期改正;屆期未改正者,按次處罰	政法上義務應受責難程度及其所生影
之。	響,針對特定非公務機關未依第十八條
	第二項規定,通報資通安全事件之情形,
	明定所課予之行政裁罰。
第五章 附則	章名。
第二十二條 本法施行細則,由主管機	本法施行細則之訂定機關。
關定之。	
第二十三條 本法施行日期,由主管機	本法施行日期,考量配套子法作業時程,
關定之。	並為周延法制,以落實本法規定之執行,

爰授權由行政院定之。

# 二、資通安全管理法施行細則

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

## 第六條、第七條、第十三條修正條文對照表

<b>東六條、東</b>	七條、第十二條修止	條又對照表
修正條文	現行條文	說明
第六條 本法第十條、第	第六條 本法第十條、第	一、第一項參照資通安全
十六條第二項及第十七	十六條第二項及第十七	管理法第三條第三款
條第一項所定資通安全	條第一項所定資通安全	資通安全定義之文
維護計畫,應包括下列	維護計畫,應包括下列	字,修正第六款文字。
事項:	事項:	二、第二項未修正。
一、核心業務及其重要	一、核心業務及其重要	三、為明確資通安全維護
性。	性。	計畫及實施情形之辦
二、資通安全政策及目	二、資通安全政策及目	理要求,爰修正第三
標。	標。	項規定。
三、資通安全推動組	三、資通安全推動組	
織。	織。	
四、專責人力及經費之	四、專責人力及經費之	
配置。	配置。	
五、公務機關資通安全	五、公務機關資通安全	
長之配置。	長之配置。	
六、資通系統及資訊之	六、資訊及資通系統之	
盤點,並標示核心	盤點,並標示核心	
資通系統及相關資	資通系統及相關資	
產。	產。	
七、資通安全風險評	七、資通安全風險評	
估。	估。	
八、資通安全防護及控	八、資通安全防護及控	
制措施。	制措施。	
九、資通安全事件通	九、資通安全事件通	
報、應變及演練相	報、應變及演練相	
關機制。	關機制。	
十、資通安全情資之評	十、資通安全情資之評	
估及因應機制。	估及因應機制。	
十一、資通系統或服務	十一、資通系統或服務	
委外辦理之管理措	委外辦理之管理措	
施。	施。	
十二、公務機關所屬人	十二、公務機關所屬人	
員辦理業務涉及資	員辦理業務涉及資	
通安全事項之考核	通安全事項之考核	

機制。

機制。

十三、資通安全維護計 書與實施情形之持 續精進及績效管理 機制。

各機關依本法第十 二條、第十六條第三項 或第十七條第二項規定 提出資通安全維護計畫 實施情形,應包括前項 各款之執行成果及相關 說明。

第一項資通安全維 護計畫之訂定、修正、實 施及前項實施情形之提 出,公務機關經其上級 或監督機關同意,得由 其上級、監督機關或其 上級、監督機關所屬公 務機關辦理;特定非公 務機關經其中央目的事 業主管機關同意,得由 其中央目的事業主管機 關、中央目的事業主管 機關所屬公務機關或中 央目的事業主管機關所 管特定非公務機關辦 理。

十三、資通安全維護計 書與實施情形之持 續精進及績效管理 機制。

各機關依本法第十 二條、第十六條第三項 或第十七條第二項規定 提出資通安全維護計畫 實施情形,應包括前項 各款之執行成果及相關 說明。

第一項資通安全維 護計畫之訂定、修正、實 施及前項實施情形之提 出,公務機關得由其上 級或監督機關辦理;特 定非公務機關得由其中 央目的事業主管機關、 中央目的事業主管機關 所屬公務機關辦理,或 經中央目的事業主管機 關同意,由其所管特定 非公務機關辦理。

- 第七條 前條第一項第一 款所定核心業務,其範 圍如下:
  - 一、公務機關依其組織 法規,足認該業務 為機關核心權責所 在。
  - 二、公營事業及政府捐 助之財團法人之主 要服務或功能。
  - 三、各機關維運、提供 關鍵基礎設施所必 要之業務。
  - 四、各機關依資通安全 責任等級分級辦法 第四條第一款至第

- 第七條 前條第一項第一 款所定核心業務,其範 圍如下:
  - 一、公務機關依其組織 法規,足認該業務 為機關核心權責所 在。
  - 二、公營事業及政府捐 助之財團法人之主 要服務或功能。
  - 三、各機關維運、提供 關鍵基礎設施所必一二、第二項未修正。 要之業務。
  - 四、各機關依資通安全 責任等級分級辦法 第四條第一款至第
- 一、考量各機關如有資通 安全責任等級分級辨 法第五條第五款所定 「屬公務機關,且業 務涉及區域性或地區 性之關鍵基礎設施事 項 | 情形,該業務亦 應屬第六條第一項第 一款所定核心業務, 爰修正第一項第四款 規定。

工 4. 上 於 工	工业 上於 工	
五款或第五條第一	五款或第五條第一	
款至第五款涉及之	款至第四款涉及之	
業務。	業務。	
前條第一項第六款	前條第一項第六款	
所稱核心資通系統,指	所稱核心資通系統,指	
支持核心業務持續運作	支持核心業務持續運作	
必要之系統,或依資通	必要之系統,或依資通	
安全責任等級分級辦法	安全責任等級分級辦法	
附表九資通系統防護需	附表九資通系統防護需	
求分級原則之規定,判	求分級原則之規定,判	
定其防護需求等級為高	定其防護需求等級為高	
者。	者。	
第十三條 本細則之施行	第十三條 本細則之施行	一、 第一項未修正。
日期,由主管機關定之。	日期,由主管機關定	二、 增訂第二項,定明本
本細則修正條文自	之。	細則修正條文之施
發布日施行。		行日期。

# 資通安全管理法施行細則

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定

條文 說明 本細則依資通安全管理法 明定本細則訂定之依據。 第一條 (以下簡稱本法)第二十二條規定訂定 之。 第二條 本法第三條第五款所稱軍事 參考國家情報工作法及檢察機關辦理刑 機關,指國防部及其所屬機關(構)、 事案件與軍事機關聯繫要點之規定,明 部隊、學校;所稱情報機關,指國家情 定本法第三條第五款所稱軍事機關及情 報工作法第三條第一項第一款及第二 報機關之範圍。 項規定之機關。

- 第三條 公務機關或特定非公務機關 (以下簡稱各機關)依本法第七條第 三項、第十三條第二項、第十六條第五 項或第十七條第三項提出改善報告, 應針對資通安全維護計畫實施情形之 稽核結果提出下列內容,並依主管機 關、上級或監督機關或中央目的事業 主管機關指定之方式及時間,提出改 善報告之執行情形:
  - 一、 缺失或待改善之項目及內容。
  - 二、 發生原因。
  - 三、 為改正缺失或補強待改善項目 所採取管理、技術、人力或資源 等層面之措施。
  - 四、前款措施之預定完成時程及執 行進度之追蹤方式。
- 第四條 各機關依本法第九條規定委 外辦理資通系統之建置、維運或資通 服務之提供(以下簡稱受託業務),選 任及監督受託者時,應注意下列事項:
  - 一、 受託者辦理受託業務之相關程 序及環境,應具備完善之資通安 全管理措施或通過第三方驗證。
  - 二、 受託者應配置充足且經適當之 資格訓練、擁有資通安全專業證 照或具有類似業務經驗之資通 安全專業人員。
  - 三、 受託者辦理受託業務得否複委 託、得複委託之範圍與對象,及

明定公務機關或特定非公務機關(以下 簡稱各機關)之資通安全維護計畫實施 情形經稽核發現缺失或待改善時,所提 改善報告應包含之內容,以及後續執行 情形之提出,說明如下:

- 一、第一款及第二款為該缺失或待改善 事項之具體項目與內容及發生原
- 二、第三款所定措施,係因應缺失或待 改善項目所採取之機關組織、作業 程序、應變機制、人員管考、教育訓 練、實體或虛擬設備等管理、技術、 人力或資源等層面之相關措施。
- 三、第四款所定預定完成時程及執行進 度之追蹤方式,係因應缺失或待改 善項目所規劃採行相關措施之時程 評估,及為確認其效果所進行之追 蹤、管考。
- 一、依本法第九條規定各機關於本法適 用範圍內,委外辦理資通系統之建 置、維運或資通服務之提供,應考量 受託者之專業能力與經驗、委外項 目之性質及資通安全需求,選任適 當之受託者,並監督其資通安全維 護情形。為利執行,爰於第一項明定 相關注意事項,說明如下:
  - (一)為確保受託者辦理受託業務之程 序及環境具安全性, 並得妥善執 行受託業務,爰為第一款及第二 款規定。第一款所稱第三方,係 指通過我國標準法主管機關委託

- 複委託之受託者應具備之資通 安全維護措施。
- 四、 受託業務涉及國家機密者,執行 受託業務之相關人員應接受適 任性查核,並依國家機密保護法 之規定,管制其出境。
- 六、受託者執行受託業務,違反資通 安全相關法令或知悉資通安全 事件時,應立即通知委託機關及 採行之補救措施。
- 七、 委託關係終止或解除時,應確認 受託者返還、移交、刪除或銷毀 履行契約而持有之資料。
- 八、 受託者應採取之其他資通安全 相關維護措施。
- 九、委託機關應定期或於知悉受託 者發生可能影響受託業務之資 通安全事件時,以稽核或其他適 當方式確認受託業務之執行情 形。

委託機關辦理前項第四款之適任 性查核,應考量受託業務所涉及國家 機密之機密等級及內容,就執行該業 務之受託者所屬人員及可能接觸該國 家機密之其他人員,於必要範圍內查 核有無下列事項:

- 一、曾犯洩密罪,或於動員戡亂時期終止後,犯內亂罪、外患罪,經判刑確定,或通緝有案尚未結案。
- 二、 曾任公務員,因違反相關安全保 密規定受懲戒或記過以上行政

- 機構認證之機構,其驗證標準可為國際、國家或團體標準。
- (二)委託機關應依受託業務之性質, 決定是否允許受託者就受託業務 為複委託;如允許複委託,應注 意得複委託之範圍與對象,及複 委託之對象應具備之資通安全維 護措施,爰為第三款規定。
- (三)考量國家機密牽涉國家之安危或 重大利益,應嚴加保護,爰於第 四款明定受託業務涉及國家 時,受託者辦理該項業務之相關 人員應接受適任性查核,管制其明 人員應保護法之規定審酌其出 境,以利各機關謹慎審酌其辨理 受託業務之合宜性及維護國家機 密。
- (四)為確保受託業務執行之適法性及 安全性,受託業務如包含客製化 資通系統之開發,應確保該資通 系統之安全性, 如委託金額達一 定金額以上,或該資通系統為委 託機關核心資通系統時,應由委 託機關自行或委託公正之第三方 進行安全性檢測之複測;且該業 務如涉及利用非自行開發之系統 或資源,受託者並應標示與揭露 該系統或資源之內容與其來源, 及提供授權證明,爰為第五款規 定。所定委託金額達新臺幣一千 萬元以上,係參考目前政府採購 法勞務採購之查核金額定之。所 稱第三方,同上開(一)之說明。
- (五)受託者執行受託業務,有違反資 通安全相關法令之情形,或思 資通安全事件時,為避免損害擴 大,應立即將相關情狀通知委 機關,並採行諸如啟動備援、 機關轉、損害管制等適當之補救 措施,爰為第六款規定。
- (六)為確保對於受託業務相關資料及 系統之保護,受託者於委託關係 結束時,應返還、移交、刪除或銷

懲處。

- 三、 曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫,從事不利國家安全或重大利益情事。
- 四、 其他與國家機密保護相關之具 體項目。

第一項第四款情形,應記載於招標公告、招標文件及契約;於辦理適任性 性查核前,並應經當事人書面同意。

- 毀為履行契約所持有之資料,爰 為第七款規定。
- (七)委託機關就委外辦理之業務,得 要求受託者依業務之性質及內 容,調整其須具備之資通安全相 關維護措施,爰為第八款規定。
- (八)為確保受託業務執行之妥適性, 委託機關應定期檢視執行狀況; 於知悉受託者發生可能影響受託 業務之資通安全事件時,亦應確 認受託業務之執行情形,爰為第 九款規定。

第五條 前條第三項及本法第十六條 第一項之書面,依電子簽章法之規定, 得以電子文件為之。 明定本辦法及本法所定書面,依電子簽章法之規定,得以電子文件為之。

- 第六條 本法第十條、第十六條第二 項及第十七條第一項所定資通安全維 護計畫,應包括下列事項:
  - 一、 核心業務及其重要性。
  - 二、 資通安全政策及目標。
  - 三、 資通安全推動組織。
  - 四、 專責人力及經費之配置。
  - 五、 公務機關資通安全長之配置。
  - 六、 資訊及資通系統之盤點,並標示 核心資通系統及相關資產。
  - 七、 資通安全風險評估。
  - 八、資通安全防護及控制措施。
  - 九、 資通安全事件通報、應變及演練 相關機制。
  - 十、 資通安全情資之評估及因應機

- 一、為利各機關訂定、修正及實施資通 安全維護計畫,爰於第一項明定該 計畫應包括之內容,說明如下:
  - (一)各機關為有效落實其資通系統之 安全管理,應釐清其核心業務, 並說明該業務之重要性為何,爰 為第一款規定。
  - (二)各機關依其業務性質推動資通安全政全維護事項,應建立資通安全政策,並應於各內部單位建立與資通安全政策一致之資通安全目標,爰為第二款規定。
- (三)第三款至第五款明定計畫應包括 機關內部推動資通安全事務之組 織,與為達成資通安全政策及目

制。

- 十一、 資通系統或服務委外辦理 之管理措施。
- 十二、公務機關所屬人員辦理業務涉 及資通安全事項之考核機制。
- 十三、資通安全維護計畫與實施情形 之持續精進及績效管理機制。

各機關依本法第十二條、第十六 條第三項或第十七條第二項規定提出 資通安全維護計畫實施情形,應包括 前項各款之執行成果及相關說明。

第一項資通安全維護計畫之訂 定、修正、實施及前項實施情形之提 出,公務機關得由其上級或監督機關 辨理;特定非公務機關得由其中央目 的事業主管機關、中央目的事業主管 機關所屬公務機關辦理,或經中央目 的事業主管機關同意,由其所管特定 非公務機關辦理。

- 標,所配置之專責人力及資源, 公務機關並應配置資通安全長。
- (四)各機關為有效推動資通安全管理,應盤點其資訊、資通系統,並應標示核心資通系統及相關資產,以利執行風險評估等作業,爰為第六款規定。
- (五)第七款明定資通安全維護計畫之 內容應包括資通安全風險評估相關之資訊,例如:機關應建立相關之政計估機制,並了實體主 資訊儲存區域、組織可實體主 技術面及作業面等資通安等 設,風險評估之範圍,包含第六 款規定盤點之資訊、資通系統及 相關資產。
- (六)第八款明定資通安全維護計畫之內容應包括機關針對其資訊、資通系統及相關資產,應採取之防護及控制措施。
- (七) 第九款明定資通安全維護計畫之 內容應包括機關資通安全事件通 報、應變及演練相關機制。
- (八)為強化各機關對於資通安全情資之應用,於第十款明定機關應之相關機制,例如於收受資通安全情資後,應評估及因應之情資後,應評估資源安全情資之內容,據以決定是否就資通安全維護計畫、資通安全事件之通報、應變方式或其他資金維護事宜為調整及因應。
- (九)第十一款明定資通安全維護計畫 應載明委外辦理資通系統或服務 時之管理措施,以利執行本法第 九條所定對受託者進行之監督。
- (十)公務機關所屬人員辦理業務涉及 資通安全事項者,應適時予以考 核,爰於第十二款明定資通安全 維護計畫應包含公務機關所屬人 員辦理業務涉及資通安全事項之 考核機制。
- (十一) 第十三款明定資通安全維護 計畫應包含該計畫與實施情形之

- 持續精進及績效管理機制,例如 計書合宜性、適切性及有效性之 持續改善方式,以及對於相關人 員之績效管理機制。
- 二、 為利各機關依本法規定提出資通安 全維護計畫實施情形,爰於第二項 明定其提出資料應包括之必要內 容。
- 三、 考量部分公務機關或特定非公務機 關之人力等行政資源可能較為不 足,其資通安全維護計畫之訂修、 執行及實施情形之提出等事宜,倘 由其上級或監督機關、中央目的事 業主管機關、中央目的事業主管機 關所屬公務機關、中央目的事業主 管機關所管特定非公務機關統一辦 理,較符合行政效率;為符合實務 執行需求,以利資通安全維護業務 之推展, 爰於第三項明定資通安全 維護計畫之訂定、修正、實施及其 實施情形之提出,除由各機關自行 辦理外,亦得由其上級或監督機關、 中央目的事業主管機關、中央目的 事業主管機關所屬公務機關辦理, 或經中央目的事業主管機關同意後 由其所管特定非公務機關辦理。
- 第七條 前條第一項第一款所定核心 業務,其範圍如下:
  - 一、公務機關依其組織法規,足認該 業務為機關核心權責所在。
  - 二、公營事業及政府捐助之財團法人 之主要服務或功能。
  - 三、各機關維運、提供關鍵基礎設施 所必要之業務。
  - 四、各機關依資通安全責任等級分級 辦法第四條第一款至第五款或第 五條第一款至第四款涉及之業 務。

前條第一項第六款所稱核心資通 系統,指支持核心業務持續運作必要 之系統,或依資通安全責任等級分級 辦法附表九資通系統防護需求分級原 則之規定,判定其防護需求等級為高 二、第二項明定第六條第一項第六款之

- 一、第一項明定第六條第一項第一款之 核心業務之範圍。公務機關之核心 業務,應視其組織法規之規定或業 務是否係屬維運、提供關鍵基礎設 施所必要進行判斷;於公營事業及 政府捐助財團法人,則視其是否係 屬主要服務或功能所在;各機關業 務如涉關鍵基礎設施,則其維運、提 供關鍵基礎設施所必要之業務,以 及各機關依資通安全責任等級分級 辦法第四條第一款至第五款或第五 條第一款至第四款涉及之業務,亦 屬各機關之核心業務。另是否係屬 核心業務,除由特定非公務機關自 行認定外,中央目的事業主管機關 亦得協助認定之,併予敘明。

者。

核心資通系統,指支持核心業務持續運作必要之系統,或依資通系統 責任等級分級辦法附表九資通系統 防護需求分級原則之規定,判定其 防護需求等級為高者,以利各機關 辦理本法及相關法令要求之事項, 並強化各機關之資通安全防護。

- 第八條 本法第十四條第三項及第十 八條第三項所定資通安全事件調查、 處理及改善報告,應包括下列事項:
  - 一、 事件發生或知悉其發生、完成損 害控制或復原作業之時間。
  - 二、 事件影響之範圍及損害評估。
  - 三、 損害控制及復原作業之歷程。
  - 四、事件調查及處理作業之歷程。
  - 五、 事件根因分析。
  - 六、為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。
  - 七、前款措施之預定完成時程及成 效追蹤機制。

明定資通安全事件調查、處理及改善報 告應包括之內容。

第九條 中央目的事業主管機關依本 法第十六條第一項規定指定關鍵基礎 設施提供者前,應給予其陳述意見之 機會。

第十條 本法第十八條第三項及第五 項所稱重大資通安全事件,指資通安 全事件通報及應變辦法第二條第四項 及第五項規定之第三級及第四級資通 安全事件。 為保障人民權益,明定中央目的事業主 管機關依本法第十六條第一項規定指定 關鍵基礎設施提供者前,應給予其陳述 意見之機會。

明定重大資通安全事件之定義。

第十一條 業主管機關知悉重大資通安全事件, 依本法第十八條第五項規定公告與事 件相關之必要內容及因應措施時,應 載明事件之發生或知悉其發生之時 間、原因、影響程度、控制情形及後 續改善措施。

前項與事件相關之必要內容及因 應措施,有下列情形之一者,不予公 告:

一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊,或公開有侵害公務機關、個人、法人

為利相關機關辦理本法第十八條第五項 重大資通安全事件之公告,使民眾了解 其事件之必要內容及因應措施,並考量 民眾權益之保護及公共利益之維護,爰 明定公告時應載明之事項及不予公告之 情形。 或團體之權利或其他正當利益。 但法規另有規定,或對公益有必 要,或為保護人民生命、身體、 健康有必要,或經當事人同意 者,不在此限。

二、 其他依法規規定應秘密、限制或 禁止公開之情形。

第一項與事件相關之必要內容及 因應措施含有前項不予公告之情形 者,得僅就其他部分公告之。

第十二條 特定非公務機關之業務涉及數中央目的事業主管機關之權責者,主管機關得協調指定一個以上之中央目的事業主管機關,單獨或共同辦理本法所定中央目的事業主管機關應辦理之事項。

考量特定非公務機關之業務性質可能涉及數個中央目的事業主管機關之權養關之權養關之權養關之營養生該等中央目的事業主管機關 非一個以上之中央目的事業主管機關,單獨或共同辦理本法所定中央目的事業主管機關應辦理之事項。

第十三條 本細則之施行日期,由主管機關定之。

明定本細則之施行日期,由主管機關定之。

# 三、資通安全責任等級分級辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 108 年 8 月 26 日行政院院臺護字第 1080184606 號令修正 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

# 第五條、第六條、第七條修正條文對照表

	777 7 6 7 9 2 1	
修正條文	現行條文	說明
第五條 各機關有下列情	第五條 各機關有下列情	一、配合科技部於一百零
形之一者,其資通安全	形之一者,其資通安全	八年將「政府資助敏
責任等級為 B級:	責任等級為 B 級:	感科技研究計畫安全
一、業務涉及公務機關	一、業務涉及公務機關	管制作業手冊」修正
捐助、資助或研發	捐助、資助或研發	為「政府資助國家核
之 <u>國家核心科技</u> 資	之敏感科學技術資	心科技研究計畫安全
訊之安全維護及管	訊之安全維護及管	管制作業手冊」,並於
理。	理。	該手冊規定國家核心
二、業務涉及區域性、地	二、業務涉及區域性、地	科技之定義,爰將現
區性民眾服務或跨	區性民眾服務或跨	行第一款所定「敏感
公務機關共用性資	公務機關共用性資	科學技術」修正為「國
通系統之維運。	通系統之維運。	家核心科技」。
三、業務涉及區域性或	三、業務涉及區域性或	二、其餘各款未修正。
地區性民眾個人資	地區性民眾個人資	
料檔案之持有。	料檔案之持有。	
四、業務涉及中央二級	四、業務涉及中央二級	
機關及所屬各級機	機關及所屬各級機	
關(構)共用性資通	關(構)共用性資通	
系統之維運。	系統之維運。	
五、屬公務機關,且業務	五、屬公務機關,且業務	
涉及區域性或地區	涉及區域性或地區	
性之關鍵基礎設施	性之關鍵基礎設施	
事項。	事項。	
六、屬關鍵基礎設施提	六、屬關鍵基礎設施提	
供者,且業務經中	供者,且業務經中	
央目的事業主管機	央目的事業主管機	
關考量其提供或維	關考量其提供或維	
運關鍵基礎設施服	運關鍵基礎設施服	
務之用戶數、市場	務之用戶數、市場	
占有率、區域、可替	占有率、區域、可替	
代性,認其資通系	代性,認其資通系	
統失效或受影響,	統失效或受影響,	
對社會公共利益、	對社會公共利益、	
民心士氣或民眾生	民心士氣或民眾生	

命、身體、財產安全	命、身體、財產安全	
將產生嚴重影響。	將產生嚴重影響。	
七、屬公立區域醫院或	七、屬公立區域醫院或	
地區醫院。	地區醫院。	
第六條 各機關維運自行	第六條 各機關維運自行	考量各機關使用之資通系
或委外 <u>設置、</u> 開發之資	或委外開發之資通系統	統有非屬自行或委外開發
通系統者,其資通安全	者,其資通安全責任等	者,例如市面販售之目錄
責任等級為 C 級。	級為C級。	服務系統、電子郵件系統
前項所定自行或委		等,係屬其自行或委外採
外設置之資通系統,指		購設置,該等具權限區分
具權限區分及管理功能		及管理功能之資通系統之
之資通系統。		資安風險仍應進行較高之
		管控作為,資通安全責任
		等級宜列為 C 級, 爰將現
		行條文列為第一項,增訂
		「設置」之情形,並增訂
		第二項,定明第一項所定
		自行或委外設置之資通系
		統之範圍。
第七條 各機關自行辦理	第七條 各機關自行辦理	配合第六條修正維運自行
資通業務,未維運自行	資通業務,未維運自行	或委外設置之資通系統者
或委外 <u>設置、</u> 開發之資	或委外開發之資通系統	之資通安全責任等級為 C
通系統者,其資通安全	者,其資通安全責任等	級,修正本條所定資通安
責任等級為D級。	級為D級。	全責任等級為 D 級之情
		形。
		<b>10</b>

# 第十一條附表一修正對照表

		修正規	定			現行規	定	説
		A 級之公務機關應				A 級之公務機關應		一、考量 資通
制度面向	辨理項目	辨理項目細項	辨理內容	制度面向	辨理項目	辨理項目細項	辨理內容	由主
	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,並完成附表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。		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,並完成附表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。	定屬
管理面	資訊安全管理 過公正第三方	系統之導入及通 之驗證	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,於三年內完成公正第三方 驗證,並持續維持其驗證有效性。		資訊安全管理 過公正第三方	!系統之導入及通 ·之驗證	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,於三年內完成公正第三方驗證,並持續維持其驗證有效性。	調關危安制爰有
	資通安全專責	人員	初次受核定或等級變更後之一年內,配置四人;須以專職人員配置之。		資通安全專責	人員	初次受核定或等級變更後之一年內,配 置四人;須以專職人員配置之。	危害 安全
	內部資通安全	稽核	每年辦理二次。	管理面	內部資通安全稽核		每年辦理二次。	項目
	業務持續運作	演練	全部核心資通系統每年辦理一次。		業務持續運作	演練	全部核心資通系統每年辦理一次。	定,
	資安治理成熟	度評估	每年辦理一次。		資安治理成熟	度評估	每年辦理一次。	行備
	安全性檢測	<u>弱點掃描</u> 渗透測試	全部核心資通系統每年辦理二次。 全部核心資通系統每年辦理一次。		XXX		一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定	害國全產
技術面	資通安全健診	灣路架構檢視 網路惡 機視 者動檢視 一般 意 器 檢視 一般 意 器 檢視 一般 意 器 檢視 一般 意 器 檢視 一般 是 發展 一般 是 發展 一般 是 最 是 最 是 最 是 最 是 最 是 最 是 最 是 最 是 最 是	每年辦理一次。		限制使用危害	:國家資通安全產	之廠商生產、研發、製造或提供之 危害國家資通安全產品。 二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管 機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管 機關核可採購之危害國家資通安 全產品,應列冊管理,且不得與公 務網路環境介接。	二 三 三 三明為測性辦名為通測應爰。使月,理稱完安管監修
	資通安全威脅	偵測管理機制	初次受核定或等級變更後之一年內,完成威脅偵測機制建置,並持續維運及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心	技術面	安全性檢測資通安全健診	網站安全弱點檢測 系統滲透測試 網路架構檢視 網路惡意活動 檢視	全部核心資通系統每年辦理二次。 全部核心資通系統每年辦理一次。 每年辦理一次。	及內資考統而安內資考統而安

			資通系統之資通設備紀錄及資訊服務	
			或應用程式紀錄。	
	山上, 华井,	24 <del>.</del>	初次受核定或等級變更後之一年內,依	
	政府組態基	半	主管機關公告之項目,完成政府組態基	
			準導入作業,並持續維運。	
			一、初次受核定或等級變更後之一年	
			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	
			<u>料。</u>	
	資通安全弱!	點通報機制	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	
			於修正施行後一年內,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。	
			一、初次受核定或等級變更後之二年	
			內,完成端點偵測及應變機制導入	
			作業,並持續維運及依主管機關指	
			定之方式提交偵測資料。	
	地里佔洲亚	庇 (試 1版 比)	二、本辦法中華民國一百十年八月二	
	端點偵測及	<u> 医愛機制</u>	十三日修正施行前已受核定者,應	
			於修正施行後二年內,完成端點偵	
			測及應變機制導入作業,並持續維	
			運及依主管機關指定之方式提交	
			<u>偵測資料。</u>	
		防毒軟體		
		網路防火牆		
		具有郵件伺服器		
		者,應備電子郵		
		件過濾機制	和力巫坛它才签加鳞西纸之 左南,它	
	次活户入	入侵偵測及防禦	初次受核定或等級變更後之一年內,完	
	資通安全	機制	成各項資通安全防護措施之啟用,並持	
	防護	具有對外服務之	續使用及適時進行軟、硬體之必要更新	
		核心資通系統	或升級。	
		者,應備應用程		
		式防火牆		
		進階持續性威脅		
		攻擊防禦措施		
÷11 k -	次江ウ入	次活应入市础)	每人每年至少接受十二小時以上之資	
認知	資通安全	資通安全專職人	通安全專業課程訓練或資通安全職能	
與訓練	教育訓練	員	訓練。	
	•	•		

		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	
	資通安全威尔	脅偵測管理機制	初次受核定或等級變更後之一年內,完成威脅偵測機制建置,並持續維運及依主管機關指定之方式提交監控管理資料。
			初次受核定或等級變更後之一年內,依
	→ □ 政府組態基準	售	主管機關公告之項目,完成政府組態基
	<b>以</b> /// 温心至	1	準導入作業,並持續維運。
		防毒軟體	了 47CFF 亚 10 % 体之
		網路防火牆	
		具有郵件伺服器	
		者,應備電子郵	
		件過濾機制	
		入侵偵測及防禦	初次受核定或等級變更後之一年內,完
	資通安全	機制	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
	防護	具有對外服務之	
		核心資通系統	或升級。
		者,應備應用程	
		式防火牆	
		進階持續性威脅	
		攻擊防禦措施	
		<b>以手</b> /// 示相他	   每人每年至少接受十二小時以上之資
		資通安全專職人 員	通安全專業課程訓練或資通安全職能訓練。
÷π 4	資通安全 教育訓練	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。
認知 與訓練		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	<u>資通安全專業證</u> 照	初次受核定或等級變更後之一年內,資 通安全專職人員總計應持有四張以上, 並持續維持證照之有效性。
未	資通安全職能評 量證書	初次受核定或等級變更後之一年內,資 通安全專職人員總計應持有四張以上, 並持續維持證書之有效性。	

嚴重,資通安 全責任等級 A 級之公務機關 宜導入資通安 全弱點通報 (VANS)機制, 以即時掌握弱 點情形,爰於 技術面增訂資 通安全弱點通 報機制之規 定,並於備註 定明其定義。 五、考量資通安全

- 威脅日趨多 樣,為提升資 通安全責任等 級A級之公務 機關主動式偵 測、漏洞防護、 行為分析與回 應之能力,宜 導入端點安全 防護作業,爰 於技術面增訂 端點偵測及應 變機制之規 定,並於備註 定明其定義。
- 六、有關資通安全 專職人員就資 通安全專業證 照及資通安全 職能訓練證書 之持有,應為 每人持有一張 以上,爰修正 相關文字,以 資明確。
- 七、現行備註欄第 二點增訂第三 方核發之驗證 證書認證標誌

_	資通安全專職人 員以外之資訊人 員 一般使用者及主 管	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。 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 證書	<b><b></b> </b>	一、初次受核定或等級變更後之一年 內,至少四名資通安全專職人員, 分別各自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。 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 於修正施行後一年內符合規定。

### 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構<u>;</u> 第三方核發之驗證證書應有前開委託機構之認證標誌。
- 三、資通安全專職人員,指應全職執行資通安全業務者。
- 四、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。
- 五、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。
- 六、端點偵測及應變機制,指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或 異常活動行為分析及相關威脅程度呈現功能之防護作業。
- <u>七</u>、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。

- 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。
- 三、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 四、資通安全專職人員,指應全職執行資通安全業務者。
- 五、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。
- 六、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。

之規定,第五點,第五點,其修正,集修正,未修正,未修正。

# 第十一條附表二修正對照表

		修正規	定			現行規	定	說明
	, , , , ,	及A級之特定非公	務機關應辦事項			吸 A 級之特定非公	務機關應辦事項	一、考量危害
制度面向	辨理項目	辨理項目細項	辦理內容	制度面向	辨理項目	辨理項目細項	辦理內容	國家資通安全
	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, 並完成附 表十之控制措施; 其後應每年至少檢 視一次資通系統分級妥適性。		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,並完成附 表十之控制措施;其後應每年至少檢		資通系統分級	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 對通系統分級及防護基準 附表九完成資通系統分級,並完成附 表十之控制措施;其後應每年至少檢 視一次資通系統分級妥適性。		產品由主管機關核定 商 滿 與 益 有 限 , 後 續 將 由 主 管 機關透 過 跨 音
管理面 資訊安全管理系統之導入及通過公正第三方之驗證		• • •	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,於三年內完成公 正第三方驗證,並持續維持其驗證有 效性。		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,於三年內完成公 正第三方驗證,並持續維持其驗證有		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,於三年內完成公	會格數通限,面理使物機局。一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個
	資通安全專責	人員	初次受核定或等級變更後之一年內, 配置四人。	管理面			初次受核定或等級變更後之一年內, 配置四人。	資通安全產品 辦理項目之本
	內部資通安全	稽核	每年辦理二次。		內部資通安全稽核    每年辦理二次。		關規定,並用	
	業務持續運作	演練	全部核心資通系統每年辦理一次。		業務持續運作	<b>F演練</b>	全部核心資通系統每年辦理一次。	除現行備註三
	بعد ۱ ا ا ۱ ا م	弱點掃描	全部核心資通系統每年辦理二次。				一、除因業務需求且無其他替代方案	對危害國家資
	安全性檢測	渗透測試	全部核心資通系統每年辦理一次。				外,不得採購及使用主管機關核定	通安全產品之
技術面	<b>資通安全健</b>	網網機 使惡 同意 目 定 線 設 連 線 報 報 題 題 題 題 題 題 題 題 題 題 題 題 題 題 題 題 題	- 每年辦理一次。		限制使用危害品	害國家資通安全 <u>產</u>	之廠商生產、研發、製造或提供之 危害國家資通安全產品。 二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管 機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管 機關核可採購之危害國家資通安 全產品,應列冊管理,且不得與業 務網路環境介接。	說為測性辦名為通測應明使用,理稱完安管監測性辦名為通測應整全理控整。 整全理控整 人名英格勒 人名英格格 人名英格格 人名英格格 人名英格格 人名英格格 人名英格格 人名英格格克格格 人名英格格克格格 人名英格格克格格格格 人名英格格格格格格格格格格格格格格格格格格格格格格格格格格格格格格格格
	資通安全威脅	偵測管理機制	初次受核定或等級變更後之一年內, 完成威脅偵測機制建置,並持續維 運。其監控範圍應包括本表所定「資 通安全防護」之辦理內容、目錄服務 系統與機關核心資通系統之資通設備 紀錄及資訊服務或應用程式紀錄。	技術面	安全性檢測 資通安全健 診	網路 一	全部核心資通系統每年辦理二次。 全部核心資通系統每年辦理一次。 每年辦理一次。	爰 修 容明 量 弱 是 是 。 資 考 統 而 安 最 五 是 全 最 。 資 者 。 是 会 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。

	資通安全弱點通報機制		一、關鍵基礎設施提供者初次受核定 或等級變更後之一年內,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 於修正施行後一年內,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	防網具器子制入禦具之統用進脅施數防郵,件 負制對心,式持擊體將伺備濾 及 服通備火性無過 外資應防續防 外資應防續防 人 服通備火性禦	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。
	資通安全 教育訓練	資人 資人 資子 等人 資子 等人 。 等人 。 。 等人 。 。 。 。 。 。 。 。 。 。 。 。 。	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。 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。
認知與訓練	一般使用者及 主管 資通安全專業證照		每人每年接受三小時以上之資通安全 通識教育訓練。 一、初次受核定或等級變更後之一年 內,至少四名資通安全專責人 員,各自持有證照一張以上,並 持續維持證照之有效性。 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, 應於修正施行後一年內符合規 定。

		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	
	資通安全威力	脅偵測管理機制	初次受核定或等級變更後之一年內, 完成威脅偵測機制建置,並持續維 運。
	資通安全 防護	防網具器子制入禦具之統用進脅施數防郵,件 偵制對心,式持擊體人件應過 測 外資應防續防續防緩 及 服通備火性禦	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。
		資通安全專責 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。
認知與訓練	資通安全 教育訓練	資通安全專責 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	業證照	初次受核定或等級變更後之一年內,資 通安全專責人員總計應持有四張以上, 並持續維持證照之有效性。

全級設導弱(V以點技鍵供通報定定責之施入 NAP時術基者安機,明任關提資點S)時形面礎應全制並其等鍵供通通機掌,增設導弱制於定級基者安 制握爰訂施入點之備義A 礎宜全報,弱於關提資通規註。

- 五、有關責安持, 全有關資金,其一人。 
  東通照為張山,文確與 
  東通明,有 
  東通明,有 
  東京,有 
  東京,有 
  東京,有 
  東京,有 
  東京,有 
  東京。
- 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。
- 三、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政 府運作或社會安定之資通系統或資通服務。

## 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構<u>;</u> 第三方核發之驗證證書應有前開委託機構之認證標誌。
- 三、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業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。
- <u>五</u>、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。
- <u>六</u>、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。

- 四、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 五、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。

# 第十一條附表三修正對照表

修正規定			現行規定				說明	
附表三 資通安全責任等級 B 級之公務機關應辦事項 [				附表三 資通安全責任等級 B 級之公務機關應辦事項				
制度面向	辨理項目	辦理項目細項	辨理內容	制度面向	辨理項目	辦理項目細項	辦理內容 初次受核定或等級變更後之一年內,針	國家資通安 產品由主管
何及国内	資通系統分級	,	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,依附表力完成資通系統分級,並完成附表十之		資通系統分級	及防護基準	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,並完成附表十之 控制措施;其後應每年至少檢視一次資	關核定廠商單效益有門後續將由3
管理面	資訊安全管理系統之導入及通 過公正第三方之驗證 資通安全專責人員		控制措施;其後應每年至少檢視一次資通系統分級妥適性。 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,於三年內完成公正第三方驗證,並持續維持其驗證有效性。		資訊安全管理系統之導入及通 過公正第三方之驗證		通系統分級妥適性。 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,於三年內完成公正第三方驗證,並持續維持其驗證有效性。初次受核定或等級變更後之一年內,配	機會各推資之宜理使資關協機動通限,面用通資明關危安制爰有危安則爰有危安則
			初次受核定或等級變更後之一年內,配置二人;須以專職人員配置之。	管理面	資通安全專責 內部資通安全	稽核	置二人;須以專職人員配置之。	
	內部資通安全		每年辦理一次。		業務持續運作	演練	全部核心資通系統每二年辦理一次。	關規定,立
	業務持續運作	演練	全部核心資通系統每二年辦理一次。		資安治理成熟度評估		每年辦理一次。	除現行備記
	資安治理成熟	度評估	每年辦理一次。				一、除因業務需求且無其他替代方案	對危害國家
	安全性檢測	弱點掃描 渗透測試	全部核心資通系統每年辦理一次。 全部核心資通系統每二年辦理一次。				外,不得採購及使用主管機關核定 之廠商生產、研發、製造或提供之	通安全產品 説明。
技術面	<b>資通安全健</b>	網路架構檢視 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			限制使用危害國家資通安全產品		危害國家資通安全產品。 二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管機關核可採購之危害國家資通安 全產品,應列冊管理,且不得與公務網路環境介接。	二、為別性辦名為通測應於安詞修目 規威機範則 應於 無 類 整 全 理 控 號 經 報 養 餐 監 經 報 數 養 報 數 養 報 數 養 報 數 看 數 看 看 看 看 看 看 看 看 看 看 看 看 看 看 看 看
資通安全威脅		定及防火牆連 線設定檢視 偵測管理機制	初次受核定或等級變更後之一年內,完成威脅偵測機制建置,並持續維運及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點 值測及應變機制」與「資通安全防護」 之辦理內容、目錄服務系統與機關核心	技術面	安全性檢測資通安全健診	網站安全弱點 檢測 系統渗透測試 網路架構檢視 網路 網路 機用者 競用者 電腦 發見 一個 一個 一個 一個 一個 一個 一個 一個 一個 一個 一個 一個 一個	全部核心資通系統每年辦理一次。 全部核心資通系統每二年辦理一次。 每二年辦理一次。	爰內資者 一 一 一 一 一 一 一 一 一 一 一 一 一

			資通系統之資通設備紀錄及資訊服務
			或應用程式紀錄。
			初次受核定或等級變更後之一年內,依
	政府組態基	準	主管機關公告之項目,完成政府組態基
			準導入作業,並持續維運。
			一、初次受核定或等級變更後之一年
			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
			—————————————————————————————————————
	資通安全弱	點通報機制	二、本辦法中華民國一百十年八月二
			—————————————————————————————————————
			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。
			內,完成端點偵測及應變機制導入
			作業,並持續維運及依主管機關指
			定之方式提交偵測資料。
			二、本辦法中華民國一百十年八月二
	端點偵測及	應變機制	十三日修正施行前已受核定者,應
			於修正施行後二年內,完成端點偵
			測及應變機制導入作業,並持續維
			運及依主管機關指定之方式提交
			值測資料。
		防毒軟體	N/A X (1)
		網路防火牆	-
		具有郵件伺服器	
		者,應備電子郵	
		件過濾機制	初次受核定或等級變更後之一年內,完
	資通安全	入侵偵測及防禦	成各項資通安全防護措施之啟用,並持
	防護	機制	續使用及適時進行軟、硬體之必要更新
		具有對外服務之	或升級。
		核心資通系統	
		者,應備應用程	
		バル 八個	<b>————————————————————————————————————</b>
		資通安全專職人	強火母十五ノ役又   一小門以上之員
認知	四 資通安全		一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
與訓練	教育訓練	資通安全專職人	אןיש יין אן אר
六明外	7人月 训练	員以外之資訊人	每人每二年至少接受三小時以上之資
		貝以外之貝 訊入   員	通安全專業課程訓練或資通安全職能
		只	

		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				
		•	初次受核定或等級變更後之一年內,完			
	次区户入土。	3. 14 四 14 H.I	成威脅偵測機制建置,並持續維運及依			
	貝迪女主威尔	脅偵測管理機制	主管機關指定之方式提交監控管理資			
			料。			
			初次受核定或等級變更後之一年內,依			
	政府組態基準	<b>集</b>	主管機關公告之項目,完成政府組態基			
			準導入作業,並持續維運。			
		防毒軟體				
		網路防火牆				
		具有郵件伺服器				
		者,應備電子郵	初为巫坛宁老笠加磁西从上,左中一			
	次另中入	件過濾機制	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			
	資通安全 防護	入侵偵測及防禦				
	沙 碊	機制	· 或升級。			
		具有對外服務之	3. 月 · 0. ·			
		核心資通系統				
		者,應備應用程				
		式防火牆				
		資通安全專職人	每人每年至少接受十二小時以上之資			
		員過女主守順八	通安全專業課程訓練或資通安全職能			
		只	訓練。			
	資通安全	資通安全專職人	每人每二年至少接受三小時以上之資			
	教育訓練	員以外之資訊人	通安全專業課程訓練或資通安全職能			
	3人 月 m/m		訓練,且每年接受三小時以上之資通安			
認知		Х	全通識教育訓練。			
與訓練		一般使用者及主	每人每年接受三小時以上之資通安全			
31 84616		管	通識教育訓練。			
		資通安全專業證	初次受核定或等級變更後之一年內,資			
	資通安全專	照	通安全專職人員總計應持有二張以上,			
	業證照及職	<u> </u>	並持續維持證照之有效性。			
	能訓練證書	資通安全職能評	初次受核定或等級變更後之一年內,資			
	70 - 101-00	量證書	通安全專職人員總計應持有二張以上,			
		<u> </u>	並持續維持證書之有效性。			
備註:						

#### 借註:

- 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。

- 全級宜全(V以點技通報定定責之導弱NS)時形面全制於其納人以點機通過制於定級機通過制經差計點之備義與機通過制安報,弱於資通規註。
- 五、考量資通安全 威脅日趨多 樣,為提升資 通安全責任等 級B級之公務 機關主動式偵 測、漏洞防護、 行為分析與回 應之能力,宜 導入端點安全 防護作業,爰 於技術面增訂 端點偵測及應 變機制之規 定,並於備註 定明其定義。 六、有關資通安全
- 不專通照職之每以相資 人全資訓有持,文確 員專通練,有爰字。 就業安證應一修, 文就業安證應一修,
- 七、現行備註欄第 二點增訂第三 方核發之驗證 證書認證標誌 之規定,第四

			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	每人每年接受三小時以上之資通安全
		管	通識教育訓練。
			一、初次受核定或等級變更後之一年
			內, <u>至少二名</u> 資通安全專職人員 <u>,</u>
次	にはか入苗州	Y	分別各自持有證照及證書各一張
		<b><i><b>*</b> </i></b>	以上,並持續維持證照及證書之有
	證書		效性。
			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
			於修正施行後一年內符合規定。

## 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構<u>;</u> 第三方核發之驗證證書應有前開委託機構之認證標誌。
- 三、資通安全專職人員,指應全職執行資通安全業務者。
- 四、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。
- 五、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。
- 六、端點偵測及應變機制,指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或 異常活動行為分析及相關威脅程度呈現功能之防護作業。
- <u>七</u>、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。

- 三、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 四、資通安全專職人員,指應全職執行資通安全業務者。
- 五、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。
- 六、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。

點、第五點及 第六點點次酌 作修正,其餘 各項目未修 正。

# 第十一條附表四修正對照表

修正規定					現行規	定	說明	
		B級之特定非公務		附表四 資道	通安全責任等級	B級之特定非公務	5機關應辦事項	一、考量
制度面向	辦理項目	辨理項目細項	辦理內容	制度面向	辨理項目	辨理項目細項	辦理內容	危害國家資通
	資通系統分級	初次受核定或等級變更後之一年 對自行或委外開發之資通系統, 資通系統分級及防護基準 九完成資通系統分級,並完成附 控制措施;其後應每年至少檢視 通系統分級妥適性。			資通系統分級及防護基準 資訊安全管理系統之導入及通 過公正第三方之驗證		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,並完成附表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。	安全產品 核單
管理面	資訊安全管理系統之導入及通過公正第三方之驗證		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,於三年內完成公正第三方驗證,並持續維持其驗證有效性。				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,於三年內完成公正第三方驗證,並持續維持其驗證有效性。	臺與推關 國國 選 與
	資通安全專責	人員	初次受核定或等級變更後之一年內,配置二人。	tt	資通安全專責	人員	初次受核定或等級變更後之一年內,配置二人。	限制使用危害國家資通安全
	内部資通安全	稽核	每年辦理一次。	管理面	內部資通安全	· 稽核	每年辦理一次。	產品辦理項目
	業務持續運作	演練	全部核心資通系統每二年辦理一次。		業務持續運作演練		全部核心資通系統每二年辦理一次。	之相關規定, 並刪除現行備
	安全性檢測	弱點掃描	全部核心資通系統每年辦理一次。				一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定	註三對危害國
技術面	資通安全健診	<u>參透</u> 網網檢 網機 網 機 題 網 機 題 者 動 主 。 器 動 員 形 活 器 動 員 的 防 院 大 長 人 股 、 股 、 股 、 股 、 股 、 股 、 股 、 股 、 股 、 股	全部核心資通系統每二年辦理一次。 每二年辦理一次。		<u>限制使用危害國家資通安全產</u> <u>品</u>		之廠商生產、研發、製造或提供之 危害國家資通安全產品。 二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管 機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管 機關核可採購之危害國家資通安 全產品,應列冊管理,且不得與業 務網路環境介接。	家品 性致其項為通測應資之 檢性辦名完安管題為測,理稱整全理控安明使用爰項。規威機範空明使用爰項。規威機範控
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內,完成威脅偵測機制建置,並持續維運。其 監控範圍應包括本表所定「資通安全防 護」之辦理內容、目錄服務系統與機關 核心資通系統之資通設備紀錄及資訊 服務或應用程式紀錄。	技術面	安全性檢測資通安全健診	網站安全弱點檢測系統滲透測試網路架構檢視網路惡意活動檢視 使用者端電腦	全部核心資通系統每年辦理一次。 全部核心資通系統每二年辦理一次。 每二年辦理一次。	爰修正其辨理 內資明確。 內資明國 內資量因 內資量 內 內 內 內 內 內 內 內 內 內 內 內 內 內 內 內 內 內
	資通安全弱點通報機制		一、 <u>關鍵基礎設施提供者初次受核定</u> 或等級變更後之一年內,完成資通			· 展高活動檢視		安全威脅日趨 嚴重,資通安

	1		
			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是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,應於修正施行後一年內,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 網方數學 與有應機制 與有應機制 與人 機制 與人 機制 對 資 的 數 的 數 的 數 的 數 的 數 的 。 應 機 制 的 的 的 的 的 的 的 的 的 的 的 的 的 的 的 的 的 的	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。
	資通安全 教育訓練	資通安全專責人 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。
		資通安全專責人 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。
認知與訓練		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	一、初次受核定或等級變更後之一年 內,至少二名資通安全專責人員 <u>,</u> 各自持有證照一張以上,並持續維 持證照之有效性。 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 於修正施行後一年內符合規定。

### 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構<u>;</u> 第三方核發之驗證證書應有前開委託機構之認證標誌。
- 三、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。

		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	
	次冯卢入士。	多占测盆珊城剧	初次受核定或等級變更後之一年內,完
	貝迪女生威尔	脅偵測管理機制	成威脅偵測機制建置,並持續維運。
		防毒軟體	
		網路防火牆	
		具有郵件伺服器	
		者,應備電子郵	   初次受核定或等級變更後之一年內,完
	資通安全	件過濾機制	成各項資通安全防護措施之啟用,並持
	<b>  財政</b> 安全	入侵偵測及防禦	放谷項貝迪女主的設備地之成而,並行
		機制	· 頭仗用及過时延行款· 峽腦之必安文制 · 或升級。
		具有對外服務之	
		核心資通系統	
		者,應備應用程	
		式防火牆	
		資通安全專責人	每人每年至少接受十二小時以上之資
		貝迦女王守貝八	通安全專業課程訓練或資通安全職能
		Х	訓練。
	資通安全	資通安全專責人	每人每二年至少接受三小時以上之資
	教育訓練	員以外之資訊人	通安全專業課程訓練或資通安全職能
認知	32,7 5 101	月 月	訓練,且每年接受三小時以上之資通安
與訓練			全通識教育訓練。
		一般使用者及主	每人每年接受三小時以上之資通安全
		管	通識教育訓練。
		ate.	初次受核定或等級變更後之一年內,資
	資通安全專業	業證照	通安全專責人員總計應持有二張以上,
			並持續維持證照之有效性。
<b>借註:</b>			

#### 借註

- 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。
- 三、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 四、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 五、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- 六、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。

全級設導弱(V以點技鍵供通報定定責之施入 NS的時形面礎應全制並其等鍵供通通機掌,增設導弱制於定級基者安 制握塞;增設導弱制於定級基者安 制握爱訂施入點之備義B礎宜全報,弱於關提資通規註。

- 五、有專通照為 持兵 实就業,有爰字之每以相關 以相 , 文確 。 以相 資 。

- 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。
- <u>六</u>、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。

# 第十一條附表五修正對照表

修正規定				現行規定				
附表五 資主制度面向	通安全責任等級辦理項目	C 級之公務機關應 辦理項目細項	辨事項辦理內容	附表五 資通	鱼安全責任等級	C級之公務機關應	辦事項	一、 考量 危害國家資道
門及画門	州华项日	州 生 切 日 加 功	初次受核定或等級變更後之一年內,針	制度面向	辨理項目	辦理項目細項	辦理內容	安全產品由主
	資通系統分級及防護基準		初天交核足或等級愛更後之一平內, 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,完成以表十之批制共統。	管機關核定顧 商清單效益有 限,後續將由 主管機關透過 跨部會協調平
管理面			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。		資訊安全管理	成附表十之控制措施。 初次受核定或等級變更後之二年內,部核心資通系統導入 CNS 27001 或 IS 27001 等資訊安全管理系統標準、其何 具有同等或以上效果之系統或標準,其他公務機關自行發展並經主管機 認可之標準,並持續維持導入。		臺與各機關海 國家 是 國家 是 明
	資通安全專責		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。		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。	限制使用危害國家資通安全
	內部資通安全	稽核	每二年辦理一次。	管理面	內部資通安全稽核		每二年辦理一次。	產品辨理項目
	業務持續運作	演練	全部核心資通系統每二年辦理一次。		業務持續運作演練		全部核心資通系統每二年辦理一次。	之相關規定, 並刪除現行係
	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。 全部核心資通系統每二年辦理一次。				一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定	註二對危害國家資通安全產
技術面	資通安全健診	<u>參透</u> 網網檢 網 機 題 網 題 題 題 題 者 動 主 題 題 題 題 題 題 題 題 題 題 題 題 題 題 題 題 題 題	全部核心員		限制使用危害	<b>等國家資通安全產</b>	之廠商生產、研發、製造或提供之 危害國家資通安全產品。 二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管 機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管 機關核可採購之危害國家資通安 全產品,應列冊管理,且不得與公 務網路環境介接。	品為則性辨名考統而安則全詞修目 資本之數 明 後 明 後 明 多 項 。 因 點 生 威 要 看 新產 全 歲 而 安 全 歲 而 安 全 歲 元
	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	技術面	安全性檢測資通安全健診	網站安全弱點檢測 系統滲透測試 網路際標檢視 網路惡 競視 使用者端電腦	全部核心資通系統每二年辦理一次。 全部核心資通系統每二年辦理一次。 每二年辦理一次。	嚴重,資額 全責任務機 宜導及資 宜等 以 以 以 即 時 對 以 以 以 以 以 以 以 以 以 以 以 以 以 以 以 以 以 以
			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			惡意活動檢視		點情形,爰

		I h M au	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 網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制	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。
		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 教育訓練	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。
認知與訓練		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。
與訓練	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。
- <u>五</u>、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。

		,	
		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	
		防毒軟體	和力妥拉宁七笙加缕百级之 生由,宁
	次区户入	網路防火牆	初次受核定或等級變更後之一年內,完
	資通安全	具有郵件伺服	成各項資通安全防護措施之啟用,並持
	防護	器者,應備電子	續使用及適時進行軟、硬體之必要更新
		郵件過濾機制	或升級。
		次记中入市叫	每人每年至少接受十二小時以上之資
		資通安全專職	通安全專業課程訓練或資通安全職能
		人員	訓練。
		<b>容温 0 入 亩 11</b>	每人每二年至少接受三小時以上之資
	資通安全	資通安全專職 人員以外之資	通安全專業課程訓練或資通安全職能
	教育訓練		訓練,且每年接受三小時以上之資通安
認知		訊人員	全通識教育訓練。
與訓練		一般使用者及	每人每年接受三小時以上之資通安全
		主管	通識教育訓練。
		資通安全專業	資通安全專職人員總計應持有一張以
	資通安全專	證照	上,並持續維持證照之有效性。
	業證照及職	次另中入聯业	初次受核定或等級變更後之一年內,資
	能訓練證書	資通安全職能	通安全專職人員總計應持有一張以上,
		評量證書	並持續維持證書之有效性。
<b>进</b> :			

## 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、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政 府運作或社會安定之資通系統或資通服務。
- 三、資通安全專職人員,指應全職執行資通安全業務者。
- 四、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。
- 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。

- 技術面增訂資 通報 機 並 於 備 並 於 備 註 定 明 其 定 義
- 四有關職之每以相資資人全資證定,有關職之每以能持人上關明資人主關納,有爰字。確議,有爰字。
- 五、現行備註欄第 三點及第四點 點次酌作修 正,其餘各項 目未修正。

# 第十一條附表六修正對照表

修正規定				現行規定				說明	
		C級之特定非公務		附表六 資通	鱼安全责任等級	C級之特定非公務	5機關應辦事項	<b>一、</b>	考量危害
制度面向	辨理項目	辨理項目細項	辨理內容	制度面向	辨理項目	辨理項目細項	辦理內容		家資通安全
	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	關單後機會	品核益網透調的一個人類的人類的人類的人類的人類的人類的人類的人類的人類的人類的人類的人類的人類的人
管理面			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。		資訊安全管理	成附表十之控制措施。 初次受核定或等級變更後之二年的 部核心資通系統導入 CNS 27001 27001 等資訊安全管理系統之導入 具有同等或以上效果之系統或標準 其他公務機關自行發展並經主管		推資之宜理	機動通限,面內機關危安制幾有的人物,不是一個人物,不可以不可以不可以不可以不可以不可以不可以不可以不可以不可以不可以不可以不可以不
	資通安全專責		初次受核定或等級變更後之一年內,配置一人。		資通安全專責人員		認可之標準,並持續維持導入。 初次受核定或等級變更後之一年內,配 置一人。	資	用危害國家通安全產品
	內部資通安全	稽核	每二年辦理一次。	管理面	內部資通安全稽核		每二年辦理一次。		詳理項目之相 14日 - 共同
	業務持續運作	演練	全部核心資通系統每二年辦理一次。		業務持續運作演練		全部核心資通系統每二年辦理一次。	除	規定,並刪 :現行備註二
	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。		限制使用危害國家資通安全產品		一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定	通說為測性辦名考統而安明使用,理稱量弱產全。安言爰琈。 医黑生	危害國家資  安全產品之
技術面	資通安全健診	<u>渗透料</u> 網機機 網機 機 機 機 機	全部核心資通系統每二年辦理一次。 每二年辦理一次。				之廠商生產、研發、製造或提供之 危害國家資通安全產品。 二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管 機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管 機關核可採購之危害國家資通安 全產品,應列冊管理,且不得與業 務網路環境介接。		明使用,理稱量弱產全。安詞修目 資本之數條目 資未之齊性一正細 通修資日
	資通安全弱點通報機制		一、關鍵基礎設施提供者初次受核定 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	技術面	安全性檢測 資通安全健 診	網站安全弱點檢測 系統滲透測試 網路架構檢視 網路 惡意活動檢視 使用者端電腦 惡意活動檢視	全部核心資通系統每二年辦理一次。 全部核心資通系統每二年辦理一次。 每二年辦理一次。	全級設導弱(V	重責關鍵 大海 大 大 大 大 大 大 大 大 大 大 大 大 大 大 大 大 大 大

			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 網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制	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。
	資通安全 教育訓練	資通安全專責 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。
認知與訓練		資通安全專責 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		初次受核定或等級變更後之一年內, <u>至</u> 少一名資通安全專責人員持有 <u>證照</u> 一 張以上,並持續維持證照之有效性。

## 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、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 三、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。
- 四、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。
- 五、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。

		伺服器主機惡 意活動檢視 目錄伺服器設 定及防火牆連	
	資通安全 防護	線設定檢視 防毒軟體 網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制	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。
認知與訓練	資通安全 教育訓練	資通安全專責 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。
		資通安全專責 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		初次受核定或等級變更後之一年內,資 通安全專責人員總計應持有一張以上, 並持續維持證照之有效性。

#### 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、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 三、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 四、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- 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。

- 點技鍵供通報定院形面礎應到機並與所述與導弱之情並與場別之情義於關提資通規註。
- 四、有專通照為張正以育員員專有持人上關明資人全持人上關明資,以相資明確。
- 五、現行備註欄第 三點、 及第五點 。 配作修正 。 餘各項目未修 正。

# 第十一條附表七修正對照表

			3, 1	1	<b>沙亚</b> 式,			Γ	
修正規定					現行規定				
附表七 資主	通安全責任等?	級D級之各機關應熟	辛事項	附表七 資道	一、 考量危害				
制度面向	辨理項目	辨理項目細項	辨理內容	制度面向	辨理項目	辨理項目細項	辨理內容	國家資通安全	
技術面	資通安全 防護	防毒軟體 網路防火牆	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。				一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定 之廠商生產、研發、製造或提供之 危害國家資通安全產品。	產品由主管核關核定廠商污 關核定廠商污 單效益有限, 後續將由主管	
認知與訓練	資通安全 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。	管理面		害國家資通安全產	二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管	機關透過跨部 會協調平臺與各機關溝通,	
			議關得視實際需求,於符合本辦法規定之 關之資通安全應辦事項。		<u>aa</u>		機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管 機關核可採購之危害國家資通安 全產品,應列冊管理,且不得與公 務(業務)網路環境介接。	推動危害國家 資通安全產品 之限制使用等 宜,爰關限管 理面有關限制	
				技術面	資通安全 防護	防毒軟體 網路防火牆 具有郵件伺服器 者,應備電子郵 件過濾機制	· 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。	使用危害国家	
				認知與訓練	資通安全 教育訓練	一般使用者及主	每人每年接受三小時以上之資通安全 通識教育訓練。	對危害國家資 通安全產品之	
				內,另往	<b>行訂定其所管</b>	持定非公務機關之資	得視實際需求,於符合本辦法規定之範圍 通安全應辦事項。 全具有直接或間接造成危害風險,影響政	說明。 二、配合第六條修 正後包含維達 具帳號權限管	
						资通系統或資通服務		理功能之資道 系統之情形, 其資通安全責 任等級為(	
								級,本表所定 技術面之資達 安全防護中	
								「具有郵件信服器者」,係屬	
								維運具帳號構限管理功能之資通系統之情形,其資通安	

	第六條規定應 為 C 級,爰刪 除該辦理項目 細項之規定。

# 第十一條附表八修正對照表

		修正規	定			現行規	定	說明
附表八 資通安全責任等級 E 級之各機關應辦事項			附表八 資通安全責任等級 E 級之各機關應辦事項				考量危害國家資通	
制度面向	辨理項目	辨理項目細項	辨理內容	制度面向	辨理項目	辦理項目細項	辦理內容	安全產品由主管機
認知	資通安全	一般使用者及主	每人每年接受三小時以上之資通安全				一、除因業務需求且無其他替代方案	關核定廠商清單效
與訓練	教育訓練	管	通識教育訓練。				外,不得採購及使用主管機關核定	益有限,後續將由
備註:特定非	· 卡公務機關之中	· 中目的事業主管機	關得視實際需求,於符合本辦法規定之				之廠商生產、研發、製造或提供之	主管機關透過跨部
			關之資通安全應辦事項。				危害國家資通安全產品。	會協調平臺與各機
7024	, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	(77 B IN 7C) T CANAL					二、必須採購或使用危害國家資通安全	關溝通,推動危害
				    管理面	限制使用危	害國家資通安全產	產品時,應具體敘明理由,經主管	國家資通安全產品
					<u> </u>		機關核可後,以專案方式購置。	之限制使用事宜,
							三、對本辦法修正施行前已使用或因業	爰刪除管理面有關
							務需求且無其他替代方案經主管	限制使用危害國家
							機關核可採購之危害國家資通安	資通安全產品辦理
							全產品,應列冊管理,且不得與公	項目之相關規定,
							務(業務)網路環境介接。	並刪除現行備註二
				認知	資通安全	一般使用者及主	每人每年接受三小時以上之資通安全	對危害國家資通安
				與訓練	教育訓練	管	通識教育訓練。	全產品之說明。
				備註:				
				一、特定非公	·務機關之中央	:目的事業主管機關	得視實際需求,於符合本辦法規定之範圍	
				內,另行	<b>亍訂定其所管</b> 特	<b>寺定非公務機關之</b> 資	<b>予通安全應辦事項。</b>	
				二、危害國家	<b>飞資通安全產品</b>	L,指對國家資通安	全具有直接或間接造成危害風險,影響政	
				府運作或	<b>戊社會安定之</b> 資	货通系統或資通服務	<u>Ç o</u>	

# 第十一條附表十修正對照表

修正規定 附表十 資通系統防護基準					現行規定				說明	
					附表十 貧	附表十 資通系統防護基準				
系統 控制措施 構面	防護需求 分級 措施內 容	高	中	普	条統 控制措施 構面	防護需求 分級 措施內 容	市同	中	普	(一)有關帳號管之高級控制。 施 關 報 明 强 明 强 民 明 强 民 开 明 强 民 开 开 开 开 开 开 开 开 开 开 开 开 开 开 开 开 开 开
存制	· · · · · · · · · · · · · · · · · · ·	一、機統或與使件逾之可系使應情用監號違報等機統或與使件逾之可系使應情用監號違報等度置用系況 所時限自出規件統系通發用者中提義時期統及 許間時動。定,。統帳時之,指於國際人。統帳時之。	一、二、三、四、白、白、白、白、白、白、白、白、白、白、白、白、白、白、白、白、白、白	建立帳號管理機制, 包含帳號之申請、建 立、修改、啟用 用及刪除之程序。	存取控	· · · · · · · · · · · · · · · · · · ·	情用監號違管等控權人, 。統帳回之。, 傳紹新聞資如使者「措限為指於實理級制權人,應所不可,所以對於一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	緊除資號定統修用等有 在機長之端密縣。所為禁審號、刪「持關權之政際,所以,所以,所以,所以,所以,所以,所以,所以,所以,所以,所以,則以,以,以,以,	包含帳號之申請、開 之 傳用及刪除之程	生義關統或與使件類制限址及等措作並點合定點適,應之可資用,型、制、存。施文與至前遞至用爰定閒使通情例與操、連取現第字現第開移第上增義置用系況如功作來線取行一修行四增為五之訂各時期統及帳能時源數資控點正第點訂第點
	最小權限	採最小權限原則,僅	應為機關已預先定義	無要求。 <u>一、</u> 對於每一種允許 之遠端存取類		遠端存取	三、 <u>資通系統</u> 遠端存 預先定義及管理 四、等級「普」之所	之存取控制點。	先取得授權,建立使 用限制、組態需求、 連線需求及文件化, 使用者之權限檢查 作業應於伺服器端 完成。	(二)帳號管理之級及普級控措施規定的文字修正。 (三)有關京,因
	遠端存取	<u>二</u> 、等級「普」之所	有控制措施。	型,均應先取得授權,建立使用限制、組態需求人主線需求及文件化。 二、使用者之權限檢查作業應於伺	稽核與 可歸 性	稽核事件	一、應定期審查稽核 二、等級「普」之所		一、依規定時間週期 及紀錄留稽核紀 策,保留稽核紀 錄。 二、確保資通系統有 稽核特定事件之 功能,並決定應	之 實務 是 與 是 與 是 我 我 是 我 我 是 我 我 是 我 是 我 是 我 是

			服器端完成。
			三、應監控遠端存取
			機關內部網段
			或資通系統後
			臺之連線。
			四、應採用加密機
			<u>制。</u>
		一、應定期審查機關所保留資通系統產生	一、訂定日誌之記錄
		<u>之日誌</u> 。	時間週期及留存
		二、等級「普」之所有控制措施。	政策, <u>並</u> 保留 <u>日</u>
			<u>誌至少六個月</u> 。
			二、確保資通系統有
	記錄事		記錄特定事件之
	件		功能,並決定應
			記錄之特定資通
			系統事件。
			三、應 <u>記錄</u> 資通系統
			管理者帳號所執
			行之各項功能。
	日誌紀	資通系統產生之 <u>日誌</u> 應包含事件類型、發生	
	録內容	何與事件相關之使用者身分識別等資訊,採	
	- 姚门 <del>台</del>	保輸出格式之一致性,並應依資通安全政	策及法規要求納入其
		他相關資訊。	
事件日	日誌儲	依據日誌儲存需求,配置所需之儲存容量	0
<u>誌</u> 與可	存容量		
歸責性		一、機關規定需要即 資通系統於日誌處理	失效時,應採取適當
		時通報之日誌 之行動。	
		處理失效事件	
	- \1 E	發生時,資通系	
	日誌處	<b>統應於機關規</b>	
	理失效	定之時效內,對	
	之回應	特定人員提出	
		警告。	
		二、等級「中」及「普」	
		之所有控制措	
		施。	次记名从亦从四方
		一、系統內部時鐘應 <u>定期</u> 與基準時間源進	資通系統應使用系
	1 ま 羽し コ	行同步。	統內部時鐘產生日
	時戳及	二、等級「普」之所有控制措施。	<u>誌</u> 所需時戳,並可以
	校時		對應到世界協調時
			間(UTC)或格林威
			治標準時間(GMT)。

	稽核紀錄內容	一、資通系統產生之稽核紀錄,應依需求 納入其他相關資訊。 二、等級「普」之所有控制措施。	稽統籍理之系統教生件分用制定。通統執。 稽件發事身採機之事務就是是問題等日期別一生會間與者並發及之資誌出關等日賴的主人,與者也與者的一個,與者也與者,與者的一個,與者的一個,與者的一個,與者的一個,與
	稽核儲	依據稽核紀錄儲存需求,配置稽核紀錄所寫	一致性。 雲之儲存容量。
	存容量		
	稽核處 理失效 之回應	一、機關規定需要即 時通報之稽核失 效事件發生時, 資通系統於稽核處理 之行動。 之行動。 發達所 , 資通系統應於機 關規定之時效 內,對特定人員 提出警告。 二、等級「中」及「普」 之所有控制措 施。	失效時,應採取適當
	時戳及 校時	一、系統內部時鐘應依機關規定之時間週 期與基準時間源進行同步。 二、等級「普」之所有控制措施。	資通系統應使用系統應使用系統內部時鐘產生稽核紀錄所需時戳,並可以對應到世界協調時間(UTC)或格關治標準時間(GMT)。
	稽核資訊之保	一、定期備份稽核紀 錄至與原稽核 系統不同之實 體系統。 二、等級「中」之所 有控制措施。	對稽核紀錄之存取 管理,僅限於有權限 之使用者。
運持計畫	系統備 份	一、應將備份還原, 作為營運持續 計畫測試之一 部分。	一、訂定系統可容忍 資料損失之時 間要求。

施第並類部系行控點正點點定之四定型網統高制酌,遞及。第點明為段後級措作並移第三規監機或臺及施文與為二點定控關資。中第字第第點及,之內通現級三修四一規及,之內通現級三修四一規

- 二、稽核與可歸責 性構面:
- (二) 之施應記及並少級措定正於普,訂錄留保六及施酌。 於難,訂錄留保六及施酌。 於實明日間政日月級一文 時存留個中第作

營續

		一、定期備份日誌至	一、應運用雜湊或其	對 <u>日誌</u> 之存取管理,
	日誌資	原系統外之其	他適當方式之	僅限於有權限之使
	<u> </u>	<u>他</u> 實體系統。	完整性確保機	用者。
	訊之保	二、等級「中」之所	制。	
	護	有控制措施。	二、等級「普」之所	
			有控制措施。	
		一、應將備份還原,	一、應定期測試備份	一、訂定系統可容忍
		作為營運持續	資訊,以驗證備	資料損失之時
		計畫測試之一	份媒體之可靠	間要求。
		部分。	性及資訊之完	二、執行系統源碼與
		二、應在與運作系統	整性。	資料備份。
	A 11 114	不同地點之獨	二、等級「普」之所	
	系統備	立設施或防火	有控制措施。	
	份	櫃中,儲存重要	7 .=	
營運持		資通系統軟體		
續計畫		與其他安全相		
/ / _		關資訊之備份。		
		三、等級「中」之所		
		有控制措施。		
		• • • • • • • • • • • • • • • • • • • •	中斷後至重新恢復服	無要求。
		務之可容忍時間		, ,
	系統備 援	二、原服務中斷時,		
			2方式取代並提供服	
		務。	<u> </u>	
		一、對資通系統之存	資通系統應具備唯一	識別及鑑別機關使用
	內部使	取採取多重認		者行為之程序)之功
	用者之	證技術。	能,禁止使用共用帳	號。
	識別與	二、等級「中」及「普」		
	鑑別	之所有控制措		
	•	施。		
		一、身分驗證機制應	防範自動化程式之登	一、使用預設密碼登
		入或密碼更換嘗	試。	入系統時,應於
म्मे गा क्ष		二、密碼重設機制對	使用者重新身分確認	登入後要求立
識別與		後,發送一次性	及具有時效性符記。	即變更。
鑑別		三、等級「普」之所	有控制措施。	二、身分驗證相關資
	4 2 54	_		訊不以明文傳
	身分驗			輸。
	證管理			三、具備帳戶鎖定機
				制,帳號登入進
				行身分驗證失
				敗達五次後,至
				少十五分鐘內
				不允許該帳號
	<u> </u>			,

		二、應在與運作系統		二、執行系統源碼與
		不同處之獨立	整性。	資料備份。
			二、等級「普」之所	
		中,儲存重要資	有控制措施。	
		通系統軟體與		
		其他安全相關		
		資訊之備份。		
		三、等級「中」之所		
		有控制措施。		
		一、訂定資通系統從	中斷後至重新恢復服	無要求。
	系統備	務之可容忍時間	要求。	
	援	二、原服務中斷時,	於可容忍時間內,由	
		備援設備取代提	供服務。	
		一、對帳號之網路或	資通系統應具備唯一	識別及鑑別機關使用
	內部使	本機存取採取多	者(或代表機關使用	者行為之程序)之功
	用者之	重認證技術。	能,禁止使用共用帳	號。
	識別與	二、等級「中」及「普」		
	鑑別	之所有控制措		
		施。		
		一、身分驗證機制應	防範自動化程式之登	一、使用預設密碼登
		入或密碼更換當		入系統時,應於
			使用者重新身分確認	登入後要求立
			及具有時效性符記。	即變更。
		三、等級「普」之所		二、身分驗證相關資
			71 12 11 11 10	訊不以明文傳
				輸。
				三、具備帳戶鎖定機
識別與				制,帳號登入進
鑑別				行身分驗證失
				<b>り</b> 対 が 破
	身分驗			少十五分鐘內
	證管理			不允許該帳號
				繼續嘗試登入
				越傾 昌 田 登 八 一 或 使 用 機 關 自
				或使用機關目 建之失敗驗證
				•
				機制。
				四、基於密碼之鑑別
				資通系統應強
				制最低密碼複
				雜度;強制密碼
				最短及最長之
				效期限制。

- 爰修正為「資 通安全政策及 法規要求」,以 資明確。
- (四) 之控點免未間用義規規期期時高制規實規週上,定定於及及施,上相,產將依時為校中第為機關致生現機間「之正縣」,與關係與與於,是相,與與於於,與與於於,是,與於於,與與於於,與於於,與與於於,與於於
- 三、營運持續計畫 構面:
- (一)系統備份之高 級控制措施第 二點規定酌作 文字修正。
- 四、識別與鑑別構

			繼續嘗試登入
			或使用機關自
			建之失敗驗證
			機制。
			四、使用密碼進行驗
			<u>證時,</u> 應強制最
			低密碼複雜度;
			強制密碼最短
			及最長之效期
			限制。
			五、密碼變更時,至
			少不可以與前
			三次使用過之
			密碼相同。
			六、第四點及第五點
			所定措施,對非
			內部使用者,可
			依機關自行規
			範辦理。
	鑑別資	資通系統應遮蔽鑑別過程中之資訊。	
	訊回饋		
	加密模	資通系統如以密碼進行鑑別時,該密碼應	無要求。
	組鑑別	加密或經雜湊處理後儲存。	
	非內部	資通系統應識別及鑑別非機關使用者(或代	表機關使用者行為之
	使用者	程序)。	
	之識別		
	與鑑別		
	系統發	針對系統安全需求(含機密性、可用性、完	完整性)進行確認。
	展生命		
	週期需		
	求階段		
	系統發	一、根據系統功能與要求,識別可能影響	無要求。
	展生命	系統之威脅,進行風險分析及評 	
系統與	週期設	估。	
服務獲	計階段	二、將風險評估結果回饋需求階段之檢核	
得		項目,並提出安全需求修正。	ر الماري
-		一、執行「源碼掃描」一、應針對安全需求	
	系統發	安全檢測。 二、應注意避免軟體	吊見漏洞及貫作必要
	展生命	二、系統應具備發生 控制措施。	田七万二世町二然仁
	週期開	嚴重錯誤時之 三、發生錯誤時,使	
	發階段		,不包含詳細之錯
		三、等級「中」及「普」 誤訊息。	
		之所有控制措	

		工 从四九五边应证
		五、使用者更換密碼
		時,至少不可以
		與前三次使用
		過之密碼相同。
		六、第四點及第五點
		所定措施,對非
		內部使用者,可
		依機關自行規
		範辦理。
	鑑別資	資通系統應遮蔽鑑別過程中之資訊。
	訊回饋	
	加密模	資通系統如以密碼進行鑑別時,該密碼應 無要求。
	組鑑別	加密或經雜湊處理後儲存。
	非內部	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之
	使用者	程序)。
	之識別	
	與鑑別	
	系統發	針對系統安全需求(含機密性、可用性、完整性),以檢核表方
	展生命	式進行確認。
	週期需	
	求階段	
	系統發	一、根據系統功能與要求,識別可能影響 無要求。
	展生命	系統之威脅,進行風險分析及評估。
	週期設	二、將風險評估結果回饋需求階段之檢核
	計階段	項目,並提出安全需求修正。
		一、執行「源碼掃描」一、應針對安全需求實作必要控制措施。
	2 bt xx	安全檢測。  二、應注意避免軟體常見漏洞及實作必要
	系統發展上会	二、具備系統嚴重錯 控制措施。
系統與	展生命	誤之通知機制。 三、發生錯誤時,使用者頁面僅顯示簡短
服務獲	週期開 發階段	三、等級「中」及「普」  錯誤訊息及代碼,不包含詳細之錯誤
旅游復   得	7 16 代	之所有控制措 訊息。
行		施。
		│一、執行「滲透測 │執行「弱點掃描」安全檢測。
	系統發	試」安全檢
	展生命	測。
	週期測	二、等級「中」及
	試階段	「普」之所有
		控制措施。
	系統發	一、於系統發展生命週期之維運階段,須 一、於部署環境中應
	展生命	注意版本控制與變更管理。 針對相關資通安
	週期部	二、等級「普」之所有控制措施。    全威脅,進行更
	署與維	新與修補,並關
	運階段	閉不必要服務及
-		

- 面:
- (一) 內部使用者 之識別與鑑別 之高級控制的 施第一點的 作文字義明 使文義明確 以利理解。
- 五、系統與服務獲 得構面:
- (二)系統發展生命 週期開發階段 之高級控制措 施第二點規定 酌作文字修 正。

		施。	
	1. 14 14	一、執行「滲透測試」 執行「弱點掃描」	
	系統發	安全檢測。	•
	展生命	二、等級「中」及「普」	
	週期測	之所有控制措	
	試階段	施。	
		一、於系統發展生命週期之維運階段,	應一、於部署環境中應
			<del>-</del>
	系統發	執行版本控制與變更管理。	針對相關資通
	展生命	二、等級「普」之所有控制措施。	安全威脅,進行
	週期部		更新與修補,並
	署與維		關閉不必要服
	運階段		務及埠口。
	Z1111X		二、資通系統不使用
			預設密碼。
	系統發	資通系統開發如委外辦理,應將系統發	<b>秦</b> 展生命週期各階段依等
	展生命	級將安全需求(含機密性、可用性、完	整性)納入委外契約。
	週期委		
	外階段		
	獲得程	開發、測試及正式作業環境應為區隔。	無要求。
	序	WAY STANDARD	, m 2 1
	系統文	應儲存與管理系統發展生命週期之相關	文件。
	件		
		一、資通系統應採用 無要求。	無要求。
		加密機制,以防	
		止未授權之資	
		訊揭露或偵測	
		資訊之變更。但	
		傳輸過程中有	
		替代之實體保	
		護措施者,不在	
		上限。 此限。	
2 4 编	傳輸之	, ,	
系統與	機密性	二、使用公開、國際	
通訊保	與完整	機構驗證且未	
護	性	遭破解之演算	
		法。	
		三、支援演算法最大	
		長度金鑰。	
		四、加密金鑰或憑證	
		<u>應定期</u> 更換。	
		五、伺服器端之金鑰	
		保管應訂定管	
		理規範及實施	
		應有之安全防	

				埠口。
				二、資通系統相關軟
				體,不使用預設
	么从攻	次记名从明改儿子从	地四 应约么从政员	密碼。
	系統發	資通系統開發如委外		
	展生命	級將安全需求(含機	密性、可用性、完整	生)納入委外契約。
	週期委			
	外階段			
	獲得程	開發、測試及正式作	業環境應為區隔。	無要求。
	序			
	系統文	應儲存與管理系統發	展生命週期之相關文化	L
	件	737411711 = 71.0072	X = 1	'
	''	一、資通系統應採用	無要求。	無要求。
		加密機制,以防	無女化	無安化
		1		
		止未授權之資		
		訊揭露或偵測		
		資訊之變更。但		
		傳輸過程中有		
		替代之實體保		
		護措施者,不在		
		此限。		
	傳輸之	1		
		二、使用公開、國際		
	機密性	機構驗證且未		
系統與	與完整	遭破解之演算		
通訊保	性	法。		
頀		三、支援演算法最大		
		長度金鑰。		
		四、加密金鑰或憑證		
		週期性更換。		
		五、伺服器端之金鑰		
		保管應訂定管		
		理規範及實施		
		應有之安全防		
		護措施。		
	資料儲	静置資訊及相關具	無要求。	無要求。
	存之安	保護需求之機密資		
	全	訊應加密儲存。		
		一、定期確認資通系:		系統之漏洞修復應
	漏洞修	態。		測試有效性及潛在
系統與	復	二、等級「普」之所:	<b>有控制措施</b> 。	影響,並定期更新。
資訊完		<del> </del>	一、監控資通系統,	
整性	資通系			
1- 1-h	統監控	自動化工具監		
	100 7117 17	控進出之通信	未授權之連	機關特定人員。

- 六、系統與通訊保 護構面:
- (一)傳輸之機密性 與完整性之高 級控制措施第 四點規定酌作 文字修正。
- (二) 資料儲存之安 全之高級控制 措施酌作文明 修正,並刪解 備註一對靜置 資訊之說明。
- 七、其餘構面及措 施內容未修 正。

		NAP 111 V.		
		護措施。	5	5
		資通系統重要組態	無要求。	無要求。
	資料儲	設定檔案及其他具		
	存之安	保護需求之資訊應		
	全	加密或以其他適當		
		<u>方式</u> 儲存。		
	漏洞修	一、定期確認資通系	統相關漏洞修復之狀	系統之漏洞修復歷
	復	態。		測試有效性及潛石
	1文	二、等級「普」之所	有控制措施。	影響,並定期更新
		一、資通系統應採用	一、監控資通系統,	發現資通系統有衫
		自動化工具監	以偵測攻擊與	入侵跡象時,應通幸
		控進出之通信	未授權之連	機關特定人員。
		流量,並於發現	線,並識別資	
	資通系	不尋常或未授	通系統之未授	
	統監控	權之活動時,針	權使用。	
		對該事件進行	二、等級「普」之所	
		分析。	有控制措施。	
系統與		二、等級「中」之所		
<b>示</b> 統		有控制措施。		
貝矶元整性		一、應定期執行軟體	一、使用完整性驗證	無要求。
正江		與資訊完整性	工具,以偵測未	
		檢查。	授權變更特定	
		二、等級「中」之所	軟體及資訊。	
		有控制措施。	二、使用者輸入資料	
	軟體及		合法性檢查應	
	資訊完		置放於應用系	
	整性		統伺服器端。	
			三、發現違反完整性	
			時,資通系統應	
			實施機關指定	
			之安全保護措	
			施。	

備註:特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之 範圍內,另行訂定其所管特定非公務機關之系統防護基準。

	流量,並於發現	線,並識別資	
	不尋常或未授	通系統之未授	
	權之活動時,針	權使用。	
	對該事件進行	二、等級「普」之所	
	分析。	有控制措施。	
	二、等級「中」之所		
	有控制措施。		
	一、應定期執行軟體	一、使用完整性驗證	無要求。
	與資訊完整性	工具,以偵測未	
	檢查。	授權變更特定軟	
	二、等級「中」之所	體及資訊。	
お 配曲 刀	有控制措施。	二、使用者輸入資料	
軟體及		合法性檢查應置	
資訊完		放於應用系統伺	
整性		服器端。	
		三、發現違反完整性	
		時,資通系統應	
		實施機關指定之	
		安全保護措施。	
 L	I		

#### 備註:

- 一、靜置資訊,指資訊位於資通系統特定元件,例如儲存設備上之狀態,或與系統相關需要保護之資訊,例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符內容等資訊。
- 二、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範 圍內,另行訂定其所管特定非公務機關之系統防護基準。

#### 資通安全責任等級分級辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 108 年 8 月 26 日行政院院臺護字第 1080184606 號令修正

#### 部分條文修正條文對照表

修正條文	現行條文	說明
第四條 各機關有下列	第四條 各機關有下列	一、序文、第一款至第四
情形之一者,其資通安	情形之一者,其資通安	款與第六款及第七
全責任等級為 A 級:	全責任等級為 A 級:	款未修正。
一、業務涉及國家機	一、業務涉及國家	二、考量未來關鍵基礎
密。	機密。	設施之領域可能因
二、 業務涉及外交、	二、業務涉及外交、	應科技發展、環境改
國防或國土安全	國防或國土安	變等因素調整,爰修
事項。	全事項。	正第五款以保留彈
三、業務涉及全國性	三、業務涉及全國	性及符合實務需求。
民眾服務或跨公	性民眾服務或	
務機關共用性資	跨公務機關共	
通系統之維運。	用性資通系統	
四、業務涉及全國性	之維運。	
民眾或公務員個	四、業務涉及全國	
人資料檔案之持	性民眾或公務	
有。	員個人資料檔	
五、屬公務機關,且	案之持有。	
業務涉及全國性	五、屬公務機關,且	
之關鍵基礎設施	業務涉及全國	
事項。	性之能源、水資	
六、屬關鍵基礎設施	源、通訊傳播、	
提供者,且業務	交通、銀行與金	
經中央目的事業	融、緊急救援事	
主管機關考量其 提供或維運關鍵	項。 六、屬關鍵基礎設	
基礎設施服務之	八、屬 關 疑 圣 旋 設 施提供者,且業	
五 一 用戶數、市場占	務經中央目的	
有率、區域、可替	事業主管機關	
代性,認其資通	考量其提供或	
★統失效或受影	維運關鍵基礎	
響,對社會公共	設施服務之用	
利益、民心士氣	戶數、市場占有	
或民眾生命、身	率、區域、可替	
體、財產安全將	代性,認其資通	
產生災難性或非	系統失效或受	
常嚴重之影響。	影響,對社會公	

- 七、屬公立醫學中心。
- 七、屬公立醫學中心。
- 第五條 各機關有下列 情形之一者,其資通安 全責任等級為B級:
  - 一、業務涉及公務機關 捐助<u>、資助</u>或研發 之敏感科學技術 資訊之安全維護 及管理。
  - 二、業務涉及區域性、 地區性民眾服務 或跨公務機關共 用性資通系統之 維運。
  - 三、業務涉及區域性 或地區性民眾個 人資料檔案之持 有。
  - 四、業務涉及中央二級機關及所屬各級機關(構)共用性資通系統之維運。
  - 五、屬公務機關,且業 務涉及區域性或 地區性之<u>關鍵基</u> 礎設施事項。

- 第五條 各機關有下列 情形之一者,其資通安 全責任等級為B級:
  - 一、業務涉及公務機 關捐助或研發之 敏感科學技術資 訊之安全維護及 管理。
  - 二、 業務涉及區域 性、地區性民眾 服務或跨公務機 關共用性資通系 統之維運。
  - 三、業務涉及區域性 或地區性民眾個 人資料檔案之持 有。

  - 五、屬提經主提基用有代系響利鍵者 中 管供礎戶率性統,益嬰果,目關維施、與數、,失對、基則,因認效社民心。與其事量關務場可資受公士、與其事量關務場可資受公士、

- 一、序文、第二款及第三 款未修正。
- 三、考量公務機關之業 器若涉及中各級關 關(構)共用是與 關(構)共用與 系統資通安全 當之資 資質 第四 大開情形規定。
- 五、現行第五款及第六 款款次配合遞移為 第六款及第七款,內 容未修正。

社會公共利益、民 心士氣或民眾生 命、身體、財產安 全將產生嚴重影響。

<u>七</u>、屬公立區域醫院 或地區醫院。 或民眾生命、身 體、財產安全將 產生嚴重影響。 六、 屬公立區域醫

院或地區醫院。

- 第八條 各機關有下列 情形之一者,其資通安 全責任等級為 E 級:
  - 一、無資通系統且未 提供資通服務。
  - 二、屬公務機關業務 其全部級機關或上機關或上門機關指定之公務機關兼辦或代 機關一大學

- 第八條 各機關有下列 情形之一者,其資通安 全責任等級為E級: 五、無資通系統且未 提供資通服務。
  - 六、屬公務機關,且 其全部資通業務 由其上級或監督 機關兼辦或代 管。
  - 七、屬關通目關業公央機公代特,業的、主務目關務事中管機的所機。非其由業央機關事管關公全其主目關,業特兼關政主定共產,業的所或主定辦機資央機事屬中管的所或主定辦機

- 一、序文及第一款未修 正。

第十一條 各機關應依 其資通安全責任等級, 辦理附表一至附表八 之事項。

第十一條 各機關應依 其資通安全責任等級, 辦理附表一至附表八 之事項。

- 一、第一項、第四項及第 五項未修正。

機關就特定類型資通 系統之防護基準認有 另為規定之必要者,得 自行擬訂防護基準,報 請主管機關核定後,依 其規定辦理。

各機關辦理附表 一至附表八所定事項 或執行附表十所定控 制措施,因技術限制、 個別資通系統之設計、 結構或性質等因素,就 特定事項或控制措施 之辦理或執行顯有困 難者,得經第三條第二 項至第四項所定其等 級提交機關或同條第 五項所定其等級核定 機關同意,並報請主管 機關備查後,免執行該 事項或控制措施;其為 主管機關者,經其同意 後,免予執行。

公務機關之資通 安全責任等級為 A 級 或 B 級者,應依主管機 關指定之方式,提報第 一項及第二項事項之 辦理情形。

中央目的事業主 管機關得要求所管特 定非公務機關,依其指 定之方式提報第一項 及第二項事項之辦理 情形。

第十二條 本辦法之施 行日期,由主管機關定 之。

<u>本辦法修正條文</u> 自發布日施行。 主管機關就特定類型 資通系統之防護基準 認有另為規定之必護基 者,得自行擬訂防護基 準,報請主管機關核定 後,依其規定辦理。

一或制個結特之難項級五機機事 機表附,通性項或經四機定 關八表因系質或執第項關其,後 關八表因系質或執第項關其,後 實或執第項關其,後 對理定所限設素措有第其條核主行。 附事定制計,就施困二等第定管該

公務機關之資通 安全責任等級為 A 級 或 B 級者,應依主管機 關指定之方式,提報第 一項及第二項事項之 辦理情形。

中央目的事業主 管機關得要求所管特 定非公務機關,依其指 定之方式提報第一項 及第二項事項之辦理 情形。 第十二條 本辦法之施 行日期,由主管機關定 之。 一、第一項未修正。

二、為明定本辦法修正 條文之施行日期,爰 增訂第二項規定。

# 附表一修正對照表

		修正規	定			現行規	定	訪
		A 級之公務機關應		附表一 資道	鱼安全責任等級	A級之公務機關應	辨事項	一、於
制度面向	辨理項目	辨理項目細項	辦理內容	制度面向	辨理項目	辨理項目細項	辨理內容	資
	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,並完成附表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。 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		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,並完成附表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。 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 資訊	理入正驗實定270訊
	過公正第三方		27001 音頁訊安全管理系統條準、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,於三年內完成公正第三方 驗證,並持續維持其驗證有效性。 初次受核定或等級變更後之一年內,配	管理面	過公正第三方		安全管理系統 <u>國家</u> 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,於三年內完成公正第三方驗證,並 持續維持其驗證有效性。 初次受核定或等級變更後之一年內,配	<b>二、機通</b>
<b>然</b> 田 工	資通安全專責		置四人;須以專職人員配置之。		資通安全專責	. , ,	置四人;須以專職人員配置之。	護家
管理面	內部資通安全稽核 業務持續運作演練		每年辦理二次。		內部資通安全		每年辦理二次。	全
			全部核心資通系統每年辦理一次。		業務持續運作		全部核心資通系統每年辦理一次。	於
	資安治理成熟	<b>度評估</b>	每年辦理一次。		資安治理成熟	1	每年辦理一次。	中
			一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定 之廠商生產、研發、製造或提供之		安全性檢測	網站安全弱點檢測 系統渗透測試	全部核心資通系統每年辦理二次。	制害
	限制使用危害品	國家資通安全產	危害國家資通安全產品。  二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品,應列冊管理,且不得與公務網路環境介接。	技術面	資通安全健 診	網路架構檢視 網路惡意活動檢視 使用者端電腦	- 每年辦理一次。	通品於訓對全人安訓為
技術面	安全性檢測 資通安全健 診	網站安全弱點檢測 系統滲透測試 網路架構檢視 網路惡意活動檢視 使用者端電腦	全部核心資通系統每年辦理二次。 全部核心資通系統每年辦理一次。 每年辦理一次。		資通安全威脅	線設定檢視	初次受核定或等級變更後之一年內,完 成威脅偵測機制建置,並持續維運及依 主管機關指定之方式提交監控管理資 料。	為全員年受時資專

		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	
			2. 4 应 1 户 2 茨 加 6
			初次受核定或等級變更後之一年內,
	<b>資通安全威</b> 有	曾 偵測管理機制	成威脅偵測機制建置,並持續維運及
	X 3X = M()	, , , , , , , , , , , , , , , , , , ,	主管機關指定之方式提交監控管理
			料。
			初次受核定或等級變更後之一年內,
	政府組態基準	<b>崖</b>	主管機關公告之項目,完成政府組態
			準導入作業,並持續維運。
		防毒軟體	
		網路防火牆	
		具有郵件伺服器	
		者,應備電子郵	
		件過濾機制	
		入侵偵測及防禦	初次受核定或等級變更後之一年內,
	資通安全	機制	成各項資通安全防護措施之啟用,並
	防護	具有對外服務之	續使用及適時進行軟、硬體之必要更
			或升級。
		核心資通系統	
		者,應備應用程	
		式防火牆	
		進階持續性威脅	
		攻擊防禦措施	
		   資通安全專職人	<u>每人</u> 每年至少接受十二小時以上之
		員	通安全專業課程訓練或資通安全職
		<u> </u>	訓練。
	資通安全	資通安全專職人	<u>每人每二</u> 年至少接受 <u>三</u> 小時以上之
	教育訓練	員以外之資訊人	通安全專業課程訓練或資通安全職
	秋月町派		訓練,且每年接受三小時以上之資通
±17 4		<u>員</u>	全通識教育訓練。
認知		一般使用者及主	每人每年接受三小時以上之資通安
與訓練		管	通識教育訓練。
		次记山入市业地	初次受核定或等級變更後之一年內,
		資通安全專業證	通安全專職人員總計應持有四張以上
	資通安全專	照	並持續維持證照之有效性。
	業證照及職	than it is it is	初次受核定或等級變更後之一年內,
	能訓練證書	資通安全職能評	通安全專職人員總計應持有四張以上
		量證書	並持續維持證書之有效性。

	政府組態基準	<b>集</b>	初次受核定或等級變更後之一年內,依 主管機關公告之項目,完成政府組態基 準導入作業,並持續維運。
	資通安全 防護	防舞 男者件入機 具核者式進數 數	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。
	資通安全 教育訓練	資通安全及資訊 人員 一般使用者及主 管	每年至少 <u>四名人員各</u> 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。 每人每年接受三小時以上之 <u>一般</u> 資通 安全教育訓練。
認知與訓練	資通安全專	資通安全專業證 照	初次受核定或等級變更後之一年內,資 通安全專職人員總計應持有四張以上, 並持續維持證照之有效性。
	業證照及職能訓練證書	資通安全職能評 量證書	初次受核定或等級變更後之一年內,資 通安全專職人員總計應持有四張以上, 並持續維持證書之有效性。

#### 供社

- 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。
- 三、資通安全專職人員,指應全職執行資通安全業務者。
- 四、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。
- 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。

課程;其他 資訊人員 每人每二 年至少接 受三小時 以上之資 通安全專 業訓練課 程,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,修正 為每人每 年接受三 小時以上 之資通安 全通識教 育訓練,以 使規範明 確。

五、其餘內容 未修正。

- 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。
- 三、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 四、資通安全專職人員,指應全職執行資通安全業務者。
- <u>五</u>、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。
- <u>六</u>、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。

# 附表二修正對照表

		修正規	定			現行規	見定	說明
附表二 資	通安全責任等級	A級之特定非公務	<b>5機關應辦事項</b>	附表二 資達	通安全責任等級	k A 級之特定非公科	务機關應辦事項	一、於管理面之
制度面向	辨理項目	辨理項目細項	辨理內容	制度面向	辨理項目	辦理項目細項	辦理內容	資訊安全管
管理面	資通系統分級		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,並完成附表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。		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,並完成附表十之 控制措施;其後應每年至少檢視一次資 通系統分級妥適性。	理系統之導 入及通過公 正第三方之 驗證,配合
	過公正第三方		部核心資通系統導入 CNS 27001 <u>或</u> 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,於三年內完成公正第 三方驗證,並持續維持其驗證有效性。	管理面	資訊安全管理過公正第三方	里系統之導入及通 「之驗證	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 資訊安全管理系統國家標準、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,於三年內完成公正第三方驗證,並持續維持其驗證有效性。	實務包 27001 全標 解
	資通安全專責		初次受核定或等級變更後之一年內,配置四人。		資通安全專責	人員	初次受核定或等級變更後之一年內,配 置四人。	機關之資
	內部資通安全		每年辦理二次。		内部資通安全	<b>*</b> 稽核	每年辦理二次。	護,降低國
	業務持續運作	演練	全部核心資通系統每年辦理一次。		業務持續運作	<b>F演練</b>	全部核心資通系統每年辦理一次。	家資通安
			一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定		安全性檢測	網站安全弱點 檢測	全部核心資通系統每年辦理二次。	全風險,爰 於管理面
			之廠商生產、研發、製造或提供之			系統滲透測試	全部核心資通系統每年辦理一次。	中增訂限
The die T	限制使用危害品 安全性檢測	F國家資通安全產 網站安全弱點	危害國家資通安全產品。  二、必須採購或使用危害國家資通安全產品時,應具體敘明理由,經主管機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品,應列冊管理,且不得與業務網路環境介接。  全部核心資通系統每年辦理二次。	技術面	資通安全健 診	網路架構檢視 網路 競視 化 电 电 电 电 电 电 电 电 电 电 电 电 电 电 电 电 电 电	- 每年辦理一次。	一制害通品於訓對全人制害通品於訓對全人員資產。與針安訊通
技術面	文主任级内	檢測 系統滲透測試	全部核心資通系統每年辦理一次。		資通安全威脅	線設定檢視	初次受核定或等級變更後之一年內,完 成威脅偵測機制建置,並持續維運。	安全教育訓練,修正為資通安
	資通安全健 診	網路架構檢視網路惡意活動檢視 使用者端電腦惡意活動檢視	每年辦理一次。		資通安全 防護	防毒軟體 網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制	初次受核定或等級變更後之一年內,完 一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。	· 一章 年 章 年 受 時 一章 兵 年 受 時 一章 兵 上 一 上 一 上 一 一 上

		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	
	資通安全威脅	偵測管理機制	初次受核定或等級變更後之一年內,完
			成威脅偵測機制建置,並持續維運。
	資通安全	防毒軟體	初次受核定或等級變更後之一年內,完
	防護	網路防火牆	成各項資通安全防護措施之啟用,並持
		具有郵件伺服	續使用及適時進行軟、硬體之必要更新
		器者,應備電	或升級。
		子郵件過濾機	
		制	
		入侵偵測及防	
		禦機制	
		具有對外服務	
		之核心資通系	
		統者,應備應	
		用程式防火牆	
		進階持續性威	
		脅攻擊防禦措	
		施	
認知	資通安全	資通安全專責	每人每年至少接受十二小時以上之資通
與訓練	教育訓練	人員	安全專業課程訓練或資通安全職能訓
		<u> </u>	練。
		資通安全專責	<u>每人</u> 每二年至少接受三小時以上之資通
		人員以外之資	安全專業課程訓練或資通安全職能訓
		訊人員	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	每人每年接受三小時以上之資通安全通
		主管	<u>識</u> 教育訓練。
	資通安全專業	證照	初次受核定或等級變更後之一年內,資
			通安全專責人員總計應持有四張以上,
			並持續維持證照之有效性。

- 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。
- 三、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 四、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。

		入侵偵測及防	
		禦機制	
		具有對外服務	
		之核心資通系	
		統者,應備應用	
		程式防火牆	
		進階持續性威	
		脅攻擊防禦措	
		施	
		資通安全及資	每年至少四名人員各接受十二小時以上
	資通安全	訊人員	之資通安全專業課程訓練或資通安全職
	教育訓練	机尺只	能訓練。
認知	我月町杯	一般使用者及	每人每年接受三小時以上之 <u>一般</u> 資通安
與訓練		主管	全教育訓練。
			初次受核定或等級變更後之一年內,資
	資通安全專業	證照	通安全專責人員總計應持有四張以上,
			並持續維持證照之有效性。

#### 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。
- 三、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 四、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- 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。

資通安全 專業訓練 課程;其他 資訊人員 每人每二 年至少接 受三小時 以上之資 通安全專 業訓練課 程,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,修正 為每人每 年接受三 小時以上 之資通安 全通識教 育訓練,以 使規範明 確。

四次訂家全定明合第第點共構危資產義確將三五次於註害通品以並現點點移定註 医通口炎

五、其餘內容 未修正。

五、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。	
六、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。	

# 附表三修正對照表

	修正規	上定			現行規	見定	說明
			附表三 資通	1安全責任等級	B級之公務機關應	辨事項	一、於管理面之
	辨埋項目細項		制度面向	辦理項目	辦理項目細項	辦理內容	資訊安全行
資訊安全管理	系統之導入及通	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,並完成附表十之 控制措施;其後應每年至少檢視一次資 通系統分級妥適性。 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,於三年內完成公正第三方驗證,	管理面	資通系統分級資訊安全管理	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,依附表力完成資通系統分級,並完成附表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。 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 資訊安全管理系統國家標準、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,	理入正驗實定27001 全標的工程 放通三,需含 等管準統 等管準確 以資
		初次受核定或等級變更後之一年內,配置二人;須以專職人員配置之。		資通安全專責	-人員	維持其驗證有效性。 初次受核定或等級變更後之一年內,配 置二人;須以專職人員配置之。	二、為強化行機關之可
				內部資通安全	稽核	每年辦理一次。	護,降低
	*					全部核心資通系統每二年辦理一次。	家資通
<b>育安治埋成</b> 熟月	<b>支</b> 評估	* 1 2 1				每年辦理一次。	全風險,
		不得採購及使用主管機關核定之廠 商生產、研發、製造或提供之危害國		安全性檢測	網站安全弱點 檢測	全部核心資通系統每年辦理一次。	於管理 · · · · · · · · · · · · · · · · · · ·
限制使用危害!	<b>國家資通安全產</b>	二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管機 關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管機 關核可採購之危害國家資通安全產 品,應列冊管理,且不得與公務網路	技術面	資通安全健	網路架構檢視網路惡意活動檢視 伊用者端 稅 惡意活動檢視 同服 器主機 惡意活動檢視 音話動檢視 器 設 日錄 伺服 器 設	- 每二年辦理一次。	害通品於訓對全人內國安之認練資及員入
安全性檢測資通安全健	檢測 系統滲透測試 網路架構檢視 網路惡意活動	全部核心資通系統每年辦理一次。 全部核心資通系統每二年辦理一次。 每二年辦理一次。		資通安全威脅	定及防火牆連 線設定檢視 傾測管理機制	初次受核定或等級變更後之一年內,完 成威脅偵測機制建置,並持續維運及依 主管機關指定之方式提交監控管理資 料。	安訓為全員年受致為軍母至十
	辦理	<ul> <li>●安全責任等級 B 級之公務機關應</li> <li>一方</li></ul>	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,並完成附表十之 控制措施;其後應每年至少檢視一次資 通系統分級與適性。 初次受核定或等級變更後之二年內,全 部核心資通系統等入 CNS 27001 或 ISO 27001 等資訊安全管理系統是其他具 有同等或以上效果之系統標準,其他具 有同等或以上效果之系統標準。其他公務機關自行發展並經主管機關認可 之標準,於三年內完成公正第三方驗證, 並持續維持其驗證有效性。 初次受核定或等級變更後之一年內,配 置二人;須以專職人員配置之。 每年辦理一次。 等等持續運作演練 全部核心資通系統每二年辦理一次。 每年辦理一次。 一、除因業務需求且無其他替代方案外, 不得採購及使用主管機關核定之廠。 高生產、研發、製造或提供之危害國家資通安全產 產品時、應具體敘明理由,經主管機關核可發,以專案方式購置。 三、必須採購或使用危害國家資通安全產 產品時、應具體敘明理由,經主管機關核可採購之危害國家資通安全產 品。三、必須採購之危害國家資通安全產品。。一次沒採購之危害國家資通安全產品。是於實施大時而已使用或因業 務需求且無其他替代方案外, 不得採購及使用主管機關核定之廠。  一、除因業務需求且無其他替代方案外, 不得採購及使用主管機關核定之廠。  一、除因業務不是由其他替代方案外, 不得採購及使用方害國家資通安全產產品時,應到體核可發,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案外。 全部核心資通系統每年辦理一次。 全部核心資通系統每年辦理一次。 全部核心資通系統每年辦理一次。	西安全責任等級 B 級之公務機關應辦事項     が理項目	一次日本学校 B 級之公務機關應辦事項   一次	●安全青任等級 B 級之公務機關應辦事項	新型項目 解理項目項項 新型項目 解理項目項項 初次受益定及單級變更後之一年內,針對自行或差外所屬交互自無熱,依附表上 沒無於分級及防護基準 初次受益定及單級變更後之一年內,針對自行或差外所屬交互自無熱,依附表上 沒無於分級及防護基準 打發應每年至少檢視一次資 透系統分級及防護基準 打發應每年至少檢視一次資 超過系統分級及防護基準 打發應每年至少檢視一次資 超過系統分級及防護基準 打發應每年至少檢視一次資 超減系統分級及防護基準 打發應每年至少檢視一次資 超減系統分級及防護基準 化公請機關自行勞基金與主管機關認可之權 非特別維持其驗證有效性 化於 27001 至 1800 27001 至 所以 美文 至 大學

信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 初次受核定或等級變更後之一年內成威脅偵測機制建置,並持續維運主管機關指定之方式提交監控管料。	及依
定及防火牆連線設定檢視 初次受核定或等級變更後之一年內 成威脅偵測機制建置,並持續維運主管機關指定之方式提交監控管 料。	及依
資通安全威脅偵測管理機制 主管機關指定之方式提交監控管 料。	及依
	<b>-</b> X
初次受核定或等級變更後之一年內 政府組態基準 主管機關公告之項目,完成政府組 準導入作業,並持續維運。	
防毒軟體 網路防火牆 具有郵件伺服 器者,應備電子	
資通安全 資通安全 所護 一 一 一 一 一 一 一 一 一 一 一 一 一	並持
統者,應備應用 程式防火牆	
<u>資通安全專職</u> 人員 每人每年至少接受十二小時以上之安全專業課程訓練或資通安全職練。	
資通安全 教育訓練 <u>資通安全專職</u> 人員以外之資 訊人員 <u>調識教育訓練。</u>	能訓
四般使用者及 每人每年接受三小時以上之資通安 主管 <u>識</u> 教育訓練。	全通
資通安全專業 資通安全專業 證照 業證照及職 資通安全專業 一類 一類 一類 一類 一類 一類 一類 一類 一類 一類	
能訓練證書 資通安全職能 評量證書 初次受核定或等級變更後之一年內 通安全專職人員總計應持有二張以 並持續維持證書之有效性。	, ,

- 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。

	政府組態基準		初次受核定或等級變更後之一年內,依 主管機關公告之項目,完成政府組態基 準導入作業,並持續維運。
	資通 <del>安</del> 全 防護	防毒軟體 網有有 網有 門 門 門 門 門 門 門 門 門 門 門 門 門 門 門 門	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。
	資通安全 教育訓練	資通安全及資 訊人員	每年至少 <u>二名人員各</u> 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。
認知		一般使用者及 主管	每人每年接受三小時以上之 <u>一般</u> 資通安     全教育訓練。
與訓練		資通安全專業 證照	初次受核定或等級變更後之一年內,資 通安全專職人員總計應持有二張以上, 並持續維持證照之有效性。
<b>佑註</b> :		資通安全職能 評量證書	初次受核定或等級變更後之一年內,資 通安全專職人員總計應持有二張以上, 並持續維持證書之有效性。

#### 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。
- 三、資通安全專職人員,指應全職執行資通安全業務者。
- 四、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。
- 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。

資通安全 專業訓練 課程;其他 資訊人員 每人每二 年至少接 受三小時 以上之資 通安全專 業訓練課 程,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,修正 為每人每 年接受三 小時以上 之資通安 全通識教 育訓練,以 使規範明 確。

四次 訂家全定明合第第點共構危資產義確將三五次於註害通品以並現點點穩定 的 過 報 國 安 之資配 行至 之。

五、其餘內容 未修正。

- 三、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政 府運作或社會安定之資通系統或資通服務。
- 四、資通安全專職人員,指應全職執行資通安全業務者。
- <u>五</u>、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。
- <u>六</u>、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。

# 附表四修正對照表

		修正規	見定			現行規	見定		說明
附表四 資通 制度面向	通安全責任等級 辦理項目	B級之特定非公務 辦理項目細項	機關應辦事項辦理內容	附表四 資通制度面向	全 全 全 全 章 全 章 任 等級 一 競 理 項 目 日	B級之特定非公務 辦理項目細項	機關應辦事項辦理內容	- \	於管理面之 訊安全管理
管理面	新珪項日 新珪項日細項 資通系統分級及防護基準 資訊安全管理系統之導入及通 過公正第三方之驗證		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,依附表力完成資通系統分級,並完成附表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。	14/交出19	資通系統分級及防護基準 資訊安全管理系統之導入及通 過公正第三方之驗證		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,依附表力完成資通系統分級,並完成附表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。		統之導入及 過公正第三 之驗證,配合 務需求明定
			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,於三年內完成公正第三方驗證,並持續維持其驗證有效性。	管理面			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 資訊安全管理系統國家標準、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,於三年內完成公正第三方驗證,並持續維持其驗證有效性。	資系明為之	含ISO 27001 資訊安全管 系統標準, 明確。 為強強。 各資 養養 養養
	資通安全專責人員 內部資通安全稽核		初次受核定或等級變更後之一年內,配 置二人。 每年辦理一次。				每年辦理一次。		資通安全 險,爰於管 面中增訂限
	業務持續運作演練 限制使用危害國家資通安全產 品		全部核心資通系統每二年辦理一次。 一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定 之廠商生產、研發、製造或提供之	技術面	業務持續運作安全性檢測	演練 網站安全弱點 檢測 系統渗透測試	全部核心資通系統每二年辦理一次。     全部核心資通系統每年辦理一次。     全部核心資通系統每二年辦理一次。		使用危害國 資通安全。 之規定。 於認知與訓
			○ 表		資通安全健 診	網路架構檢視 網路惡意活動 檢視 使用者端電腦	每二年辦理一次。		中安員育為責年二資計及通練通員少時安置與通過員少時安置
技術面	安全性檢測	網站安全弱點檢測 系統滲透測試	全部核心資通系統每年辦理一次。 全部核心資通系統每二年辦理一次。		資通安全威脅	線設定檢視 偵測管理機制	初次受核定或等級變更後之一年內,完 成威脅偵測機制建置,並持續維運。		訓練課程; 他資訊人員 人每二年至
	資通安全健 診	網路架構檢視 網路惡意活動 檢視 使用者端電腦 惡意活動檢視	每二年辦理一次。		資通安全 防護	防毒軟體 網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制	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。	,	接上專程受之業,且所通知,但是資源,但是資源,是不可以不可以不可以不可以不可以不可以不可以不可以不可以不可以不可以不可以不可以不

		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	
	資通安全威脅	,偵測管理機制	初次受核定或等級變更後之一年內,完 成威脅偵測機制建置,並持續維運。
		防毒軟體	
		網路防火牆	
		具有郵件伺服	
		器者,應備電子	   初次受核定或等級變更後之一年內,完
	資通安全 防護	郵件過濾機制	· 成各項資通安全防護措施之啟用,並持
		入侵偵測及防	放谷項貝迪女主的設相地之級用,並行
		禦機制	或升級。
		具有對外服務	( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )
		之核心資通系	
		統者,應備應用	
		程式防火牆	
		資通安全專責 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。
認知與訓練	資通安全 教育訓練	資通安全專責 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	每人每年接受三小時以上之資通安全通
		主管	<u>識</u> 教育訓練。
			初次受核定或等級變更後之一年內,資
	資通安全專業	證照	通安全專責人員總計應持有二張以上,
			並持續維持證照之有效性。

- 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。 三、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政 府運作或社會安定之資通系統或資通服務。
- 四、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 五、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- <u>六</u>、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。

		入侵惧測及防 禦機制 具有對外服務 之核,應備應用 程式防火牆	
	資通安全 教育訓練	資通安全及資 訊人員	每年至少 <u>二名人員各</u> 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。
認知與訓練	· 我 月 · 即 · 亦	一般使用者及 主管	每人每年接受三小時以上之 <u>一般</u> 資通安 全教育訓練。
	資通安全專業	證照	初次受核定或等級變更後之一年內,資 通安全專責人員總計應持有二張以上, 並持續維持證照之有效性。

#### 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、「公正第三方驗證」所稱第三方,指通過我國標準法主管機關委託機構認證之機構。
- 三、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 四、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- 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。

- 五、其餘內容未修 正。

# 附表五修正對照表

		修正規	定			現行規	定		說明
付表五 資通	L安全責任等級 (	級之公務機關應到	辦事項	附表五 資通	安全責任等級(	級之公務機關應到	辦事項	一、於	於管理面之
制度面向	辨理項目	辨理項目細項	辦理內容	制度面向	辨理項目	辨理項目細項	辦理內容	通	通系統分級
管理面	資通系統分級資訊安全管理	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,依附表力完成資通系統分級;其後應每年至少檢視一次資通系統分級發更後之二年內,完成稅養之空。 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。 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。 初次受核運藥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。	管理面	資通系統分級資訊安全管理	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妥適性; <u>系</u> 統等 檢視一次資通系統分級妥適性; <u>系</u> 等 級為「高」者,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。 初次受核定或等級變更後之二年內,資 部核心資通系統與不變更後之二年內,資 部核心資通系統與不之之 等理系統國家標準、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	防防等者以級金列資完招	防涂等者以吸针外资完空護現級」明之對開通成制基行為之確公自發系附措準「『文規務行之統表施
	資通安全專責人員 內部資通安全稽核 業務持續運作演練		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。 每二年辦理一次。 全部核心資通系統每二年辦理一次。		準,並持續維持導入。 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 業務持續運作演練 全部核心資通系統每二年辦理一次。		二、於部	間。 於管理面= 訊安全管3 統之導入	
			一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定 之廠商生產、研發、製造或提供之 危害國家資通安全產品。		亲務持續建作安全性檢測	網站安全弱點 檢測 系統渗透測試 網路架構檢視	全部核心資通系統每二年辦理一次。 全部核心資通系統每二年辦理一次。 全部核心資通系統每二年辦理一次。	定 2'	合實務需 定 包 含 27001 等 5 安全管理 <i>5</i>
	限制使用危害國家資通安全產品		二、必須採購或使用危害國家資通安全產品時,應具體敘明理由,經主管機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品,應列冊管理,且不得與公務網路環境介接。	技術面	資通安全健 診	網路惡意活動 檢視 使用者端電腦	- - - - - - - - - - - - - - - - - - -	三、之語資	票確為之獲資儉準。強資,通過降過,他通降安於與人人。
技術面	安全性檢測	網站安全弱點檢測 系統渗透測試	全部核心資通系統每二年辦理一次。			定及防火牆連 線設定檢視 防毒軟體		使	面中增訂[ 使用危害] 資通安全]
	資通安全健診	網路架構檢視 網路惡意活動檢視 使用者端電腦 惡意活動檢視	每二年辦理一次。		資通安全 防護	網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制		2 四、於中	《之於中安員 《規認,安全資本 《定知針及通 資安 資金

		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 防護	防毒軟體 網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制	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。
認知與訓練	資通安全 教育訓練	資通安全專職 人員 資通安全專職 人員與 人員 人員 人員 人員 人員 人員 人員 人員 人員 人員 人員 人員 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。 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。 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	資通安全專業 證照 資通安全職能 評量證書	資通安全專職人員總計應持有一張以上,並持續維持證照之有效性。 初次受核定或等級變更後之一年內,資 通安全專職人員總計應持有一張以上, 並持續維持證書之有效性。

- 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、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 三、資通安全專職人員,指應全職執行資通安全業務者。
- 四、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。
- <u>五</u>、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。

	資通安全 教育訓練	資通安全及資 訊人員	每年至少 <u>一名人員</u> 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。
認知		一般使用者及 主管	每人每年接受三小時以上之 <u>一般</u> 資通 安全教育訓練。
與訓練	資通安全專	資通安全專業 證照	資通安全專職人員總計應持有一張以 上。
	業證照及職 能訓練證書	資通安全職能 評量證書	初次受核定或等級變更後之一年內,資 通安全專職人員總計應持有一張以上, 並持續維持證書之有效性。

#### 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。
- 育訓練,修正 為資通安全專 職人員每人每 年至少接受十 二小時以上之 資通安全專業 訓練課程;其 他資訊人員每 人每二年至少 接受三小時以 上之資通安全 專業訓練課 程,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,修正為 每人每年接受 三小時以上之 資通安全通識 教育訓練,以 使規範明確。
- 五、於中安照續有定通員並附六致納針專訂證性確專業表及與對專訂證性確專業表及與數數資業應照之保職性一附定無通證持之規資人,至表一
- 六、於備註增訂危 害國家資通安 全產品之定 義,以資明確,

	並配合將現行
	並配合將現行 第二點至第四 點 之 點 次 遞
	移。
	七、其餘內容未修 正。

# 附表六修正對照表

		修正規	見定			現行規	見定	說明
附表六 資道	通安全責任等級	C 級之特定非公務	機關應辦事項		1	C級之特定非公務		一、於管理面之
制度面向	辨理項目	辦理項目細項	辦理內容	制度面向	辨理項目	辦理項目細項	辨理內容	通系統分級
~	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。	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; <u>系統等</u> 級為「高」者,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	防護基準, 除現行「系 等級為『高。 者」之文字, 明確規範C系 之特定非公元
			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。初次受核定或等級變更後之一年內,配		資訊安全管理	!系統之導入	施。 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 資訊安全管理系統國家標準、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。	機關針對自然 或委外開發 各級資通 統,應完成 表十之控制
管理面	資通安全專責		置一人。		資通安全專責人員 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一		施之時間。 二、於管理面之	
	內部資通安全稽核 業務持續運作演練		全部核心資通系統每二年辦理一次。		內部資通安全	<b>:</b> 稽核	每二年辦理一次。	訊安全管理
	未扮行领廷仆	<b>供</b> 体	一、除因業務需求且無其他替代方案		業務持續運作演練		全部核心資通系統每二年辦理一次。	統之導入,配
	限制使用危害國家資通安全產 品		外,不得採購及使用主管機關核定 之廠商生產、研發、製造或提供之	技術面	安全性檢測	網站安全弱點檢測 系統滲透測試	全部核心資通系統每二年辦理一次。	實務需求明 包含 ISO 2700
			危害國家資通安全產品。  二、必須採購或使用危害國家資通安全產品時,應具體敘明理由,經主管機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品,應列冊管理,且不得與業務網路環境介接。		資通安全健 診	網路架構檢視 網路惡意活動檢視 使用者端電腦	- 每二年辦理一次。	等資紙標。 等 選
	安全性檢測	網站安全弱點檢測	全部核心資通系統每二年辦理一次。			定及防火牆連 線設定檢視		面中增訂限制 使用危害國家 資通安全產品
技術面	資通安全健 診	系統滲透測試 網路架構檢視 網路惡意活動 檢視 使用者端電腦 惡意活動檢視	全部核心資通系統每二年辦理一次。 每二年辦理一次。		資通安全 防護	防毒軟體 網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制		之規定。四、於認知與訓中,針對資安全及資訊員資通安全

		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	
		防毒軟體	初次受核定或等級變更後之一年內,完
	資通安全	網路防火牆	成各項資通安全防護措施之啟用,並持
	防護	具有郵件伺服 器者,應備電子	續使用及適時進行軟、硬體之必要更新 或升級。
		郵件過濾機制	<b>以</b> 月級:
	資通安全 教育訓練	資通安全專責 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。
認知與訓練		資通安全專責 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		初次受核定或等級變更後之一年內,資 通安全專責人員總計應持有一張以上, 並持續維持證照之有效性。

- 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、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 三、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 四、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- <u>五</u>、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。

	資通安全 教育訓練	資通安全及資 訊人員	每年至少 <u>一名人員</u> 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。
認知		一般使用者及	每人每年接受三小時以上之一般資通
與訓練		主管	安全教育訓練。
	資通安全專業證照		初次受核定或等級變更後之一年內,資
			通安全專責人員總計應持有一張以上,
			並持續維持證照之有效性。

#### 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、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執 行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 三、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- 四、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。

為資通安全專 責人員每人每 年至少接受十 二小時以上之 資通安全專業 訓練課程;其 他資訊人員每 人每二年至少 接受三小時以 上之資通安全 專業訓練課 程,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,修正為 每人每年接受 三小時以上之 資通安全通識 教育訓練,以 使規範明確。

- 五、精註增資品。 當國家 是 養 就 配 等 是 養 就 配 等 第 是 实 的 是 第 第 第 二 之 。 移
- 一六、其餘內容未修 正。

# 附表七修正對照表

修正規定					現行規定			
附表七 資道	通安全責任等級	D級之各機關應辦	事項	附表七 資通	安全責任等級	D級之各機關應辦	事項	一、為強化各機關
制度面向	度面向 辦理項目 辦理項目細項 辦理內容				辨理項目	辨理項目細項	辦理內容	之資通安全防
			一、 <u>除因業務需求且無其他替代方案</u> 外,不得採購及使用主管機關核定			防毒軟體	初次受核定或等級變更後之一年內,完	護,降低國家資 通安全 压
			之廠商生產、研發、製造或提供之	,, ., _	資通安全	網路防火牆	成各項資通安全防護措施之啟用,並持	險,爰於管理
			<u>危害國家資通安全產品。</u>	技術面	防護	具有郵件伺服	續使用及適時進行軟、硬體之必要更新	面中增訂限制
#	限制使用危害國家資通安全產		二、 <u>必須採購或使用危害國家資通安</u> 全產品時,應具體敘明理由,經主			器者,應備電子 郵件過濾機制	或升級。	使用危害國家 資通安全產品
管理面	<u> </u>		<b>管機關核可後,以專案方式購置。</b>					之規定。
	<u>業</u> 管 安		三、對本辦法修正施行前已使用或因	認知	資通安全 教育訓練		每人每年接受三小時以上之一般資通	二、於認知與訓練
			業務需求且無其他替代方案經主	與訓練		主管	安全教育訓練。	中,針對一般 使用者及主
			管機關核可採購之危害國家資通	備註:特定非	世			
			安全產品,應列冊管理,且不得與 公務(業務)網路環境介接。	範圍內,另行	人每年接受三			
		7 + 1/ mb						小時以上之資
		防毒軟體						通安全通識教
技術面	資通安全	網路防火牆						育訓練,以使 規範明確。
文 师 田	防護	具有郵件伺服 器者,應備電子 郵件過濾機制						三、於備註增訂危害國家資通安全產品之定
			每人每年接受三小時以上之資通安全 <u>通識</u> 教育訓練。					義,以資明確 四、其餘內容未修 正。
備註:	1	1						
<u>一、</u> 特定非	公務機關之中中	·目的事業主管機關	<b>]得視實際需求,於符合本辦法規定之範圍</b>					
內,另行訂定其所管特定非公務機關之資通安全應辦事項。								
二、危害國	家資通安全產品	L,指對國家資通安	全具有直接或間接造成危害風險,影響政					
府運作	或社會安定之資	<b>通系統或資通服務</b>	<u>;</u> °					

# 附表八修正對照表

		修正規	定			現行規	.定	說明
附表八 資訊	通安全責任等級	E級之各機關應辦	事項	附表八 資通	附表八 資通安全責任等級 E 級之各機關應辦事項			一、為強化各機關
制度面向	辨理項目	辦理項目細項	辦理內容	制度面向	辨理項目	辦理項目細項	辨理內容	之資通安全防
管理面	限制使用危气品	害國家資通安全產	一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定 之廠商生產、研發、製造或提供之 危害國家資通安全產品。 二、必須採購或使用危害國家資通安 全產品時,應具體敘明理由,經主 管機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因 業務需求且無其他替代方案經主 管機關核可採購之危害國家資通 安全產品,應列冊管理,且不得與 公務(業務)網路環境介接。				每人每年接受三小時以上之 <u>一般</u> 資通 安全教育訓練。 機關得視實際需求,於符合本辦法規定之 機關之資通安全應辦事項。	護資險面使資之於中使管人, 通, 中用通規認, 用, 每点低安於訂害全。與對者正接. 國全管限國產 訓一及為受家風理制家品 練般主每三次
認知與訓練	資通安全 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。					小時以上之資 通安全通識教 育訓練,以使
內,另二、危害國	行訂定其所管料 家資通安全產品	<b>手定非公務機關之資</b>	得視實際需求,於符合本辦法規定之範圍 通安全應辦事項。 全具有直接或間接造成危害風險,影響政 5。					規範明確。 三、 無國 是 實 是 真 是 真 是 真 实 是 真 实 是 真 实 是 真 实 是 实 是 。 其 飲 內 容 表 。 正。

# 附表九修正對照表

附表允 資通系統防護需求分級原則    下放護需求
#
通系統受影響時,可能
通系統受影響時,可能
發生資通安全事件致資 發生資通安全事件致資 過系統受影響時,可能 通系統受影響時,可能 造成對資訊、資通系統 造成對資訊、資通系統 之存取或使用之中斷, 之存取或使用之中斷, 之存取或使用之中斷, 對機關之營運、資產或 信譽等方面將產生非常 信譽等方面將產生嚴重 信譽等方面將產生有限 最重或災難性之影響。 之影響。 發生資通安全事件致資 發生資通安全事件致資 發生資通安全事件致資 通系統受影響時,可能 通系統受影響時,可能 通系統受影響時,可能 造成對資訊、資通系統 造成對資訊、資通系統 造成對資訊、資通系統 造成對資訊、資通系統 之存取或使用之中斷, 之存取或使用之中斷, 之存取或使用之中斷 之存取或使用之中斷 之存取或使用之中斷 之存取或使用之中斷 之存取或使用之中斷 之存取或使用之中 對機關之營運、資產或 一對機關之營運、資產或 一對機關之營運、資產或 一大學等方面將產生嚴重 一位學等方面將產生不 一位學等方面將產生不 一定學等方面將產生不 一定學等 一定學等方面將產生不 一定學等方面, 一定學等方面, 一定學等方面, 一定學等方面, 一定學等方面, 一定學等一定學 一定學 一定學 一定學 一定學 一定學 一定學 一定學 一定學 一定學
如未確實遵循資通系統 設置或運作涉及之資通 設置或運作涉及之資通 设置或運作涉及之資通 安全相關法令,可能使 資通系統受影響而導致 資通安全事件,或影響 他人合法權益或機關執 行業務之公正性及正當性,並使機關所屬人員 負刑事責任。

# 附表十修正對照表

		修	正規定				現	行規定	
			附表十 資通系統防護基準						
系統 控制措施 構面	防護需求分級大力	高	中	普	控制措施構面	法防護需求 分級 措施內 容	高	中	普
存取控制	<b>帳號管</b>	期, 是 是 是 是 是 是 是 是 是 是 是 是 是 是 是 是 是 是 是	緊禁通應期 意應期 意應期 。 於。 於。 於。 於。 於。 於。 於。 於。 於。	含帳號之申請、開通、停用及刪除之程序。	存取控制	· · · · · · · · · · · · · · · · · · ·	期間 使應登應代資監號常理等時間,與關門,與關係統通控,使者級制則,使者級制則,使者級制,使者級制,與人人,與人人,與人人,與人人,與人人,與人人,與人人,與人人,與人人,與人	或資號與無 為 關 。 統 改 删 等 独 不 然 改 删 等 被 我 那 然 成 删 等 被 我 就 以 除 以 除 以 除 以 附 级 措 施 。 统 及 册 , 所 有 , 有	含帳號之申請、開通、 停用及刪除之程序。
最小權限		採最小權限原則,僅允許使用者(或代表使用 者行為之程序)依機關任務及業務功能,完成 指派任務所需之授權存取。		無要求。		最小權限	採最小權限原則,僅允許使用者(或代表使用 者行為之程序)依機關任務及業務功能,完成 指派任務所需之授權存取。		無要求。
	遠端存取	一、應監控資通系統遠 二、資通系統遠端存取 三、資通系統遠端存取 定義及管理之存取 四、等級「普」之所有	密機制。 之來源應為機關已預先 控制點。	對於每一種允許之遠 時期型,均應先取 得授權,建立使用限 制、組態需求、連線需 求及文件化,使用者之 權限檢查作業應於 服器端完成。		遠端存取	一、應監控資通系統遠 二、資通系統遠端存即 三、資通系統遠端存取 定義及管理之存取 四、等級「普」之所有	密機制。 之來源應為機關已預先 控制點。	對於每一種允許之遠 常存取類型,均應先取 得授權,建立使用限 制、組態需求、連線需 求及文件化,使用者之 權限檢查作業應於 服器端完成。
稽核與 可歸責 性	稽核事 件	一、應定期審查稽核事件。 二、等級「普」之所有控制措施。		一、依規定時間週期 及紀錄留存政策, 保留稽核紀錄。 二、確保資通系統有 稽核特定事件之	稽核與 可歸責	一般板里	一、應定期審查稽核事 二、等級「普」之所有		四、依規定時間週期 及紀錄留存政策, 保留稽核紀錄。 五、確保資通系統有稽核特定事件之

			功能,並決定應稽
			核之特定資通系
			統事件。
			三、應稽核資通系統
			管理者帳號所執
			行之各項功能。
		一、資通系統產生之稽核紀錄,應依需求納入	資通系統產生之稽核
		其他相關資訊。	紀錄應包含事件類型、
		二、等級「普」之所有控制措施。	發生時間、發生位置及
	稽核紀		任何與事件相關之使
	錄內容		用者身分識別等資訊,
			並採用單一日誌紀錄
			機制,確保輸出格式之
			一致性。
	稽核儲	依據稽核紀錄儲存需求,配置稽核紀錄所需之信	皆存容量。
	存容量		
		一、機關規定需要即 資通系統於稽核處理失	效時,應採取適當之行
		時通報之稽核失 動。	
		效事件發生時,資	
	稽核處	通系統應於機關	
	理失效	規定之時效內,對	
	之回應	特定人員提出警	
		告。	
		二、等級「中」及「普」	
		之所有控制措施。	
		一、系統內部時鐘應依機關規定之時間週期與	資通系統應使用系統
		基準時間源進行同步。	內部時鐘產生稽核紀
	時戳及	二、等級「普」之所有控制措施。	錄所需時戳,並可以對
	校時		應到世界協調時間
			(UTC)或格林威治標準
			時間(GMT)。
		一、定期備份稽核紀 一、應運用雜湊或其	對稽核紀錄之存取管
	优上次	錄至與原稽核系 他適當方式之完	理,僅限於有權限之使
	稽核資	統不同之實體系 整性確保機制。	用者。
	訊之保	統。    二、等級「普」之所有	
	護	二、等級「中」之所有 控制措施。	
		控制措施。	
		一、應將備份還原,作 一、應定期測試備份	一、訂定系統可容忍
		為營運持續計畫 資訊,以驗證備份	資料損失之時間
營運持	系統備	測試之一部分。 媒體之可靠性及	要求。
續計畫	份	二、應在與運作系統 資訊之完整性。	二、執行系統源碼與
		不同處之獨立設 二、等級「普」之所有	資料備份。
		施或防火櫃中,儲 控制措施。	
	I		1

			功能,並決定應稽 核之特定資通系 統事件。
			六、應稽核資通系統 管理者帳號所執 行之各項功能。
	稽核紀錄內容	<ul><li>一、資通系統產生之稽核紀錄,應依需求納入 其他相關資訊。</li><li>二、等級「普」之所有控制措施。</li></ul>	資通系統產生之稽核 紀錄應包含事件類型、 發生時間、發生位置及 任何與事件相關之使 用者身分識別等資訊, 並採用單一日誌紀錄 機制,確保輸出格式之 一致性。
	稽核儲	依據稽核紀錄儲存需求,配置稽核紀錄所需之儲	皆存容量。
	存	一、機關規定需要即 時通報之稽核失 效事件發生時,資 通系統應於機關 規定之時效內,對 特定人員提出警 告。 二、等級「中」及「普」 之所有控制措施。 一、系統內部時鐘應依機關規定之時間週期與 基準時間源進行同步。 二、等級「普」之所有控制措施。	效時,應採取適當之行 資通系統應使用系統 強所需時戳,並可以 等所需時戳,並可時間 (UTC)或格林威治標準
	稽核資訊之保護	一、定期備份稽核紀 錄至與原稽核系 統不同之實體系 統。 二、等級「中」之所有 控制措施。	時間(GMT)。 對稽核紀錄之存取管 理,僅限於有權限之使 用者。
運持畫	系統備 份	一、應將備份還原,作 為營運持續計畫 測試之一部分。 二、應在與運作系統 不同處之獨立設 施或防火櫃中,儲	一、訂定系統可容忍 資料損失之時間 要求。 二、執行系統源碼與 資料備份。

	系統備援	存重要資通系統 軟體與其他安全 相關資訊之備份。 三、等級「中」之所有 控制措施。 一、訂定資通系統從中斷後至重新恢復服務之 可容忍時間要求。 二、原服務中斷時,於可容忍時間內,由備援設	無要求。
	內部使用 者之識別 與鑑別	備取代提供服務。  一、對帳號之網路或本 資通系統應具備唯一識別及金 機存取採取多重認 使用者行為之程序)之功能, 證技術。  二、等級「中」及「普」 之所有控制措施。	
識別與	身分驗證	一、身分驗證機制應防範自動化程式之登入或密碼更換 嘗試。 二、密碼重設機制對使用者重新身分確認後,發送一次 性及具有時效性符記。 三、等級「普」之所有控制措施。	時,應於登入後要求立
	鑑別資訊 回饋 加密模組	資通系統應遮蔽鑑別過程中之資訊。 資通系統如以密碼進行鑑別時,該密碼應加密或經雜湊	無要求。
	加鑑別 銀門 銀門 銀門 北田 北田 北田 北田 北田 北田 北田 北田 北田 北田	員通系統如以密偽進行鑑別时,該密偽應加密或經雜凑處理後儲存。 資通系統應識別及鑑別非機關使用者(或代表機關使用者	
系統與	系統發展 生命週期 需求階段	針對系統安全需求 (含機密性、可用性、完整性),以核	
服務獲得	系統發展 生命週期 設計階段	<ul><li>一、根據系統功能與要求,識別可能影響系統之威脅, 進行風險分析及評估。</li><li>二、將風險評估結果回饋需求階段之檢核項目,並提出 安全需求修正。</li></ul>	無要求。

		存重要資通系統 軟體與其他安全	
		N 超 共 元 文 主	
		三、等級「中」之所有	
		一 寸級	
		一、訂定資通系統從中斷後至重新恢復服務之	
	系統備	可容忍時間要求。	·····································
	援	二、原服務中斷時,於可容忍時間內,由備援設	
	182	一	
		一、對帳號之網路或本 資通系統應具備唯一識別及	1 濫別機關使用者(或代表機關
	內部使用	機存取採取多重認 使用者行為之程序)之功能,	禁止使用共用帳號。
	者之識別	證技術。	
	與鑑別	二、等級「中」及「普」	
		之所有控制措施。	the state of the s
		一、身分驗證機制應防範自動化程式之登入或密碼更換 嘗試。	一、使用預設密碼登入系統 時,應於登入後要求立
		性及具有時效性符記。	二、身分驗證相關資訊不以
		三、等級「普」之所有控制措施。	明文傳輸。
			三、具備帳戶鎖定機制,帳
			號登入進行身分驗證失
			續嘗試登入或使用機關
	身分驗證		自建之失敗驗證機制。
識別與	管理		四、基於密碼之鑑別資通系
鑑別			統應強制最低密碼複雜
			度;強制密碼最短及最 長之效期限制。
			五、使用者更換密碼時,至
			少不可以與前三次使用
			過之密碼相同。
			六、第四點及第五點所定措
			施,對非內部使用者, 可依機關自行規範辦
			了
	鑑別資訊	資通系統應遮蔽鑑別過程中之資訊。	
	回饋		1. T. b
	加密模組鑑別	資通系統如以密碼進行鑑別時,該密碼應加密或經雜湊 處理後儲存。	無要求。
	塩 排內部使	处理俊阔仔。   資通系統應識別及鑑別非機關使用者(或代表機關使用者。	 行為シ程序)。
	用者之識	ス で 小 で U が U は U が I が I が I が I が I が I が I が I が I が	11 11 (17)
	別與鑑別		
	系統發展	針對系統安全需求 (含機密性、可用性、完整性),以檢	核表方式進行確認。
2 h 45	生命週期		
系統與服務獲	需求階段	一、 根據系統功能與要求,識別可能影響系統之威脅,	無要求。
服扮投 得	糸統發展	進行風險分析及評估。	灬女小
-	生命週期	二、 將風險評估結果回饋需求階段之檢核項目,並提出	
	設計階段	安全需求修正。	

		一、執行「源碼掃描」安 一	· 、應針對安全需求實作必	要控制措施。
	系統發展	全檢測。	-、應注意避免軟體常見漏	洞及實作必要控制措施。
	生命週期	二、具備系統嚴重錯誤 三	、 發生錯誤時,使用者頁	面僅顯示簡短錯誤訊息及代
	用發階段	之通知機制。	碼,不包含詳細之錯誤	訊息。
	的双旧汉	三、等級「中」及「普」		
		之所有控制措施。		
	4 11 10 12	一、執行「滲透測試」安 執		
	系統發展	全檢測。		
	生命週期	<b>二、</b> 等級「中」及「普」		
	測試階段	之所有控制措施。		
		一、於系統發展生命週期之維	·運階段,須注意版本控制	一、於部署環境中應針對相
	系統發展	與變更管理。	CITIC MENONATEN	關資通安全威脅,進行
	生命週期	二、等級「普」之所有控制措	上始。	更新與修補,並關閉不
	部署與維	一 寸級 目」之川为征刊相	1 / WE -	必要服務及埠口。
	運階段			二、資通系統相關軟體,不
				使用預設密碼。
	系統發展	資通系統開發如委外辦理,應;	將系統發展生命週期各階段	依等級將安全需求(含機密
	生命週期	性、可用性、完整性)納入委然	外契約。	
	委外階段			
	獲得程序	開發、測試及正式作業環境應	為區隔。	無要求。
	系統文件	應儲存與管理系統發展生命週期	期之相關文件。	
		一、 資通系統應採用加 無	要求。	無要求。
		密機制,以防止未授		
		權之資訊揭露或偵		
		測資訊之變更。但傳		
		輸過程中有替代之		
		實體保護措施者,不		
		在此限。		
	傳輸之機	二、 使用公開、國際機構 驗證且未遭破解之		
系統 與	密性與完	一		
京凯保	整性	三、支援演算法最大長		
遊礼乐		<b>一 文级</b>		
哎		四、加密金鑰或憑證週		
		期性更換。		
		五、 伺服器端之金鑰保		
		管應訂定管理規範		
		及實施應有之安全		
		防護措施。		
	<b>恣</b> 刺 44 七	靜置資訊及相關具保護需 無	要求。	無要求。
	資料儲存	求之機密資訊應加密儲		
	之安全	存。		
		一、 定期確認資通系統相關漏		系統之漏洞修復應測試有
2 4t da	漏洞修復	二、 等級「普」之所有控制措		效性及潛在影響,並定期更
系統與				新。
資 訊 完 整性			一、 監控資通系統,以偵	發現資通系統有被入侵跡
正性		化工具監控進出之通	測攻擊與未授權之連	象時,應通報機關特定人
	資通系統	信流量,並於發現不	線,並識別資通系統	員。
	監控	尋常或未授權之活動	之未授權使用。	
			二、 等級「普」之所有控制	
		分析。	措施。	

	1			
		一、執行「源碼掃描」安一一	、應針對安全需求實作必	要控制措施。
	系統發展	全檢測。	、 應注意避免軟體常見漏	洞及實作必要控制措施。
	系	二、具備系統嚴重錯誤 三	、發生錯誤時,使用者頁	面僅顯示簡短錯誤訊息及代
	五 中 2 次 開發階段	之通知機制。	碼,不包含詳細之錯誤	訊息。
		三、等級「中」及「普」		
		之所有控制措施。		
	系統發展	一、執行「滲透測試」安 執	行「弱點掃描」安全檢測。	
	系	全檢測。		
	王亚迪斯   測試階段	<b>二、</b> 等級「中」及「普」		
	内叫自权	之所有控制措施。		
		一、於系統發展生命週期之維	運階段,須注意版本控制	一、於部署環境中應針對相
	系統發展	與變更管理。		關資通安全威脅,進行
	生命週期	   二、等級「普」之所有控制措。	施。	更新與修補,並關閉不
	部署與維	, , , , , , , , , , , , , , , , , , , ,		必要服務及埠口。
	運階段			二、資通系統相關軟體,不
				使用預設密碼。
	系統發展	資通系統開發如委外辦理,應用		(依等級將安全需求(含機密
	生命週期	性、可用性、完整性)納入委夕	<b>外契約。</b>	
	委外階段		v —	1. T. N
	獲得程序	開發、測試及正式作業環境應為	•	無要求。
	系統文件	應儲存與管理系統發展生命週期	., ., .,	h
		一、資通系統應採用加一無	要求。	無要求。
		密機制,以防止未授		
		權之資訊揭露或偵		
		測資訊之變更。但傳		
		輸過程中有替代之		
		實體保護措施者,不		
		在此限。		
	傳輸之機	二、使用公開、國際機構		
. 6+ c5a	密性與完	驗證且未遭破解之 演算法。		
<ul><li>統與</li><li>銀訊保</li></ul>	整性			
也 机 休 隻		二、又拔供并公取八衣		
Ę		四、加密金鑰或憑證週		
		期性更換。		
		五、 伺服器端之金鑰保		
		管應訂定管理規範		
		及實施應有之安全		
		防護措施。		
	ata a sa sa sa		要求。	
	資料儲存	求之機密資訊應加密儲		, m ~ 1-
	之安全	存。		
		一、 定期確認資通系統相關漏	洞修復之狀態。	系統之漏洞修復應測試有
	漏洞修復	二、 等級「普」之所有控制措		效性及潛在影響,並定期更
系統 與		1 2 2 4 2 2 4 4 4 4 4 4 4 4 4 4 4 4 4 4		新。
資訊完		一、 資通系統應採用自動 一	<ul><li>- 、 監控資通系統,以負</li></ul>	發現資通系統有被入侵跡
<b>隆性</b>		化工具監控進出之通	測攻擊與未授權之連	象時,應通報機關特定人
	資通系統	信流量,並於發現不	線,並識別資通系統	員。
	監控	尋常或未授權之活動	之未授權使用。	
	1		-、 等級「普」之所有控制	
		时/到到孩尹什连们   一	- ` 寸級 百 ] 【川月往时	

	二、 等級「中」之所有控制		
	措施。		
	一、 應定期執行軟體與資	一、使用完整性驗證工	無要求。
	訊完整性檢查。	具,以偵測未授權變	
	二、 等級「中」之所有控制	更特定軟體及資訊。	
	措施。	二、 使用者輸入資料合法	
軟體及資		性檢查應置放於應用	
訊完整性		系統伺服器端。	
		三、 發現違反完整性時,	
		資通系統應實施機關	
		指定之安全保護措	
		施。	

#### 備註:

- 一、靜置資訊,指資訊位於資通系統特定元件,例如儲存設備上之狀態,或與系統相關需要 保護之資訊,例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符 內容等資訊。
- 二、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內, 另行訂定其所管特定非公務機關之系統防護基準。

		ニ、	等級「中」之所有控制			
			措施。			
		<b>-</b> \	應定期執行軟體與資	1	使用完整性驗證工	無要求。
			訊完整性檢查。		具,以偵測未授權變	
		二、	等級「中」之所有控制		更特定軟體及資訊。	
			措施。	二、	使用者輸入資料合法	
ا ا	軟體及資				性檢查應置放於應用	
	訊完整性				系統伺服器端。	
				三、	發現違反完整性時,	
					資通系統應實施機關	
					指定之安全保護措	
					施。	

#### 備註:

- 一、靜置資訊,指資訊位於資通系統特定元件,例如儲存設備上之狀態,或與系統相關需要保護之資訊,例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符內容等資訊。
- 二、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內, 另行訂定其所管特定非公務機關之系統防護基準。

## 資通安全責任等級分級辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定

第一條 本辦法依資通安全管理法(以	明定本辨法訂定之依據。
下簡稱本法)第七條第一項規定訂	
定之。	
第二條 公務機關及特定非公務機關	一、明定公務機關及特定非公務機關
(以下簡稱各機關)之資通安全責任	(以下簡稱各機關)之資通安全責
等級,由高至低,分為A級、B級、C	任等級,由高至低,分為 A 級至 E
級、D級及E級。	級。
	二、有關資通安全責任等級之核定方式、

第三條 主管機關應每二年核定自身資 通安全責任等級。

條文

行政院直屬機關應每二年提交自 身、所屬或監督之公務機關及所管之 特定非公務機關之資通安全責任等 級,報主管機關核定。

直轄市、縣(市)政府應每二年提交自身、所屬或監督之公務機關,與所轄鄉(鎮、市)、直轄市山地原住民區公所及其所屬或監督之公務機關之資通安全責任等級,報主管機關核定。

直轄市及縣(市)議會、鄉(鎮、市)民代表會及直轄市山地原住民區 民代表會應每二年提交自身資通安全 責任等級,由其所在區域之直轄市、縣 (市)政府彙送主管機關核定。

總統府、國家安全會議、立法院、司法院、考試院及監察院應每二年核 定自身、所屬或監督之公務機關及所 管之特定非公務機關之資通安全責任 等級,送主管機關備查。

各機關因組織或業務調整,致須 變更原資通安全責任等級時,應即依 前五項規定程序辦理等級變更;有新 設機關時,亦同。

第一項至第五項公務機關辦理資 通安全責任等級之提交或核定,就公 務機關或特定非公務機關內之單位, 一、第一項明定主管機關應每二年核定 自身之資通安全責任等級。

區分原則及認定等級之其他考量因 素,依第三條至第十條規定為之。

說明

- 三、各機關之資通安全責任等級如因應 組織或業務調整,致須配合變更者, 應即依第一項至第五項規定辦理其 等級變更事宜;有新設機關時,亦應 立即辦理該機關資通安全責任等級 之認定,爰為第六項規定。
- 四、考量各機關可能有特定內部單位業 務性質特殊,其辦理資通安全維護 業務相較同機關之其他單位,須為 更嚴格要求之情形,此時宜單獨將

認有另列與該機關不同等級之必要 者,得考量其業務性質,依第四條至第 十條規定認定之。

- 該單位之資通安全責任等級分級為 不同之處理,爰為第七項規定。
- 第四條 各機關有下列情形之一者,其 資通安全責任等級為 A 級:
  - 一、業務涉及國家機密。
  - 二、業務涉及外交、國防或國土安全 事項。
  - 三、業務涉及全國性民眾服務或跨公 務機關共用性資通系統之維運。
  - 四、業務涉及全國性民眾或公務員個 人資料檔案之持有。
  - 五、屬公務機關,且業務涉及全國性 之能源、水資源、通訊傳播、交 通、銀行與金融、緊急救援事項。
  - 六、屬關鍵基礎設施提供者,且業務 經中央目的事業主管機關考量其 提供或維運關鍵基礎設施服務之 用戶數、市場占有率、區域、可 替代性,認其資通系統失效或受 影響,對社會公共利益、民心士 氣或民眾生命、身體、財產安全 將產生災難性或非常嚴重之影 響。
  - 七、屬公立醫學中心。

- 一、明定各機關資通安全責任等級應列 為 A 級之情形。於該等情形,因其 機關業務所涉重要性或機敏性較 高,具有較高之資通安全風險,爰應 予以較高程度之資通安全維護責 任。
- 二、第三款所稱全國性,指含括全國之 地域範圍;所稱跨公務機關共用性 資通系統,指單一公務機關主責設 置、維護或開發伺服器、網路通訊服 務之機房設施或其他資通系統,其 餘公務機關僅為該資通系統之使用 者之情形。
- 三、第四款所稱全國性民眾或公務員個 人資料檔案,指含括全國地域範圍 內之絕大部分民眾或公務員之個人 資料檔案。

- 資通安全責任等級為B級:
  - 一、業務涉及公務機關捐助或研發之 敏感科學技術資訊之安全維護及 管理。
  - 二、業務涉及區域性、地區性民眾服 務或跨公務機關共用性資通系統 之維運。
  - 三、業務涉及區域性或地區性民眾個 人資料檔案之持有。
  - 四、屬公務機關,且業務涉及區域性 或地區性之能源、水資源、通訊 傳播、交通、銀行與金融、緊急 救援事項。
  - 五、屬關鍵基礎設施提供者,且業務 經中央目的事業主管機關考量其 提供或維運關鍵基礎設施服務之 用戶數、市場占有率、區域、可 替代性,認其資通系統失效或受

- 第五條 各機關有下列情形之一者,其一、明定各機關資通安全責任等級應列 為 B 級之情形。於該等情形,其機 關業務所涉重要性或機敏性雖較第 四條所定情形為低,惟亦具有相當 之資通安全風險,爰應予以相當之 資通安全維護責任。
  - 二、第二款所稱區域性,指跨直轄市、縣 (市)之地域範圍;所稱地區性,指 單一直轄市或縣(市)之地域範圍; 所稱跨公務機關共用性資通系統, 如第四條說明二。
  - 三、 第三款所稱區域性或地區性民 眾個人資料檔案,指含括跨直轄市、 縣(市)或單一直轄市、縣(市)地 域範圍內之絕大部分民眾之個人資 料檔案。

影響,對社會公共利益、民心士 氣或民眾生命、身體、財產安全 將產生嚴重影響。

六、屬公立區域醫院或地區醫院。

第六條 各機關維運自行或委外開發之 資通系統者,其資通安全責任等級為 C 級。 各機關倘無第四條或第五條規定之情 形,而有維運自行或委外開發之資通系 統者,資通安全風險較有前二條所列情 形之機關為低,其資通安全責任等級應 列為C級,爰為本條規定。

第七條 各機關自行辦理資通業務,未 維運自行或委外開發之資通系統者, 其資通安全責任等級為 D 級。 考量各機關如屬自行辦理資通業務,未 維運自行或委外開發之資通系統,其資 通安全風險較低,其資通安全責任等級 應列為 D級,爰為本條規定。本條及第 八條所定資通業務,包含資通系統之維 運及資通服務之提供等業務。

- 第八條 各機關有下列情形之一者,其 資通安全責任等級為E級:
  - 一、無資通系統且未提供資通服務。
  - 二、屬公務機關,且其全部資通業務 由其上級或監督機關兼辦或代 管。
  - 三、屬特定非公務機關,且其全部資 通業務由其中央目的事業主管機 關、中央目的事業主管機關所屬 公務機關,或中央目的事業主管 機關所管特定非公務機關兼辦或 代管。

考量各機關如無資通系統且未提供資通 服務,或全部資通業務由其上級或監督 機關、中央目的事業主管機關、中央目的 事業主管機關所屬公務機關或中央目的 事業主管機關所管特定非公務機關 或代管,其資通安全風險較第四條至第 也條所定情形更低,資通安全責任等級 應列為E級,爰為本條規定。

第九條 各機關依第四條至前條規定, 符合二個以上之資通安全責任等級 者,其資通安全責任等級列為其符合 之最高等級。 為避免各機關依第四條至第八條規定認 定資通安全責任等級時,可能有符合二 個以上之資通安全責任等級之情形,於 辦理其等級之提交或核定將發生疑義, 爰明定有上開情形者,應列為其符合之 最高等級。

- 第十條 各機關之資通安全責任等級依 前六條規定認定之。但第三條第一項 至第五項之公務機關提交或核定資通 安全責任等級時,得考量下列事項對 國家安全、社會公共利益、人民生命、 身體、財產安全或公務機關聲譽之影 響程度,調整各機關之等級:
  - 一、業務涉及外交、國防、國土安全、 全國性、區域性或地區性之能 源、水資源、通訊傳播、交通、

有關各機關資通安全責任等級之認定, 除第四條至第八條規定外,因業務機 性、個人資料檔案之數量等不同因素,仍 可能有其他應考量事項,而有調整分 可能有其他應考量事項,而有調整分項 必要。為利第三條第一項至第五項 公務機關於提交或核定資通安全責任等 級時,得有調整之彈性,爰為本條規 多機關資通安全責任等級之認定,例外 數應依第四條至第九條規定予以適當調 得視實務狀況,依本條規定予以適當 銀行與金融、緊急救援與醫院業務者,其中斷或受妨礙。

- 二、業務涉及個人資料、公務機密或 其他依法規或契約應秘密之資 訊者,其資料、公務機密或其他 資訊之數量與性質,及遭受未經 授權之存取、使用、控制、洩漏、 破壞、竄改、銷毀或其他侵害。
- 三、 各機關依層級之不同,其功能受 影響、失效或中斷。
- 四、 其他與資通系統之提供、維運、 規模或性質相關之具體事項。

第十一條 各機關應依其資通安全責任 等級,辦理附表一至附表八之事項。

各機關辦理附表一至附表八所定 事項或執行附表十所定控制措施,因 技術限制、個別資通系統之設計、結構 或性質等因素,就特定事項或控制措 施之辦理或執行顯有困難者,得經 三條第二項至第四項所定其等級核定機 關同意,並報請主管機關備查後,免執 行該事項或控制措施。

公務機關之資通安全責任等級為 A級或B級者,應依主管機關指定之 方式,提報第一項及第二項事項之辦 理情形。

中央目的事業主管機關得要求所 管特定非公務機關,依其指定之方式 提報第一項及第二項事項之辦理情 形。 整其等級。

- 一、考量不同資通安全責任等級之機 關,其業務所涉範圍與機敏性等有 所不同,資通安全風險程度亦有所 差異,爰於第一項規定各機關應依 其資通安全責任等級辦理附表一 至附表八之事項,並於第二項明定 各機關自行或委外開發之資通系 統應依附表九及附表十辦理資通 系統分級及控制措施。另關鍵基礎 設施提供者之中央目的事業主管 機關考量特定類型資通系統之性 質,例如特定用途之工業控制系統 (Industrial Control Systems, ICS), 認有對之另定防護基準之必要者, 宜使其得衡酌實務需求,於充分考 量附表十所定各項控制措施於此 類系統之適用性後,自行擬訂防護 基準,並報請主管機關核定後,依 其規定辦理,爰於第二項後段明定 之。

	並報請主管機關備查後,得免執行
	該事項或控制措施。
	三、 資通安全責任等級為 A 級或 B 級
	之公務機關,宜強化對該等機關資
	通安全維護情形之管考,爰於第四
	項明定其應依主管機關指定之方
	式,提報第一項及第二項所定事項
	之辦理情形。
	四、考量特定非公務機關資通安全維
	護情形之管考,宜由其中央目的事
	業主管機關執行,爰為第五項規
	定。
第十二條 本辦法之施行日期,由主管	明定本辦法之施行日期,由主管機關定
機關定之。	之。

### 四、資通安全事件通報及應變辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號今修正 第六條、第十三條、第二十一條修正條文對照表

#### 修正條文

# 現行條文

#### 說明

- 第六條 公務機關知悉 資通安全事件後,應依 下列規定時間完成損 害控制或復原作業,並 依主管機關指定之方 式及對象辦理通知事 宜:
  - 一、第一級或第二級資 通安全事件,於知 悉該事件後七十 二小時內。
  - 二、第三級或第四級資 通安全事件,於知 悉該事件後三十 六小時內。

公務機關依前項 規定完成損害控制或 復原作業後,應持續進 行資通安全事件之調 查及處理,並於一個月 內依主管機關指定之 方式,送交調查、處理 及改善報告。

前項調查、處理及 改善報告送交之時限, 得經上級或監督機關 及主管機關同意後延 長之。

上級、監督機關或 主管機關就第一項之 損害控制或復原作業 及第二項送交之報告, 認有必要,或認有違反 法令、不適當或其他須 改善之情事者,得要求 公務機關提出說明及

- 第六條 公務機關知悉 資通安全事件後,應依 害控制或復原作業,並 依主管機關指定之方 式及對象辦理通知事 宜:
  - 一、第一級或第二級資 通安全事件,於知 悉該事件後七十 二小時內。
  - 二、第三級或第四級資 通安全事件,於知 悉該事件後三十 六小時內。

公務機關依前項 規定完成損害控制或 復原作業後,應持續進 行資通安全事件之調 查及處理,並於一個月 內依主管機關指定之 方式,送交調查、處理 及改善報告。

前項調查、處理及 改善報告送交之時限, 得經上級或監督機關 及主管機關同意後延 長之。

上級、監督機關或 主管機關就第二項之 調查、處理及改善報告 認有必要,或認有違反 法令、不適當或其他須 改善之情事者,得要求 公務機關提出說明及 調整。

- 一、第一項至第三項未 修正。
- 下列規定時間完成損 二、考量公務機關知悉 資通安全事件後之 損害控制或復原作 業辦理情形,亦可 能影響事件處理結 果,宜使該管機關 對其處理情形有監 督機制,爰修正第 四項規定。

調整。

- - 一、第一級或第二級資 通安全事件,於知 悉該事件後七十 二小時內。
  - 二、第三級或第四級資 通安全事件,於知 悉該事件後三十 六小時內。

前項調查、處理及 改善報告送交之時限, 得經中央目的事業主 管機關同意後延長之。

特定非公務機關 就第三級或第四交之 通安全事件送交之調 查、處理及改善報告, 中央目的事業主管機 關應於審查後送交主

- - 一、第一級或第二級資 通安全事件,於知 悉該事件後七十 二小時內。
  - 二、第三級或第四級資 通安全事件,於知 悉該事件後三十 六小時內。

前項調查、處理及 改善報告送交之時限, 得經中央目的事業主 管機關同意後延長之。

- 一、第一項至第三項及 第五項未修正。

_					
管機	關;主管機關就該	報告認有必要	要,或認有		
報告	認有必要,或認有	違反法令、不	適當或其		
違反	法令、不適當或其	他須改善之人	青事者,得		
他須	改善之情事者,得	要求特定非	公務機關		
要求	特定非公務機關	提出說明及詞	<b>周整</b> 。		
提出	說明及調整。				
第二十	一條 本辦法	第二十一條	本辨法	- `	第一項未修正。
之施	行日期,由主管機	之施行日期	由主管	二、	增訂第二項,定明
關定	之。	機關定之。			本辦法修正條文之
	本辦法修正條文				施行日期。
自發	布日施行。				

## 資通安全事件通報及應變辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定

條文 説明 第一章 總則 章名。 第一條 本辦法依資通安全管理法(以 明定本辦法訂定之依據。 下簡稱本法)第十四條第四項及第十 八條第四項規定訂定之。

第二條 資通安全事件分為四級。

公務機關或特定非公務機關(以下簡稱各機關)發生資通安全事件, 有下列情形之一者,為第一級資通安 全事件:

- 一、 非核心業務資訊遭輕微洩漏。
- 二、 非核心業務資訊或非核心資通 系統遭輕微竄改。
- 三、非核心業務之運作受影響或停頓,於可容忍中斷時間內回復 正常運作,造成機關日常作業 影響。

各機關發生資通安全事件,有下 列情形之一者,為第二級資通安全事 件:

- 一、非核心業務資訊遭嚴重洩漏,或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。
- 二、非核心業務資訊或非核心資通 系統遭嚴重竄改,或未涉及關 鍵基礎設施維運之核心業務資 訊或核心資通系統遭輕微竄 改。
- 三、非核心業務之運作受影響或停 頓,無法於可容忍中斷時間內 回復正常運作,或未涉及關鍵 基礎設施維運之核心業務或核 心資通系統之運作受影響或停 頓,於可容忍中斷時間內回復 正常運作。

各機關發生資通安全事件,有下 列情形之一者,為第三級資通安全事 件:

一、未涉及關鍵基礎設施維運之核 心業務資訊遭嚴重洩漏,或一

- 二、所定核心業務,依資通安全管理 法施行細則第七條第一項之規 定認定;所定核心資通系統,依 該細則第七條第二項之規定認 定,併予敘明。
- 三、所稱一般公務機密,參考行政院 訂定之文書處理手冊第五十一 點規定,係指公務機關持有或 保管之資訊,除國家機密外,依 法令或契約有保密義務者。
- 四、所稱敏感資訊,指包含個人資料 等非一般公務機密或國家機密 之資訊,如遭洩漏可能造成機 關本身或他人之損害或困擾, 而具保護價值之資訊。
- 五、所稱國家機密,依國家機密保護 法第二條規定,指為確保國家 安全或利益而有保密之必要, 對政府機關持有或保管之資 訊,經依該法核定機密等級者。

般公務機密、敏感資訊或涉及 關鍵基礎設施維運之核心業務 資訊遭輕微洩漏。

- 二、未涉及關鍵基礎設施維運之核 心業務資訊或核心資通系統遭 嚴重竄改,或一般公務機密、敏 感資訊、涉及關鍵基礎設施維 運之核心業務資訊或核心資通 系統遭輕微竄改。
- 三、未涉及關鍵基礎設施維運之核 心業務或核心資通系統之運作 受影響或停頓,無法於可容忍 中斷時間內回復正常運作,核 對及關鍵基礎設施維運之運作 業務或核心資通系統之運作時 影響或停頓,於可容忍中斷時 間內回復正常運作。

各機關發生資通安全事件,有下 列情形之一者,為第四級資通安全事 件:

- 一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏,或國家機密遭洩漏。
- 二、一般公務機密、敏感資訊、涉及 關鍵基礎設施維運之核心業務 資訊或核心資通系統遭嚴重竄 改,或國家機密遭竄改。
- 三、涉及關鍵基礎設施維運之核心 業務或核心資通系統之運作受 影響或停頓,無法於可容忍中 斷時間內回復正常運作。
- 第三條 資通安全事件之通報內容,應 包括下列項目:
  - 一、發生機關。
  - 二、 發生或知悉時間。
  - 三、 狀況之描述。
  - 四、等級之評估。
  - 五、 因應事件所採取之措施。
  - 六、 外部支援需求評估。
  - 七、其他相關事項。
- 第二章 公務機關資通安全事件之通 報及應變

第四條 公務機關知悉資通安全事件

為強化資通安全事件之管理、追蹤 及加速處理之效率,爰明定各機關 辦理資通安全事件通報作業之基本 通報項目。

章名。

一、第一項明定公務機關辦理資通

後,應於一小時內依主管機關指定之 方式及對象,進行資通安全事件之通 報。

前項資通安全事件等級變更時, 公務機關應依前項規定,續行通報。

公務機關因故無法依第一項規 定方式通報者,應於同項規定之時間 內依其他適當方式通報,並註記無法 依規定方式通報之事由。

公務機關於無法依第一項規定 方式通報之事由解除後,應依該方式 補行通報。

- 安全事件之通報,應於知悉後 一小時內依主管機關指定之方 式及對象為之。

- 四、第四項明定公務機關於阻礙其 依指定方式通報之事由解除 後,仍應依主管機關指定之方 式補行通報。
- 第五條 主管機關應於其自身完成資 通安全事件之通報後,依下列規定時 間完成該資通安全事件等級之審核, 並得依審核結果變更其等級:
  - 一、通報為第一級或第二級資通安 全事件者,於接獲後八小時內。
  - 二、通報為第三級或第四級資通安 全事件者,於接獲後二小時內。

總統府與中央一級機關之直屬機關及直轄市、縣(市)政府,應於其自身、所屬、監督之公務機關、所轄鄉(鎮、市)、直轄市山地原住民,以所與其所屬或監督之公務機關,民區以所與其所屬或監督之公務機關,民區以前開鄉(鎮、市)、直轄市山地原民及前開鄉(鎮、市)、直轄市山地原民民稅表會,完成資通安全事件之通安保務後,並得依審核結果

一、考量公務機關於進行資通安全 事件之通報時,因受限於時間 急迫或其他因素,就資通安全 事件等級之判斷或有不適當之 情形, 爰於第一項明定主管機 關對於其自身資通安全事件之 審核,並於第二項規範總統府 與中央一級機關之直屬機關及 直轄市、縣(市)政府,應於其 自身、所屬、監督之公務機關、 所轄鄉(鎮、市)、直轄市山地 原住民區公所與所屬或監督之 公務機關,及前開鄉(鎮、市)、 直轄市山地原住民區民代表 會,通報資通安全事件後,依規 定之時限完成對該資通安全事 件等級之審核, 並得依審核結 變更其等級。

前項機關依規定完成資通安全 事件等級之審核後,應於一小時內將 審核結果通知主管機關,並提供審核 依據之相關資訊。

總統府、國家安全會議、立法院、 司法院、考試院、監察院及直轄市、 縣(市)議會,應於其自身完成資通 安全事件之通報後,依第一項規定時 間完成該資通安全事件等級之審核, 並依前項規定通知主管機關及提供 相關資訊。

主管機關接獲前二項之通知後, 應依相關資訊,就資通安全事件之等 級進行覆核,並得依覆核結果變更其 等級。但主管機關認有必要,或第二 項及前項之機關未依規定通知審核 結果時,得就該資通安全事件逕為審 核,並得為等級之變更。

- 第六條 公務機關知悉資通安全事件 後,應依下列規定時間完成損害控制 或復原作業,並依主管機關指定之 方式及對象辦理通知事宜:
  - 一、第一級或第二級資通安全事件,於知悉該事件後七十二小時內。
  - 二、第三級或第四級資通安全事件,於知悉該事件後三十六小時內。

公務機關依前項規定完成損害 控制或復原作業後,應持續進行資通 安全事件之調查及處理,並於一個月 內依主管機關指定之方式,送交調 查、處理及改善報告。

前項調查、處理及改善報告送交 之時限,得經上級或監督機關及主管 機關同意後延長之。

上級、監督機關或主管機關就第

- 果變更其等級。
- 二、為使主管機關得掌握資通安全 事件之情況,以利適時提供 要協助,爰於第三項明定第二 項之機關完成資通安全事件等 級之審核後,應於一小時內將 審核結果及相關資訊通知主管 機關,以利主管機關進行後續 之覆核。
- 三、第四項明定總統府、國家安全會 議、立法院、司法院、考試院、 監察院及直轄市、縣(市)議會 資通安全事件等級之審核及通 知主管機關等程序。
- 一、第一項明定公務機關於知悉資 通安全事件後,應視該事件之 等級,於時限內完成損害控制 或復原作業及通知事宜。
- 三、為強化公務機關之資通安全管理,爰於第四項明定上級、監督機關或主管機關就第二項之調查、處理及改善報告認為有必

二項之調查、處理及改善報告認有必要,或認有違反法令、不適當或其他 須改善之情事者,得要求公務機關提 出說明及調整。 要,或認有違法或不當等情事者,得要求該公務機關提出說 明及調整。

第七條 總統府與中央一級機關之直 屬機關及直轄市、縣(市)政府,就 所屬、監督、所轄或業務相關之公務 機關執行資通安全事件之通報及應 變作業,應視情形提供必要支援或協 助。

主管機關就公務機關執行資通 安全事件之應變作業,得視情形提供 必要支援或協助。

公務機關知悉第三級或第四級 資通安全事件後,其資通安全長應召 開會議研商相關事宜,並得請相關機 關提供協助。

第八條 總統府與中央一級機關之直 屬機關及直轄市、縣(市)政府關 於其自身、所屬或監督之公務機關 所轄鄉(鎮、市)、直轄市山地原係 區公所與其所屬或監督之公務機關 及前開鄉(鎮、市)、直轄市山地原 民區民代表會,應規劃及辦理資 全演練作業,並於完成後 內,將執行情形及成果報告送交主 管機關。

前項演練作業之內容,應至少包 括下列項目:

- 一、每半年辦理一次社交工程演 練。
- 二、 每年辦理一次資通安全事件通 報及應變演練。

總統府與中央一級機關及直轄

- 二、總統府與中央一級機關及直轄 市、縣(市)議會,亦應辦理資

市、縣(市)議會,應依前項規定規 劃及辦理資通安全演練作業。

- 通安全演練作業,以利資通安 全事件發生時得妥為應對,爰 為第三項規定。
- 第九條 公務機關應就資通安全事件 之通報訂定作業規範,其內容應包括 下列事項:
  - 一、 判定事件等級之流程及權責。
  - 二、事件之影響範圍、損害程度及 機關因應能力之評估。
  - 三、資通安全事件之內部通報流 程。
  - 四、 通知受資通安全事件影響之其 他機關之方式。
  - 五、 前四款事項之演練。
  - 六、資通安全事件通報窗口及聯繫方式。
  - 七、 其他資通安全事件通報相關事 項。

為確保公務機關於知悉資通安全事件後,得依本辦法規定迅速進行通報及適當之處置,爰為本條規定。各公務機關訂定資通安全事件之通報作業規範時,應考量其機關特性、資源及其他需求等因素,依本條規定為之。

- 第十條 公務機關應就資通安全事件 之應變訂定作業規範,其內容應包括 下列事項:
  - 一、 應變小組之組織。
  - 二、 事件發生前之演練作業。
  - 三、 事件發生時之損害控制機制。
  - 四、 事件發生後之復原、鑑識、調查 及改善機制。
  - 五、 事件相關紀錄之保全。
  - 六、 其他資通安全事件應變相關事 項。

為確保公務機關於發生資通安全事件後,得依本辦法規定迅速且確實 進行資通安全事件之應變,爰為本 條規定。

- 第三章 特定非公務機關資通安全事 件之通報及應變
- 第十一條 特定非公務機關知悉資通安 全事件後,應於一小時內依中央目的 事業主管機關指定之方式,進行資通 安全事件之通報。

前項資通安全事件等級變更時, 特定非公務機關應依前項規定,續行 通報。

特定非公務機關因故無法依第 一項規定方式通報者,應於同項規定 之時間內依其他適當方式通報,並註 記無法依規定方式通報之事由。

特定非公務機關於無法依第一項規定方式通報之事由解除後,應依

#### 章名。

- 一、第一項明定特定非公務機關辦 理資通安全事件通報之方式與 時限。

該方式補行通報。

- 第一項規定續行通報。
- 四、第四項明定特定非公務機關於 阻礙其依指定方式通報之事由 解除後,仍應依中央目的事業 主管機關指定之方式補行通 報。
- 第十二條 中央目的事業主管機關應於 特定非公務機關完成資通安全事件 之通報後,依下列規定時間完成該資 通安全事件等級之審核,並得依審核 結果變更其等級:
  - 一、通報為第一級或第二級資通安 全事件者,於接獲後八小時內。
  - 二、通報為第三級或第四級資通安 全事件者,於接獲後二小時內。 中央目的事業主管機關依前項

規定完成資通安全事件之審核後,應依下列規定辦理:

- 一、審核結果為第一級或第二級資 通安全事件者,應定期彙整審 核結果、依據及其他必要資訊, 依主管機關指定之方式送交主 管機關。
- 二、審核結果為第三級或第四級資 通安全事件者,應於審核完成 後一小時內,將審核結果、依據 及其他必要資訊,依主管機關 指定之方式送交主管機關。

主管機關接獲前項資料後,得就 資通安全事件之等級進行覆核,並得 為等級之變更。

- 三、第三項明定主管機關接獲中央 目的事業主管機關送交之資通 安全事件審核資料後,得就資 通安全事件之等級進行覆核, 並為等級變更。

第十三條 特定非公務機關知悉資通安

一、第一項明定特定非公務機關於

全事件後,應依下列規定時間完成損 害控制或復原作業,並依中央目的 事業主管機關指定之方式辦理通知 事宜:

- 一、第一級或第二級資通安全事件,於知悉該事件後七十二小時內。
- 二、第三級或第四級資通安全事件,於知悉該事件後三十六小時內。

特定非公務機關依前項規定完成損害控制或復原作業後,應持續進行事件之調查及處理,並於一個月內依中央目的事業主管機關指定之方式,送交調查、處理及改善報告。

前項調查、處理及改善報告送交 之時限,得經中央目的事業主管機關 同意後延長之。

中央目的事業主管機關就第二項之調查、處理及改善報告認有必要,或認有違反法令、不適當或其他 須改善之情事者,得要求特定非公務 機關提出說明及調整。

特定非公務機關就第三級或第四級資通安全事件送交之調查、處理 及改善報告,中央目的事業主管機關 應於審查後送交主管機關;主管機關 就該報告認有必要,或認有違反法 令、不適當或其他須改善之情事者, 得要求特定非公務機關提出說明及 調整。

第十四條 中央目的事業主管機關就所 管特定非公務機關執行資通安全事 件之通報及應變作業,應視情形提供 必要支援或協助。

主管機關就特定非公務機關執 行資通安全事件應變作業,得視情形 提供必要支援或協助。

特定非公務機關知悉第三級或 第四級資通安全事件後,應召開會議 研商相關事宜。

- 知悉資通安全事件後,應視該 事件之等級,於時限內完成損 害控制或復原作業及通知事 官。

- 利各特定非公務機關順利完成 相關作業。
- 二、考量第三級或第四級資通安全 事件影響層面、可能發生之損 害皆較嚴峻,爰於第三項明定 特定非公務機關應召開會議研 商相關事官。
- 第十五條 特定非公務機關應就資通安 全事件之通報訂定作業規範,其內容 應包括下列事項:
  - 一、 判定事件等級之流程及權責。
  - 二、事件之影響範圍、損害程度及 機關因應能力之評估。
  - 三、資通安全事件之內部通報流程。
  - 四、 通知受資通安全事件影響之其 他機關之時機及方式。
  - 五、 前四款事項之演練。
  - 六、資通安全事件通報窗口及聯繫方式。
  - 七、 其他資通安全事件通報相關事項。

為確保特定非公務機關於知悉資通 安全事件後,得依本辦法規定迅速 進行事件之通報及適當之處置,爰 為本條規定。

- 第十六條 特定非公務機關應就資通安 全事件之應變訂定作業規範,其內容 應包括下列事項:
  - 一、 應變小組之組織。
  - 二、 事件發生前之演練作業。
  - 三、事件發生時之損害控制,及向 中央目的事業主管機關請求技 術支援或其他必要協助之機 制。
  - 四、 事件發生後之復原、鑑識、調查 及改善機制。
  - 五、 事件相關紀錄之保全。
  - 六、 其他資通安全事件應變相關事 項。

為確保特定非公務機關於知悉資通 安全事件後,得依本辦法規定迅速 且確實進行資通安全事件之應變, 爰為本條規定。

#### 第四章 附則

第十七條 主管機關就各機關之第三級 或第四級資通安全事件,得召開會 議,邀請相關機關研商該事件之損害 控制、復原及其他相關事官。

#### 章名。

考量第三級與第四級資通安全事件 之影響範圍及資訊洩漏之情形較 鉅,爰明定主管機關得針對各機關 之第三級與第四級資通安全事件 (即重大資通安全事件),邀集相關 機關召開會議,就事件之損害控制、 復原及其他相關事宜進行研商,以

提升各機關對於重大資通安全事件 之處理成效,避免類似事件再次發 生。

- 第十八條 公務機關應配合主管機關規 劃、辦理之資通安全演練作業,其內 容得包括下列項目:
  - 一、 社交工程演練。
  - 二、資通安全事件通報及應變演 練。
  - 三、網路攻防演練。
  - 四、情境演練。
  - 五、 其他必要之演練。
- 第十九條 特定非公務機關應配合主管 機關規劃、辦理之資通安全演練作 業,其內容得包括下列項目:
  - 一、 網路攻防演練。
  - 二、情境演練。
  - 三、 其他必要之演練。

主管機關規劃、辦理之資通安全 演練作業,有侵害特定非公務機關 之權利或正當利益之虞者,應先經 其書面同意,始得為之。

前項書面同意之方式,依電子簽 章法之規定,得以電子文件為之。

- 考量資通安全演練作業為資通安全 事件應變之一環,為使公務機關對 於資通安全事件之預防與應變更臻 完備,爰明定公務機關應配合主管 機關規劃、辦理之資通安全演練作 業及相關項目。
- 一、考量資通安全演練作業為資通 安全事件應變之一環,為使特 定非公務機關對於資通安全, 件之預防與應變更臻完備, 於第一項明定特定非公務機關 應配合主管機關規劃、辦理之 資通安全演練作業及相關項 目。
- 三、為提升行政效率,於第三項明定 主管機關依第二項取得特定非 公務機關之書面同意時,依電 子簽章法之規定,得以電子文 件為之。
- 第二十條 公務機關於本辦法施行前,已 針對其自身、所屬或監督之公務機關 或所管之特定非公務機關,自行或與 其他機關共同訂定資通安全事件 報及應變機制,並實施一年以上者 程經主管機關核定後,與其所屬或監 督之公務機關或所管之特定非公務 機關繼續依該機制辦理資通安全事 件之通報及應變。

前項通報及應變機制如有變更,

應送主管機關重為核定。	二十條第四款規定裁罰之。
	二、公務機關為因應業務或實務趨
	勢等內在或外在條件之改變,
	對於資通安全事件之通報及應
	變機制可能有配合調整之需
	求,其通報及應變機制經變更
	後,內容是否妥適,仍須由主管
	機關審視決定,爰為第二項規
	定。
第二十一條 本辦法之施行日期,由主	明定本辦法之施行日期,由主管機
管機關定之。	關定之。

## 五、特定非公務機關資通安全維護計畫實施情形 稽核辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正 第三條、第六條、第十條修正條文對照表

修正條文

現行條文

說明

第三條 主管機關除因不 可抗力因素外,應每年 可抗力因素外,應每年 擇定受稽核之特定非必 務機關(以下簡稱) 核機關),並以現場實 核機關之方式,稽核其資 循安全維護計畫實施情 形。

受考機模件資歷目之資養機關時之通資率 類演管主結關時之通資率練機管主結關時之通資率練機管果結構 與實之全主業與之關機或之關機或之難與之關機或之關機或人對, 重系通與之關機或之間,重系通與之關機或之

 第三條 主管機關應每年 擇定當年度各季受稽核 之特定非公務機關(以 下簡稱受稽核機關), 以現場實地稽核 以現場實地稽核 式,稽核其資通安 護計畫實施情形。

受考機模件資歷目之資養機關時之通資率機關務資、頻演管主結關時之通資率練機管里結實之全主業與定定應要統安程成或關共因定應要統安程成或關機或之定應要統安程成或關共則之致,重系通與之關機或之定應要統安程成或關其因

- 二、第二項至第四項未 修正。

資源之適當分配或稽核 成效相關之因素。 成效相關之因素。

第六條 主管機關辦理第 三條第一項之稽核,應 依同條第二項所定考量 因素,就各受稽核機關 分別組成三人<u>以上</u>之稽 核小組。

主管機關應以書面 與稽核小組成員約定利 益衝突之迴避及保密義 務。

第二項之公務機關 代表或專家學者,有下 列情形之一者,應主動 迴避擔任該次稽核之稽 核小組成員:

三、本人目前或過去二

第六條 主管機關辦理第 三條第一項之稽核, 底同條第二項所定考量 因素,就各受稽核機關 分別組成三人至七人之 稽核小組。

主管機關應以書面 與稽核小組成員約定利 益衝突之迴避及保密義 務。

第二項之公務機關 代表或專家學者,有下 列情形之一者,應主動 迴避擔任該次稽核之稽 核小組成員:

三、本人目前或過去

一、為使稽核小組組成 人數更為彈性,以利 主管機關得配合實 務需要增列小組成 員,並考量實務上具 備稽核專業、適合擔 任稽核小組成員之 人員未必屬公務機 關人員,宜降低現行 條文所定公務機關 代表不得少於全體 成員人數三分之一 之比例,爰修正第一 項稽核小組成員人 數及第二項公務機 關代表比例之規定。 二、第三項及第四項未

修正。

左 內 仁 聯 之 縣 則	一年內仁聯內緣	
年內任職之機關	二年內任職之機	
(構)或單位,曾為	關(構)或單位,	
受稽核機關之顧	曾為受稽核機關	
問,其輔導項目與	之顧問,其輔導項	
受稽核項目相關。	目與受稽核項目	
四、其他情形足認擔任	相關。	
稽核小組成員,將	四、其他情形足認擔	
對稽核結果之公正	任稽核小組成員,	
性造成影響。	將對稽核結果之	
	公正性造成影響。	
第十條 本辦法之施行日	第十條 本辦法之施行日	一、第一項未修正。
期,由主管機關定之。	期,由主管機關定之。	二、增訂第二項,定明本
本辦法修正條文自		辨法修正條文之施
發布日施行。		行日期。

## 特定非公務機關資通安全維護計畫實施情形稽核 辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定

條文 説明
第一條 本辦法依資通安全管理法(以下 明定本辦法訂定之依據。 簡稱本法)第七條第二項規定訂定 之。 第二條 本辦法所定書面,依電子簽章法 明定本辦法所定書面,依電子簽章法之 之規定,得以電子文件為之。 規定,得以電子文件為之。

第三條 主管機關應每年擇定當年度各 季受稽核之特定非公務機關(以下簡稱 受稽核機關),並以現場實地稽核之方 式,稽核其資通安全維護計畫實施情 形。

主管機關擇定前項受稽核機關時, 應綜合考量其業務之重要性與機敏性、 資通系統之規模與性質、資通安全事件 發生之頻率與程度、資通安全演練之成 果、歷年受主管機關或中央目的事業主 管機關稽核之頻率與結果或其他與資 通安全相關之因素。

主管機關為辦理第一項稽核,應訂定稽核計畫,其內容包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及中央目的事業主管機關協助事項。

主管機關決定前項稽核之重點領 域與基準及項目時,應綜合考量我國資 通安全政策、國內外資通安全趨勢、過 往稽核計畫之內容與稽核結果,及其他 與稽核資源之適當分配或稽核成效相 關之因素。

第四條 主管機關辦理前條第一項之稽 核,應將稽核計畫於一個月前以書面通 知受稽核機關。

受稽核機關如因業務因素或有其 他正當理由,得於收受前項通知後五日 內,以書面敘明理由向主管機關申請調 整稽核日期。

前項申請,除有不可抗力之事由 外,以一次為限。

- 一、第一項明定主管機關稽核特定非 公務機關資通安全維護計畫實施 情形之頻率。
- 二、為有效利用稽核資源,提升稽核成效,爰於第二項明定主管機關擇定 受稽核機關時應綜合考量之因素, 以決定最適之受稽核機關名單。
- 三、第三項明定主管機關為辦理第一項之稽核,應訂定稽核計畫及其內 容應包括之事項。
- 四、為使稽核作業能切合我國資通安 全政策之規劃內容,並適時反映國 內外資通安全相關趨勢,強化稽核 資源分配與成效,爰於第四項明定 主管機關於訂定稽核計畫,決定稽 核之重點領域與基準及其項目時, 應綜合考量之因素。

- 一、為避免主管機關辦理稽核影響受稽核機關之日常業務,並使受稽核機關有充裕時間預為準備,以增進稽核效能,爰於第一項明定主管機關應於實際辦理稽核之一個月前,以書面通知受稽核機關。
- 二、考量受稽核機關可能有因業務因 素或其他正當理由,難以依主管機 關所定日期配合稽核之情形,爰於 第二項及第三項明定於此情形,受 稽核機關得於收受第一項通知後

- 第五條 主管機關辦理第三條第一項之 稽核,得要求受稽核機關為資通安全 維護計畫實施情形之說明、協力或提 出相關之文件、證明資料供現場查閱, 並執行下列事項,受稽核機關及其所 屬人員應予配合:
  - 一、稽核前訪談。
  - 二、現場實地稽核。

受稽核機關依法律有正當理由,未 能為前項說明、協力或提出資料供現場 查閱者,應以書面敘明理由,向主管機 關提出。

主管機關收受前項書面後,應進行 審核,依下列規定辦理,並得停止稽核 作業之全部或一部:

- 一、認有理由者,應將審核之依據及 相關資訊記載於稽核結果報告。
- 二、 認無理由者,應要求受稽核機關 依第一項規定辦理;已停止稽核 作業者,得擇期續行辦理,並於 十日前以書面通知受稽核機關。

- 五日內,以書面敘明理由向主管機 關申請調整稽核日期,其申請除有 不可抗力之事由外,以一次為限。
- 一、本法第七條第二項明定主管機關 得稽核特定非公務機關之資通安 全維護計畫實施情形,並授權主管 機關就稽核之頻率、內容與方法及 其他相關事項之辦法,依其立法說 明,係為監督特定非公務機關實施 資通安全維護計畫之情形。從上開 法律規定及立法理由整體觀察,足 認受稽核之特定非公務機關有配 合主管機關辦理稽核之義務,主管 機關並應就稽核之內容、方法等相 關事項訂定規範,以利實務執行, **爰於第一項明定主管機關辦理第** 三條第一項之稽核時得要求受稽 核機關配合之事項,以利主管機關 藉由稽核確認受稽核機關遵循本 法之情形。
- 二、受稽核機關如依法律有正當理由, 不能為第一項之說明、配合措施或 提供資料,例如提供資料將侵害第 三人之權利或正當利益,此時受稽 核機關應以書面敘明其理由,向主 管機關提出,俾利主管機關審核及 決定是否繼續該項作業,爰為第二 項規定。
- 三、第三項明定主管機關收受受稽核 機關依第二項規定提出書面理由 後之處理。受稽核機關對主管機關 依本項第二款規定所為之決定不 服者,得依訴願法及行政訴訟法等 規定提起救濟,以維護自身權益。
- 一、為使主管機關對不同之特定非公 務機關均得妥適辦理其資通安全 維護計畫實施情形之稽核,爰於第 一項明定主管機關應考量相關因 素,就各受稽核機關分別組成稽核 小組。
- 二、考量稽核小組成員需具備之知能, 於第二項明定主管機關組成稽核 小組時應邀請之人員,以協助主管 機關進行稽核及提供專業意見。另
- 第六條 主管機關辦理第三條第一項之 稽核,應依同條第二項所定考量因素, 就各受稽核機關分別組成三人至七人 之稽核小組。

主管機關組成前項稽核小組時,應 考量稽核之需求,邀請具備資通安全政 策或該次稽核所需之技術、管理、法律 或實務專業知識之公務機關代表或專 家學者擔任小組成員,其中公務機關代 表不得少於全體成員人數之三分之一。 主管機關應以書面與稽核小組成 員約定利益衝突之迴避及保密義務。

第二項之公務機關代表或專家學者,有下列情形之一者,應主動迴避擔任該次稽核之稽核小組成員:

- 一、本人、其配偶、三親等內親屬、家屬或上開人員財產信託之受託人, 與受稽核機關或其負責人間有財 產上或非財產上之利害關係。
- 二、本人、其配偶、三親等內親屬或家屬,與受稽核機關或其負責人間, 目前或過去二年內有僱傭、承攬、 委任、代理或其他類似之關係。
- 三、本人目前或過去二年內任職之機關 (構)或單位,曾為受稽核機關之 顧問,其輔導項目與受稽核項目相 關。
- 四、其他情形足認擔任稽核小組成員, 將對稽核結果之公正性造成影響。

- 為確保稽核結果之公正性,明定公 務機關代表不得少於稽核小組全 體成員人數之三分之一。
- 三、為保障受稽核機關之權益,爰於第 三項明定主管機關應以書面與稽 核小組成員約定利益衝突之迴避 及保密義務。
- 四、為確保稽核結果之客觀性及避免 爭議,爰於第四項明定第二項之公 務機關代表或專家學者應主動迴 避擔任稽核小組成員之情形。

第七條 主管機關應於每季所定受稽核 機關之稽核作業完成後一個月內,將稽 核結果報告交付該季受稽核機關。

前項稽核結果報告之內容,應包括 稽核之範圍、缺失或待改善事項、第五 條第二項所定受稽核機關未能為說明、 協力或提出資料供現場查閱之情形、理 由與同條第三項所定主管機關審核結 果,及其他與稽核相關之必要內容。

果,及其他與稽核相關之必要內容。 第八條 受稽核機關經發現其資通安全 維護計畫實施情形有缺失或待改善者, 應於主管機關交付稽核結果報告後一 個月內,依主管機關指定之方式提出改 善報告,並送交中央目的事業主管機關 關;主管機關及中央目的事業主管機關

前項受稽核機關提出改善報告後, 應依主管機關指定之方式及時間,提出 改善報告之執行情形,並送交中央目的 事業主管機關;主管機關認有必要時, 得要求該受稽核機關進行說明或調整。

認有必要時,得要求該受稽核機關進行

說明或調整。

第九條 主管機關辦理第三條第一項之 稽核,得要求受稽核機關之中央目的事 業主管機關派員為必要協助。

- 一、第一項明定主管機關應於每季所 定受稽核機關之稽核作業均辦理 完成後之一個月內,將稽核結果報 告交付該季受稽核機關。
- 二、第二項明定稽核結果報告應記載 之內容。

明定主管機關辦理第三條第一項之稽核 時,得要求受稽核機關之中央目的事業 主管機關派員為必要協助,以利順利執

	行稽核,並使中央目的事業主管機關亦 得知悉受稽核機關之資通安全維護實施 情形。
第十條 本辦法之施行日期,由主管機關	明定本辦法之施行日期,由主管機關定
定之。	之。

## 六、資通安全情資分享辨法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

## 第三條、第十一條修正條文對照表

修正條文	現行條文	說明
第三條 主管機關應就情	第三條 主管機關應就情	一、第一項至第五項未修
資分享事宜進行國際合	資分享事宜進行國際合	正。
作。	作。	二、為鼓勵特定非公務機
主管機關應適時與	主管機關應適時與	關分享具效益之實質
公務機關進行情資分	公務機關進行情資分	情資,提升資通安全
字。	享。	聯防成效,爰增訂第
公務機關應適時與	公務機關應適時與	六項規定。
主管機關進行情資分	主管機關進行情資分	
享。但情資已依前項規	享。但情資已依前項規	
定分享或已經公開者,	定分享或已經公開者,	
不在此限。	不在此限。	
中央目的事業主管	中央目的事業主管	
機關應適時與其所管之	機關應適時與其所管之	
特定非公務機關進行情	特定非公務機關進行情	
資分享。	資分享。	
特定非公務機關得	特定非公務機關得	
與中央目的事業主管機	與中央目的事業主管機	
關進行情資分享。	關進行情資分享。	
前項分享之情資,		
<b>經中央目的事業主管機</b>		
關認定足以防止其他機		
關資通安全事件之發生		
或降低其損害者,中央		
目的事業主管機關得予		
以獎勵。		
第十一條 本辦法施行日	第十一條 本辦法施行日	一、 第一項未修正。
期,由主管機關定之。	期,由主管機關定之。	二、 增訂第二項,定明本
本辦法修正條文		辨法修正條文之施行
自發布日施行。		日期。

## 資通安全情資分享辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定

條文 説明

第一條 本辦法依資通安全管理法(以 下簡稱本法)第八條第二項規定訂定 之。 明定本辦法訂定之依據。

- 第二條 本辦法所稱資通安全情資(以下簡稱情資),指包括下列任一款內容之資訊:
  - 一、 資通系統之惡意偵察或情蒐活 動。
  - 二、 資通系統之安全漏洞。
  - 三、 使資通系統安全控制措施無效 或利用安全漏洞之方法。
  - 四、與惡意程式相關之資訊。
  - 五、 資通安全事件造成之實際損害 或可能產生之負面影響。
  - 六、用以偵測、預防或因應前五款情形,或降低其損害之相關措施。
  - 七、 其他與資通安全事件相關之技 術性資訊。
- 第三條 主管機關應就情資分享事宜 一、考量目前資通安全之攻擊可能來 進行國際合作。 自全球各地,為強化資通安全管理 主管機關應適時與公務機關進行 體系下之預警功能,於第一項明定 情資分享。 主管機關應就資通安全情資分享

公務機關應適時與主管機關進行情資分享。但情資已依前項規定分享

或已經公開者,不在此限。 中央目的事業主管機關應適時與 其所管之特定非公務機關進行情資分 享。

特定非公務機關得與中央目的事 業主管機關進行情資分享。

- 進行國際合作。 二、第二項至第五項明定主管機關與其 他公務機關及中央目的事業主管機 關與特定非公務機關進行情資分享 之規定,俾利各機關掌握情資,提升 其資通安全維護能量,以適時調整 資通安全應變機制,預防相關資通
- 三、另各機關於知悉自身之資通安全事件時,應依本法及資通安全事件通報及應變辦法之規定進行通報及應變,已達情資分享之效,爰本辦法就該等情形不再另行規範,併予敘明。

安全威脅之發生。

- 第四條 情資有下列情形之一者,不得 分享:
  - 一、 涉及個人、法人或團體營業上秘密或經營事業有關之資訊,其公開或提供有侵害公務機關、個

為避免各機關進行情資分享時,可能影響其他個人、法人或團體之權益,或有其他依法規規定應秘密或應限制、禁止公開之情形,爰參考美國 Cybersecurity Information Sharing Act of 2015,

人、法人或團體之權利或其他正 當利益。但法規另有規定,或對 公益有必要,或為保護人民生 命、身體、健康有必要,或經當 事人同意者,不在此限。

二、 其他依法規規定應秘密或應限 制、禁止公開之情形。

情資含有前項不得分享之內容 者,得僅就其他部分分享之。

SEC104(d)與政府資訊公開法第十八條 第一項第七款及第二項規定,明定不得 分享情資之範疇,並明定情資含有不得 分享之內容者,得僅就其他部分分享之。

第五條 公務機關或特定非公務機關 (以下簡稱各機關)進行情資分享, 應就情資進行分析及整合,並規劃適 當之安全維護措施,避免情資內容、 個人資料或依法規規定不得分享之資 訊外洩,或遭未經授權之存取或竄改。 為督促各機關妥適管理及運用情資,及 避免發生情資外洩、遭未經授權之存取 或竄改,或其他侵害個人、法人或團體權 益之情事,爰明定進行情資分享應就情 資為分析及整合,並應規劃適當之資通 安全維護措施,例如於分享前應遮蔽無 關之個人資料或其他依法規應予保密或 不得分享之資訊等。

第六條 各機關應就所接受之情資,辨 識其來源之可靠性及時效性,及時進 行威脅與弱點分析及研判潛在風險,

並採取對應之預防或應變措施。 第七條 各機關進行情資整合時,得依

情資之來源、接收日期、可用期間、

類別、威脅指標特性及其他適當項目 與內部情資進行關聯分析。

公務機關應就整合後發現之新型 威脅情資進行分享。

第八條 各機關應就所接收之情資,採 取適當之安全維護措施,避免情資內 容、個人資料或依法規規定不得分享 之資訊外洩,或遭未經授權之存取或 竄改。

第九條 各機關進行情資分享,應分別 依主管機關或中央目的事業主管機關 指定之方式為之。

各機關因故無法依前項規定方式 進行情資分享者,分別經主管機關或 中央目的事業主管機關同意後,得以 下列方式之一為之:

- 一、書面。
- 二、傳真。
- 三、 電子郵件。
- 四、資訊系統。
- 五、 其他適當方式。

考量各機關於進行情資分析時,應辨識 情資來源之可靠性與時效性以利及時研 判潛在風險,並採取適當之預防或應變 措施,爰為本條規定。

各機關於辦理情資整合時,應針對情資 之來源、時效、威脅指標類別、特性或其 他性質,與內部情資進行關聯分析;公務 機關於進行情資整合後,亦應就所發現 之新型威脅情資進行分享,爰為本條規 定。

考量各機關於接收其他機關分享之情資 後,應以適當方式確保情資之安全性,爰 參考 Cybersecurity Information Sharing Act of 2015, SEC104(d)之規範意旨,為本 條規定。

- 一、為確保情資分享之效率及正確性, 進行資通安全情資分享之方式宜臻 明確,爰於第一項明定各機關應遵 循之資通安全情資分享方式。
- 二、考量實務上可能發生各機關依規定 應進行情資分享,惟因故無法依第 一項規定方式辦理之情形,為使各 機關適時掌握情資,仍應循其他方 式進行情資分享,爰參考其他法規 所定提供資料之方式,於第二項明 定各機關於此情形得採取之情資分 享方式。

第十條 未適用本法之個人、法人或團體,經主管機關或中央目的事業主管機關同意後,得與其進行情資分享。

主管機關或中央目的事業主管機關同意前項個人、法人或團體進行情資分享,應以書面與其約定應遵守第四條至前條之規定。

- 一、考量未適用本法之個人、法人或團 體亦可能持有資通安全情資,爰於第 資通安全情資分享之需求,爰於第 一項明定該等個人、法人或團體經 主管機關或中央目的事業主管機關 同意後,得與其進行資通安全情資 分享。
- 二、為確保第一項與主管機關或中央目 的事業主管機關進行情資分享之個 人、法人或團體處理情資符合本辦 法相關規定,爰為第二項規定。

第十一條 本辦法施行日期,由主管機關 定之。

明定本辦法施行日期,由主管機關定之。

## 七、公務機關所屬人員資通安全事項獎懲辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定 中華民國 110 年 8 月 23 日行政院院臺護字第 1100182012 號令修正

#### 第四條、第七條修正條文對照表

#### 修正條文 現行條文 說明 第四條 有下列情形之一 第四條 有下列情形之一 一、序文及第一款至第三 者,予以懲處: 者,予以懲處: 款未修正。 一、未依本法、本法授權 一、未依本法、本法授 二、公務機關資通安全業 訂定之法規或機關 權訂定之法規或機 務倘有情節重大之違 內部規範辦理下列 關內部規範辦理下 失,其懲處對象應根 事項,情節重大: 列事項,情節重大: 據具體事實予以認 (一) 資通安全情資分 (一) 資通安全情資分 定。考量承辦業務人 享作業。 享作業。 員之長官或督導業務 之上級、監督機關人 (二) 訂定、修正及實 (二) 訂定、修正及實 員,如對業務督導不 施資通安全維護 施資通安全維護 力,致其屬員、所屬 計畫。 計畫。 (三)提出資通安全維 (三)提出資通安全維 或所監督機關之人員 護計畫實施情 護計畫實施情 有第一款至第三款情 形。 形,亦為應予懲處之 形。 對象,爰增訂第四款 (四) 辦理資通安全維 (四) 辦理資通安全維 護計畫實施情形 護計畫實施情形 規定。 之稽核。 之稽核。 (五) 配合上級或監督 (五) 配合上級或監督 機關資通安全維 機關資通安全維 護計畫實施情形 護計畫實施情形 稽核結果,提出 稽核結果,提出 改善報告。 改善報告。 (六) 訂定資通安全事 (六) 訂定資通安全事 件通報及應變機 件通報及應變機 制。 制。 (七) 資通安全事件之 (七) 資通安全事件之 通報或應變作 通報或應變作 業。 業。 (八) 提出資通安全事 (八) 提出資通安全事 件調查、處理及 件調查、處理及 改善報告。 改善報告。 二、辦理資通安全業務 二、辦理資通安全業務 經主管機關、上級 經主管機關、上級 或監督機關評定績 或監督機關評定績

效不良,經疏導無

效不良,經疏導無

效,情節重大。	效,情節重大。	
三、其他違反本法、本法	三、其他違反本法、本	
授權訂定之法規或	法授權訂定之法規	
機關內部規範之行	或機關內部規範之	
為,情節重大。	行為,情節重大。	
四、對業務督導不力,致		
其屬員、所屬或所監		
督機關之人員有前		
三款情形之一。		
第七條 本辦法之施行日	第七條 本辦法之施行日	一、第一項未修正。
期,由主管機關定之。	期,由主管機關定之。	二、增訂第二項,定明本
本辦法修正條文		辨法修正條文之施
自發布日施行。		行日期。

## 公務機關所屬人員資通安全事項獎懲辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定

	1行政院院臺護字第 1070213547 號令訂定
條文	說明
第一條 本辦法依資通安全管理法(以	明定本辦法訂定之依據。
下簡稱本法)第十五條第二項及第十	
九條第二項規定訂定之。	
第二條 公務機關就其所屬人員辦理	一、考量各公務機關之業務性質不同,
業務涉及資通安全事項之獎懲,得依	及其上級或監督機關對於其資通安
本辦法之規定自行訂定獎懲基準。	全業務具有監督管理權責,爰明定
	公務機關就其所屬人員辦理業務涉
	及資通安全事項之獎勵及懲處,得
	依本辦法之規定,自行訂定獎懲基 準。
	條第二項規定「各主管機關得依業
	務特殊需要,另訂記一大功、一大
	過之標準,報送銓敘部核備。」同條
	第三項規定「嘉獎、記功或申誡、記
	過之標準,由各機關視業務情形自
	行訂定,報請上級機關備查。 公務
	機關自行訂定資通安全事項之獎懲
	基準後,仍應依上開規定辦理,併
	予敘明。
第三條 有下列情形之一者,予以獎	明定公務機關人員辦理業務涉及資通安
勵:	全事項,應予獎勵之情形。
一、 依本法、本法授權訂定之法規或	
機關內部規範,訂定、修正及實	
施資通安全維護計畫,績效優	
良。	
二、 稽核所屬或監督機關之資通安	
全維護計畫實施情形,或辦理資	
通安全演練作業,績效優良。	
三、 配合主管機關、上級或監督機關	
辦理資通安全維護計畫實施情	
形之稽核或資通安全演練作業,	
經評定績效優良。	
四、 辦理資通安全業務切合機宜,防	
止資通安全事件之發生,避免本	
機關、其他機關或人民遭受損	
害。	
五、 主動發現新型態之資通安全弱	
點或入侵威脅,並進行資通安全	
情資分享,防止資通安全事件之	

發生或降低其損害。

- 六、積極查察資通安全維護之異狀, 即時發現重大資通安全事件,並 辦理通報及應變,防止其損害擴 大。
- 七、對資通安全業務提出具體建議 或革新方案,並經採行。
- 八、 辦理資通安全人才培育事務,有 具體貢獻。
- 九、 辦理資通安全科技之研發、整 合、應用、產學合作或產業發展 事務,有具體貢獻。
- 十、 辦理資通安全軟硬體技術規 範、相關服務及審驗機制發展 等事務,有具體貢獻。
- 十一、辦理資通安全政策、法制研析 或國際合作事務,有具體貢 獻。
- 十二、辦理其他資通安全業務有具 體功績。

第四條 有下列情形之一者,予以懲 處:

- 一、未依本法、本法授權訂定之法規 或機關內部規範辦理下列事項, 情節重大:
  - (一) 資通安全情資分享作業。
  - (二)訂定、修正及實施資通安全維護計畫。
  - (三)提出資通安全維護計畫實施情 形。
  - (四)辦理資通安全維護計畫實施情 形之稽核。
  - (五)配合上級或監督機關資通安全 維護計畫實施情形稽核結果, 提出改善報告。
  - (六)訂定資通安全事件通報及應變機制。
  - (七)資通安全事件之通報或應變作業。
  - (八)提出資通安全事件調查、處理 及改善報告。
- 二、辦理資通安全業務經主管機關、 上級或監督機關評定績效不良,

明定公務機關人員辦理業務涉及資通安 全事項,應予懲處之情形。

- 經疏導無效,情節重大。
- 三、 其他違反本法、本法授權訂定之 法規或機關內部規範之行為,情 節重大。
- 第五條 公務機關辦理其所屬人員之 平時考核,應審酌前二條所定獎勵及 懲處情形,依事實發生之原因、經處 行為之動機、目的、手段、表現 人員、表別 等因素為之;其所屬人員為 聘用人員、約僱人員或其他與機關有 僱傭關係之人員者,其獎勵及懲處之 情形並應納入續聘之參考。
- 一、為使公務機關就其所屬人員辦理資 通安全業務之情形給予適當評價, 並促進其所屬人員對於資通安全工 作之重視與投入,爰為本條規定。
- 二、所定公務機關所屬人員,除具有公務機關所屬人員,除具有公務機關所屬人員公務機關方子。 時用人員、為人員或技工人員與其有僱傭關係之人所屬, 等其他與其有僱傭關係之人所屬, 所應依本條規定,審酌其體 業務涉及資通安全事項之具體情 形,予以適當之獎勵或懲處, 入續聘之參考。
- 第六條 公務機關對所屬人員作成第 四條各款情形之懲處前,應給予當事 人申辯之機會;必要時,得就所涉資 通安全專業事項,徵詢相關專家學者 之意見。

為保障當事人權益,明定公務機關對所屬人員作成第四條各款情形之懲處前,應給予當事人申辯之機會;如涉及資通安全專業事項,必要時得徵詢相關專家學者之意見,俾妥適判斷案件情節及當事人是否應予懲處。

第七條 本辦法之施行日期,由主管機 關定之。 明定本辦法之施行日期,由主管機關定之。