資通安全情資分享辦法修正條文

第一條　本辦法依資通安全管理法（以下簡稱本法）第九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），指下列各款資訊：

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。

主管機關與公務機關應互相進行情資分享。

中央目的事業主管機關與其所管之特定非公務機關應互相進行情資分享。

除主管機關或中央目的事業主管機關外，其他公務機關或特定非公務機關就已分享或公開之情資，無須再行分享。

第二項或第三項分享之情資，經主管機關或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，主管機關或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，應先進行分析及整合，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　各機關應就所接收之情資，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。

主管機關或中央目的事業主管機關得就指定之情資，通知接收情資之機關回報前項措施。

第七條　各機關得依情資之來源、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及整合。

各機關應就前項分析及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、資通系統。

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，得互相進行情資分享。

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　對於資通系統、服務或產品認有危害國家資通安全之疑慮時，依危害國家資通安全產品審查辦法辦理。

第十二條　本辦法所定之情資分享、獎勵及其他相關事項，主管機關得委任所屬數位發展部資通安全署辦理之。

第十三條　本辦法自發布日施行。