

資通安全管理法施行細則修正總說明

資通安全管理法施行細則（以下簡稱本細則）自一百零七年十一月二十一日訂定發布，並定自一百零八年一月一日施行後，曾於一百十年八月二十三日修正發布施行。茲因資通安全管理法（以下簡稱本法）於一百十四年九月二十四日修正公布，並定自一百十四年十二月一日施行，為配合本法部分條文內容修正及因應實務運作所需，爰修正本細則，其修正要點如下：

- 一、 增訂本法第二條第二項定明資安專責機關為數位發展部資通安全署。（修正條文第二條）
- 二、 配合本法第三條第十款新增受政府控制之事業、團體或機構之指定程序，爰增訂中央目的事業主管機關指定前應給予其陳述意見（修正條文第四條）
- 三、 增訂本法第四條第一項第五款民間重大資通安全事件之定義（修正條文第五條）
- 四、 增訂刑法妨害電腦使用罪章之罪之前案紀錄及尚未終結之通緝案件，為受託者所屬人員辦理涉及國家機密業務之適任性查核項目。（修正條文第七條）
- 五、 增訂本法第十條第四項第三方協力機制之定義。（修正條文第八條）
- 六、 配合本法增訂特定非公務機關應置資通安全長及所屬人員辦理資通安全業務績效優良之獎勵規定，以及考量現行實務運作模式，爰修正資通安全維護計畫應包括事項之相關內容。（修正條文第九條）
- 七、 配合本法第三條第六款與第九款修正「特定財團法人」用詞，及本法第三條第六款增列受政府控制之事業、團體或機構為特定非公務機關，酌修相關文字。（修正條文第十條）
- 八、 增訂本法第十四條所定上級機關於中央機關所指情形，以符實務運作方式。（修正條文第十一條）
- 九、 配合本法增訂涉及重大資通安全事件之規定，修正相關規定。（修正條文第十三條及第十四條）

資通安全管理法施行細則修正條文對照表

修正條文	現行條文	說明
第一條 本細則依資通安全管理法(以下簡稱本法) <u>第三十四條</u> 規定訂定之。	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。	配合一百十四年九月二十四日修正公布之資通安全管理法(以下簡稱本法)，修正本細則授權訂定依據援引之條次。
第二條 本法第二條第二項所定資安專責機關為數位發展部資通安全署。		一、 <u>本條新增</u> 。 二、配合本法增訂第二條第二項，定明主管機關所指定之資安專責機關。
第三條 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。	條次變更，內容未修正。
第四條 <u>中央目的事業主管機關依本法第三條第十款規定指定受政府控制之事業、團體或機構前，應給予其陳述意見之機會</u> ；中央目的事業主管機關依本法 <u>第二十條</u> 第一項規定指定關鍵基礎設施提供者前， <u>亦同</u> 。	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。	一、條次變更。 二、配合本法第三條第十款規定，增訂前段有關受政府控制之事業、團體或機構之指定程序規範。現行條文移列為後段規定，並配合本法之修正，修正援引之條次，及酌作文字修正。
第五條 本法第四條第一項第五款所稱重大資通安全事件，指民間單位有下列情形之一者，並對社會公共利益、國民生活或經濟活動有重大影響之虞，且受社會矚目之事件： 一、核心業務資訊遭嚴重洩漏。 二、核心業務資訊或		一、 <u>本條新增</u> 。 二、配合本法第四條第一項第五款，增訂有關民間之重大資通安全事件定義，以資明確。

核心資通系統遭嚴重竄改。 三、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。		
<u>第六條</u> 公務機關或特定非公務機關（以下簡稱各機關）依本法<u>第八條第二項</u>、<u>第十六條第一項</u>、<u>第二十一條第五項</u>或<u>第二十一條第三項</u>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： 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。 <u>各機關依前項規定提出改善報告後，應依稽核機關指定之方式及時間，提出改善報告之執行情形。</u>	<u>第三條</u> 公務機關或特定非公務機關（以下簡稱各機關）依本法<u>第七條第三項</u>、<u>第十三條第二項</u>、<u>第十六條第五項</u>或<u>第十七條第三項</u>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。	一、條次變更。 二、第一項配合本法之修正，修正援引之條次。 三、第二項由現行規定後段修正移列，以明確區分改善報告及其後續之執行情形，並酌作文字修正。
<u>第七條</u> 各機關依本法<u>第十條</u>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： 二、受託者應配置充足且經適當之資格訓	<u>第四條</u> 各機關依本法<u>第九條</u>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： <u>一、受託者辦理受託業務之相關程序及環</u>	一、條次變更。 二、現行第一項第一款已提升至本法第十條第二項規範，爰予刪除，以下款次遞移，內容未修正。 三、考量妨害電腦使用犯罪與資安威脅息息相關，於受託業務涉及

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。 二、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。 三、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。 四、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。 五、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。 六、委託關係終止或解除時，應確認受託	境，應具備完善之<u>資通安全管理措施</u>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	國家機密時，對受託機關執行業務之人員進行之適任性查核項目應將刑法該罪章之罪納入，爰增訂第二項第一款，以下款次遞移。又第二項第二款現行規定之判刑確定，為含括有罪但免除其刑之情形，爰酌作修正。 四、第三項配合第一項款次調整，酌作修正。
--	---	---

者返還、移交、刪除或銷毀履行契約而持有之資料。 七、受託者應採取之其他資通安全相關維護措施。 八、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三款之適任性查核，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、<u>曾犯刑法妨害電腦使用罪章之罪，經有罪判決確定，或通緝有案尚未結案。</u> 二、曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經有罪判決確定，或通緝有案尚未結案。 三、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。 四、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。 五、其他與國家機密保	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	
---	---	--

護相關之具體項目。 第一項第三款情形，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。	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。	一、<u>本條刪除</u>。 二、配合電子簽章法第五條第二項規定，現行條文已無規範必要，爰刪除之。
第八條 本法第十條第四項所稱第三方協力機制，指主管機關、參與演練之公務機關及特定非公務機關以外，具公正性及專業性之機構。		一、<u>本條新增</u>。 二、配合本法增訂第十條第四項，爰增訂有關第三方協力機制定義，以資明確。
第九條 本法第十三條、第二十一條第二項及第二十一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、專職人力及經費之配置。 五、資通安全長之配置。	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、<u>公務機關</u>資通安全長之配置。	一、條次變更。 二、第一項修正如下： （一）配合本法之修正，修正序文援引之條次。 （二）配合本法第十八條第二項「專職人員」用詞，爰修正第四款。 （三）配合本法第二十三條增訂特定非公務機關應置資通安全長，爰刪除第五款「公務機關」等字。

六、資通系統之盤點，並標示核心資通系統及相關資產。 七、資通安全風險管理。 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、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绩效管理機制。 各機關依本法第十四條、<u>第二十一條</u>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<u>本法第十四條</u>規定收受其資通安全維護計畫實施情形之機關同意，得由收受機關或其所屬、所監督之公務機關、所轄鄉	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、<u>公務機關</u>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绩效管理機制。 各機關依本法第十二條、第十六條第二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	(四) 配合實務運作，酌修第六款文字。 (五) 考量第七款現行用詞無法涵蓋資通安全維護計畫所需之風險控管，爰酌作文字修正。 (六) 配合本法第二十六條增訂特定非公務機關對所屬人員辦理資通安全業務績效優良者應予獎勵，爰刪除第十二款「公務機關」等字。 三、第二項配合本法之修正，修正援引之條次。 四、第三項配合本法第十四條明定公務機關之資通安全維護計畫實施情形之收受機關，爰酌作文字修正。
---	---	---

<u>(鎮、市)公所、直轄市山地原住民區公所及鄉(鎮、市)民代表會、直轄市山地原住民區民代表會</u>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、所監督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。	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。	
第十條 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、各機關維運、提供關鍵基礎設施所必要之業務。 三、公營事業與<u>特定財團法人及受政府控制之事業、團體或機構</u>之主要服務或功能。 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	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。	一、條次變更。 二、考量本法納管機關受監督之強度並配合本法第三條第六款及第九款修正為「特定財團法人」，以及本法第三條第六款及第十款新增受政府控制之事業、團體或機構為特定非公務機關，爰修正現行第一項第二款及第三款之款次及相關內容。其餘款次未修正。 三、第二項未修正。

定其防護需求等級為高者。		
第十一條 本法第十四條所定上級機關，於中央機關指下列情形： 一、總統府、行政院所屬二級機關與獨立機關、考試院及監察院所屬二級機關，分別為總統府、行政院、考試院及監察院。 二、行政院、考試院及監察院所屬三級以下機關，為其所屬二級機關。 三、司法院直屬法院及法官學院，為司法院；臺灣高等法院所屬各分院、各地方法院及臺灣高雄少年及家事法院，為臺灣高等法院；福建高等法院金門分院所屬各地方法院，為福建高等法院金門分院。		一、<u>本條新增</u>。 二、為明確現行實務對資通安全維護計畫實施情形之提出與稽核，以及通報應變作業之運作情形，爰明定本法第十四條所定上級機關於中央機關之情形。 三、第三款前段所定司法院直屬法院，係指最高法院、最高行政法院、懲戒法院、臺灣高等法院、臺北高等行政法院、臺中高等行政法院、高雄高等行政法院、智慧財產及商業法院，以及福建高等法院金門分院等受司法院監督其司法行政業務之法院。
第十二條 本法第十七條第三項及第二十四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。	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。	一、條次變更。 二、配合本法之修正，修正援引之條次。

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。	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。	
<u>第十三條</u> <u>本法第十七條第五項、第十八條第二項、第二十四條第三項、第五項、第二十五條第一項與第二項規定所稱重大資通安全事件，指資通安全事件通報應變及演練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。</u>	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。	一、條次變更。 二、配合本法增訂涉及重大資通安全事件之規定，修正援引之條次，並酌作文字修正。
<u>第十四條</u> <u>主管機關、本法第十四條規定收受資通安全維護計畫實施情形之機關或中央目的事業主管機關知悉重大資通安全事件，依本法第十七條第五項、第二十四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。</u> 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	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	一、條次變更。 二、第一項配合本法第十七條第二項修正增列公務機關知悉資通安全事件時，應向主管機關及本法第十四條收受資通安全維護計畫實施情形之機關通報，及配合本法之修正，修正援引之條次，並酌作文字修正。 三、第二項及第三項未修正。

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。	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。	一、<u>本條刪除</u>。 二、現行條文已提升至本法第三十二條第三項規範，爰予刪除。
第十五條 本細則自發布日施行。	第十三條 <u>本細則之施行日期</u>，由主管機關定之。 本細則<u>修正條文</u>自發布日施行。	一、條次變更。 二、修正本細則自發布日施行，爰刪除現行第一項規定。