**資通安全管理法草案**

104年10月2日版

＊註記為細則或子法另訂之

|  |  |
| --- | --- |
| 法條 | 立法理由 |
| **第一章 總則** | |
| 1. 為積極推動國家資通安全政策及加速建構國家資通安全環境，以確保民眾數位生活福祉、資通安全產業發展及數位國土國家安全，特制定本法。 | 有鑑於資通科技之應用已普及至公、私部門，相對應之資通安全風險議題已引發各界之注意。為有效規劃我國之資通安全管理政策及其策略，並落實於公、私部門，以建構一個安心與安全之資通使用環境，進而確保民眾數位生活福祉、資安產業發展及數位國土國家安全，特制定本法。 |
| 1. 本法用詞，定義如下： 2. 資通系統：指蒐集、處理、控制、傳輸、儲存及流通資訊之資訊通信系統。 3. 資通安全：指防止資通系統及透過其運作之資訊免於遭受未經授權之存取、使用、控制、洩漏、破壞、修改、銷毀或其他作為，以確保其機密性、完整性及可用性。 4. 資通安全風險：指資通系統及透過其運作之資訊發生未經授權之存取、使用、控制、洩漏、破壞、修改、銷毀或其他作為之可能性及衝擊性。 5. 公務機關：指依法行使公權力之中央或地方機關或行政法人。 6. 非公務機關：指本法所稱之公務機關以外的法人或團體。 7. 關鍵基礎設施：指對國民生活及經濟活動具高度重要性之實體或虛擬資產、系統或網路，且其功能一旦停止運作或效能降低，將可能對國民生活、經濟活動、公眾安全或國家安全造成重大影響，包含能源、水資源、通訊傳播、交通、金融、緊急救援與醫院等重要設施。 | 1. 參考美國國家標準技術研究所（National Institute of Standards and Technology），定義資通系統等相關用詞。 2. 為降低法律用語之差異，爰比照個人資料保護法之規定內容，定義公務機關與非公務機關。 3. 參考美國31 CFR 800.208有關關鍵基礎設施(Critical infrastructure)之定義、日本網路資訊安全基本法有關重要社會基礎業者之定義、德國資訊科技安全法有關維生管線基礎設施之說明，定義關鍵基礎設施。 |
| 1. 本法所稱主管機關為科技部。 | 本法之主管機關。 |
| 1. 本法所定事項，主管機關及中央目的事業主管機關應就其權責範圍，針對資通安全政策之推動，主動規劃所需措施，對涉及相關機關之資通安全業務，應全力配合之。   主管機關及中央目的事業主管機關均應辦理資通安全政策相關事項；其權責劃分如下：   1. 主管機關：主管公務機關資通安全整體防護、資通安全科技發展及國際交流合作等相關事宜。 2. 教育主管機關：主管資通安全相關人才之培育、國民資通安全意識之提升等相關事宜。 3. 法務及警政主管機關：主管電腦網路犯罪防制、偵查及法制等相關事宜。 4. 通訊傳播主管機關：主管電信基礎設施安全等相關事宜。 5. 經濟主管機關：主管資通安全產業發展等相關事宜。 6. 其他資通安全政策相關事宜，由相關目的事業主管機關依職權辦理。   有關非公務機關資通安全維護業務之指導、監督及管理，由其所屬中央目的事業主管機關辦理。 | 1. 考量我國有關資通安全政策之推動所涉範圍甚廣，為俾利相關業務之推動，各相關機關應就其權責範圍，主動規劃相關措施，以落實資通安全政策。參考[山坡地保育利用條例](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=M0110006)第二條及兒童及少年福利與權益保障法第七條之體例，於本條第一項就主管機關及中央目的事業主管機關之權責為規定，俾利業務之有效分工與推動。 2. 第二項參考行政院國家資通安全會報要點有關資通安全政策之推動分工與現行各機關之職掌，訂定本法主管機關及中央目的事業主管機關之權責。 3. 第三項有關非公務機關之資通安全維護之指導、監督與管理，考量資通安全係伴隨於非公務機關日常業務與作業，故宜由其所屬事業之中央目的事業主管機關監督與管理。參考個人資料保護法第二十七條定之。 |
| 1. 公務機關或非公務機關之資通服務委外時，於本法適用範圍，應監督受託者資通安全之維護\*。   公務機關之資通服務委外時，應依資通服務之性質與資通安全防護需求，選任適當之受託者。 | 1. 為免公務機關或非公務機關因認其資通系統已委外建置、營運或維護等而疏於管理，導致資通安全事件之發生，進而損害國家安全、公共利益或個人權益等，故於第一項明定受託為資通系統建置、營運或維護等事項者，仍宜以委託機關為權責歸屬機關，以確保委託機關將對受託者為適當之監督。 2. 為降低公務機關資通服務委外所面臨之資通安全風險，爰於第二項明定公務機關應依資通服務之性質與資通安全防護需求，選任適當之受託者。 |
| 1. 主管機關得設置資通安全管理暨發展基金；其資金來源如下： 2. 政府預算程序之撥款。 3. 違反本法罰鍰之部分提撥。 4. 基金孳息收入。 5. 捐贈收入。 6. 其他有關收入。   前項基金之用途係用以支應創新、前瞻性或跨部會之資通安全支出，其範圍如下：   1. 資通安全專業人才之培育與全民資通安全意識之提升。 2. 資通安全專業人才認定標準之發展與推動。 3. 資通安全科技之研發、整合、應用、產學合作及國際交流合作之發展及推動。 4. 資通安全標準及其認驗證機制之發展及推動。 5. 資通安全軟體與設備技術規範及其審驗機制之發展及推動。 6. 電腦網路犯罪防制、偵查及相關法制之推動。 7. 資通基礎設施安全之規劃及推動。 8. 其他經核定之支出。   前二項基金收支、保管及運用辦法，由行政院定之＊。  另中央各機關及直轄市、縣 (市) 政府無法支應重大資通安全事件之復原重建等經費時，得報請行政院核定後，由資通安全管理暨發展基金補助之，其補助之時機、要件、基準、請求程序及其他相關事項之辦法，由行政院定之＊。 | 1. 為俾利資通安全政策相關事項之推動，主管機關得設置資通安全管理暨發展基金。 2. 有關本基金基金收支、保管及運用辦法，由行政院定之。 3. 參考[核子事故緊急應變法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=J0160056)第四十三條、[山坡地保育利用條例](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=M0110006)第二十八條、[水利法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=J0110001)第八十九條之一及[食品安全衛生管理法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=L0040001)第五十六條之一之體例定之。 4. 為免中央各機關及直轄市、縣 (市) 政府因遭到嚴重的資安攻擊而發生重大的資通安全事件，無法支應該事件之復原重建等經費，而造成我國資通安全防護體系之漏洞，有必要採取積極作為，補助其因應之。參考[災害防救法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=D0120014)第四十三條之體例定之。 |
| **第二章 資通安全推動組織** | |
| 1. 行政院為推動國家資通安全政策，應設國家資通安全會報，並設行政院資通安全辦公室，置專職人員，處理有關業務，其組織由行政院定之。   國家資通安全會報定期召開會議，其任務如下：   1. 國家資通安全政策之諮詢審議。 2. 國家資通安全通報應變機制之諮詢審議。 3. 國家資通安全重大計畫之諮詢審議。 4. 跨部會資通安全事務之協調及督導。 5. 其他依法令所規定事項。 | 一、為統籌並加速我國資通安全環境之建構，以強化資通安全能力，爰由行政院成立國家資通安全會報，以積極推動國家資通安全政策，並設立行政院資通安全辦公室作為幕僚單位，辦理相關業務，俾利國家資通安全會報之運行。參考[全民防衛動員準備法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=F0070013)第七條、災害防救法第六條、[食品安全衛生管理法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=L0040001)第二條之一定及[癌症防治法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=L0070008)第六條之體例定之。  二、為推動我國資通安全政策，國家資通安全會報定期召開會議，參考[癌症防治法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=L0070008)第六條之體例定之。  三、我國資通安全防護體系係採三級制，由國家資通安全會報審議資通安全政策與重大計畫並送行政院核定、負責跨部會資訊通信安全事務之協調及督導等事宜，爰於第二項明定國家資通安全會報之任務，俾利我國資通安全防護體系之運行。 |
| 1. 國家資通安全會報置召集人一人，由行政院院長派行政院副院長兼任之；副召集人二人，由行政院院長指派之政務委員及科技部部長兼任；協同副召集人一人，由國家安全會議諮詢委員兼任；除召集人、副召集人及協同副召集人為當然委員外，其餘委員，由行政院院長就推動資通安全有關之機關、直轄市政府副首長及學者、專家派（聘）兼之。 | 明定國家資通安全會報之組成。另，考量資通科技日新月益，資通安全防護之推進亦應與時俱進符合科技發展水準與趨勢，故應有具資通安全學識經驗之專家或學者參與本會報之運行。參考[全民防衛動員準備法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=F0070013)第八條、災害防救法第七條、[食品安全衛生管理法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=L0040001)第二條之一定及[癌症防治法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=L0070008)第八條之體例定之。 |
| 1. 主管機關承行政院之命，綜理中央行政機關及直轄市、縣 (市) 政府資通安全防護工作，並指定國家資通安全科技中心，整合與辦理資通安全防護有關業務，建立國家資通安全防護能量，並協助政府機關處理資通安全防護事宜。 | 我國資通安全防護體系係採三級制，由科技部負責公務機關資通安全防護相關工作之監督與執行，並由其所設之國家資通安全科技中心(行政法人)作為科技部之技術與行政幕僚。參考[全民防衛動員準備法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=F0070013)第八條、災害防救法第七條及[癌症防治法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=L0070008)第十條之體例定之。 |
| **第三章 公務機關資通安全管理** | |
| 1. 公務機關應依其所屬之資通安全責任等級，衡酌機關資源之合理分配，配置人員及必要資源，規劃、制定、修正及實施其資通安全維護計畫＊。   前項資通安全責任等級之分級標準、責任內容、申請等級變更及其他應遵循事項，由主管機關擬訂，報請行政院核定之。  前項資通安全責任等級之制定應衡酌政府機關層級、業務之重要性及機敏性、保有或處理之資訊種類、數量及性質、資通系統之規模及性質等條件。  公務機關得因機關裁撤（併）、組織變更、業務變更或運用之資通系統發生重大變更等事由，經主管機關報請行政院核定後，變更其所屬之資通安全責任等級。  第一項資通安全維護計畫之標準、內容與其他遵循事項，由主管機關定之。 | 1. 為確保各政府機關之資通系統蒐集、處理、傳送、儲存及流通之安全，避免因人為疏失、蓄意或自然災害等風險，致機關資通系統遭不當使用、洩漏、竄改、破壞等情事，影響及危害機關業務，應訂定及實施資通安全維護計畫，以維護其安全。參考個人資料保護法第十八條之體例定之。 2. 考量中央各機關及直轄市、縣 (市) 政府之規模與業務性質不一，故有關於其資通安全維護計畫之制定及實施亦應有程度上之不同，爰參考英國2013年10月之「政府安全分級」（Government Security Classifications）措施與我國現行「政府機關（構）資通安全責任等級分級作業規定」，明定我國公務機關資通安全維護計畫之制定及實施，應符合其所屬之資通安全責任等級。 3. 各機關單位之層級、業務、營運與機敏資料持有之程度不同，應依據其特性賦予不同之資通安全責任。 4. 有關資通安全責任等級之分級標準、責任內容、申請等級變更及其他應遵循事項，授權由主管機關擬訂，報請行政院核定之。   公務機關之資通安全責任等級宜因機關裁撤（併）、組織更改、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，以達到資安防護之最適效果。 |
| 1. 公務機關應設置資通安全長，由機關副首長兼任之，負責推動、監督機關內相關資通安全工作與事項。 | 為確保有效推動資通安全維護事項，公務機關應設置資通安全長並由其成立與督導相關推動組織。參考美國2002年聯邦資訊安全管理法（Federal Information Security Management Act of 2002）§3544定之。 |
| 1. 中央行政機關、直轄市、縣 (市) 政府及行政法人應於當年年度終了後一定期間內，就其機關資通安全維護計畫之實施情形，向主管機關提出當年度之資通安全維護計畫實施情形報告＊。   本條所定之報告義務機關、程序、格式與內容，由主管機關定之。 | 中央行政機關及直轄市、縣 (市) 政府及行政法人應每年向國家資通安全會報提出該年度之資通安全維護計畫實施情形報告，以確認各公務機關實施資通安全計畫之成效。 |
| 1. 主管機關應查核中央行政機關、直轄市、縣 (市) 政府及行政法人資通安全維護計畫之實施情形＊。   受查核之中央行政機關、直轄市、縣 (市)政府及行政法人應於查核完成次日起一定期間內，向主管機關提出查核缺失矯正預防計畫＊。  第一項之查核對象、內容及方法、第二項之缺失矯正預防計畫之內容由主管機關定之。 | 1. 主管機關應對於中央行政機關、直轄市、縣 (市) 政府及行政法人資通安全維護計畫之實施情形進行查核，以確定本法之落實。 2. 受查核機關如有缺失，應向主管機關提出缺失矯正預防計畫，以加強資通安全計畫之落實，與政府資通安全維護的強度。 3. 授權主管機關訂定相關辦法。 |
| 1. 公務機關為因應資通安全事件，應制定預防、通報及應變機制＊。   公務機關遇有重大資通安全事件者，應向主管機關通報，並應於事件發生次日起一定期間內，向主管機關提出矯正預防計畫＊。  資通安全事件如有涉及刑責之虞，相關之公務機關應妥適保全相關資料，包括但不限於數位證據及軌跡紀錄，並應通報司法機關＊。  第一項預防、通報及應變機制之內容、第二項重大資通安全事件矯正預防計畫之內容及第三項之資料保全內容及方式及其他應遵循事項，由主管機關定之。 | 1. 為即時掌控資通安全事件，並有效降低其所造成之損害，應建立資通安全事件預防、通報及應變機制。 2. 如有發生資通安全事件，公務機關應向主管機關通報並採取矯正預防措施。 3. 資通安全事件如涉及刑責之虞，公務機關應保存相關資料並通報檢警調查機關，以利事件之調查。 4. 授權主管機關訂定相關辦法。 |
| 1. 公務機關所屬人員對於所屬機關之資通安全維護績效優良者，所屬機關應予以適度之獎勵＊。   公務機關所屬人員未遵守相關資通安全義務，致國家或社會受有重大損害時，除依法追訴行為人相關刑事責任，另追究行為人、其主責機關資通安全長及相關人員之行政責任＊。  前兩項之獎懲標準與相關內容，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，爰對相關獎懲機制進行規範，以促進我國公務機關相關人員對資通安全之重視。 |
| **第四章 非公務機關資通安全管理** | |
| 1. 非公務機關保有或運用資通系統者，應採行適當之安全維護措施，以防止或降低資通安全風險之發生。   中央目的事業主管機關得指定非公務機關所提供之產品或服務，制定及實施資通安全維護計畫＊。  前項所指定之非公務機關提供之產品或服務，中央目的事業主管機關應於當年年度終了後一定期間內，就其資通安全維護業務之指導、監督與管理情形，向主管機關提出當年度之資通安全維護計畫實施情形報告＊。  第二項計畫之標準、內容與其他遵循事項，由中央目的事業主管機關定之。  第三項所定之報告義務機關、程序、格式與內容，由主管機關定之。 | 1. 鑒於非公務機關如在業務上保有或運用資通系統者，於資通系統蒐集、處理、傳送、儲存及流通過程中，因人為疏失、蓄意或自然災害等風險，而致機關資通系統遭不當使用、洩漏、竄改、破壞等情事，亦將嚴重影響及危害機關業務，故訂定非公務機關得視自身資通安全管理情形採行適當安全措施，以維護其資通安全。 2. 基於部分非公務機關所提供之產品或服務，如無店面零售業或資訊服務業，因保有大量且重要之資訊，而影響相關消費者之隱私與財產安全等，即使非屬本法所規定之關鍵基礎設施提供者，仍應負相當之安全保管責任，故應考量其組織規模及所保有之資通系統數量和內容，規劃與實施資通安全維護計畫，爰為本條之規定。 3. 有鑑於各行業均有其目的事業主管機關，而資通安全維護與該事業之經營關係密切，應屬該事業之附屬業務，宜由原各該中央目的事業主管機關一併監督管理與其業務相關之資通安全維護事項，故本法對於非公務機關資通安全維護之指導、監督及管理，採分散式管理，由各非公務機關之中央目的事業主管機關執行。爰參考個人資料保護法第二十二條立法理由定之。 |
| 1. 為確保國家與社會功能之持續運作，中央目的事業主管機關得指定非公務機關為關鍵基礎設施提供者。   關鍵基礎設施提供者為確保資通系統之安全，應考量保有或處理之資訊種類、數量及性質、資通系統之規模及性質等條件，就所保有或運用之資通系統訂定與執行資通安全維護計畫＊。  中央目的事業主管機關應就前項之義務為查核＊。  第二項維護計畫之內容及其他應遵循事項及第三項查核辦法，由中央目的事業主管機關擬訂，送行政院核定之。 | 1. 對於關鍵基礎設施（Critical Infrastructure）提供者之資通安全保護，乃現今國際針對資通安全保護所重視之議題，爰參考歐盟網路與資訊安全指令草案（The Network and Information Security Directive）、德國資訊科技安全法（IT-Sicherheitsgesetz）與日本網路資訊安全基本法（サイバーセキュリティ基本法）、美國6 U.S. Code § 132等立法例，將關鍵基礎設施提供者納入本法之適用範圍。 2. 因關鍵基礎設施涉及國土安全之維護，故有關適用本法之關鍵基礎設施提供者宜考量國家關鍵基礎設施安全防護指導綱要之規定，以維持關鍵基礎設施政管理政策之連貫性。然而，為維持管理架構之彈性，未於本法明定適用本法之關鍵基礎設施提供者，係授權由中央目的事業主管機關認定非公務機關為關鍵基礎設施提供者，並要求其應制定並實施資通安全維護計畫。 3. 為確保資通安全維護計畫落實之有效性，中央目的事業主管機關應對於所轄之關鍵基礎設施提供者進行查核，其查核之時間、內容與方式，授權由中央目的事業主管機關訂定，送行政院核定之。 |
| 1. 關鍵基礎設施提供者應於當年年度終了後一定期間內，就其機關資通安全維護計畫之實施情形，向中央目的事業主管機關提出當年度之資通安全維護計畫實施情形報告＊。   本條所定之報告義務機關、程序、格式與內容，由中央目的事業主管機關定之。 | 為使中央目的事業主管機關掌握所轄之關鍵基礎設施提供者，在資通安全維護計畫之推動狀況，關鍵基礎設施提供者每年亦應定期向中央目的事業主管機關提出資通安全報告，以利中央目的事業主管機關適時提供相關建議或挹注相關資源。 |
| 1. 關鍵基礎設施提供者及受中央目的事業主管機關指定之非公務機關所提供之產品或服務，於發生資通安全事件時，應向中央目的事業主管機關通報資通安全事件之相關內容及因應之方法＊。   關鍵基礎設施提供者之資通安全事件情節重大時，中央目的事業主管機關及主管機關得公告必要之內容及因應措施＊。  資通安全事件如有涉及刑責之虞，相關之關鍵基礎設施提供者及受中央目的事業主管機關指定之非公務機關應妥善保全相關資料包括數位證據及軌跡紀錄，並應主動通報司法機關＊。  第一項應變、通報及預防機制之內容、第二項資通安全事件情節重大之認定、公告之內容、因應措施及第三項之資料保全內容及方式及其他應遵循事項，由中央目的事業主管機關會同主管機關定之。 | 1. 按關鍵基礎設施提供者如發生資通系統遭受破壞，或不當使用之資通安全事件，為使相關主管機關及時掌握情況，以進行緊急應變處置，並在最短時間內回復，確保關鍵基礎設施提供者之正常運作，自應以適當方式通報中央目的事業主管機關及主管機關。 2. 於資通安全事件情節重大，可能影響多數人民之生命、身體或財產利益安全時，中央目的事業主管機關與主管機在接獲關鍵基礎設施提供者之通報後，並得公告必要之內容（如發生原因、影響程度及目前控制之情形等）與因應之方法，以供一般民眾得以防範而避免損害之擴大。 3. 前項通報之時間、內容與方式，及公告之內容與方式，宜有相關規範，以為依循，故另授權中央目的事業主管機關會同主管機關訂定相關規範。 4. 關鍵基礎設施提供者為落實資通安全事件通報之要求，自應制定資通安全事件通報機制與相關應變措施。 5. 如已受指定適用本法之非公務機關所提供之產品或服務，表示其所發生之資通安全事件具有一定影響力，應如同關鍵基礎設施提供者之處理方式，與相關主管機關協力儘速回應處理。 |
| 1. 中央目的事業主管機關得協助未受指定之目的事業，發展或遵循相關產品或服務之資通安全標準。 | 有鑑於資通安全議題對於各行各業之重要性及影響力皆不容忽視；應鼓勵各事業自發性地採取相關措施來保護其自身之資通安全，爰為本條之規定，使未受指定之目的事業在遵循資通安全標準時，取得必要之協助。 |
| 1. 中央目的事業主管機關為執行資通安全維護、其他例行性業務而認有必要、或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。   中央目的事業主管機關為前項檢查時，對於得沒入或可為證據之資訊，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。  中央目的事業主管機關為前項檢查時，得率同資通或司法調查人員等專業人員共同為之。  對於第一項之進入及第二項之檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。  參與檢查之人員，因檢查而知悉他人資料者，負保密義務。 | 1. 為落實資通安全之維護，應賦予監督機關有命令、檢查及處分權，爰訂定第一項，規定中央目的事業主管機關為執行監督或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入該非公務機關檢查或要求說明、提供相關證明資料，以強化監督機關之權責。 2. 檢查人員發現非公務機關違反本法規定，如將所有儲存媒介物設備予以查扣，恐有違比例原則，爰於第二項規定，檢查時依行政罰法相關規定發現得沒入或可為證據之個人資料或檔案，而有扣留或複製之必要者，得予扣留或複製之。此外，以電腦儲存之資料檔案，其消磁、刪除或移轉非常快速，如檢查時未能即時扣留或複製，該違法資料或證據極易被湮滅或消除，檢查機關亦得依行政罰法相關規定，要求應扣留或複製物之所有人、持有人或保管人提出或交付，且於第五項明定因檢查而知悉他人資料者，應負保密義務，不得洩漏。 |
| 1. 非公務機關、物之所有人、持有人、保管人或利害關係人對前條之要求、強制、扣留或複製行為不服者，得向中央目的事業主管機關聲明異議。   前項聲明異議，中央目的事業主管機關認為有理由者，應立即停止或變更其行為；認為無理由者，得繼續執行。經該聲明異議之人請求時，應將聲明異議之理由製作紀錄交付之。  對於中央目的事業主管機關前項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第一項之人依法不得對該案件之實體決定聲明不服時，得單獨對第一項之行為逕行提起行政訴訟。 | 1. 當事人或物之所有人、持有人、保管人、利害關係人，對檢查或扣留、複製資料檔案行為認有違法或不當時，應有表示不服聲明異議之權利，以為救濟，爰訂定第一項。 2. 訂定第二項，明定對於當事人等聲明之異議，執行檢查之機關認有理由者，應立即停止或變更其行為；認無理由者，得繼續執行。但因當事人等得於日後對此檢查或其他強制、扣留或複製行為，提起救濟，是以經其請求時，應將聲明異議之理由製作紀錄交付之，不得拒絕。 3. 第三項明定當事人等對於聲明異議之決定不服時，僅得於對該案件之實體決定聲明不服時一併聲明之，不得單獨提起救濟；至於當事人等依法不得對該案件之實體決定聲明不服時，則可單獨對第一項之檢查、扣留、複製或其他強制行為，逕行提起行政訴訟，以保障其權利。 |
| **第五章 罰則** | |
| 1. 違反第十七條第二項規定未訂定資通安全維護計畫者，由中央目的事業主管機關處新台幣二十萬元以上，二佰萬元以下之罰鍰，並令限期改正，屆期未改正者，按次處罰之。 |  |
| 1. 有下列情形之一者，由中央目的事業主管機關處新台幣十萬元以上，一佰萬元以下之罰緩，並令限期改正，屆期未改正者，按次處罰之。 2. 違反第十六條第二項規定未訂定資通安全維護計畫。 3. 違反第十七條第二項規定未執行資通安全維護計畫。 |  |
| 1. 有下列情形之一者，由中央目的事業主管機關處新台幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，得按次處罰之。 2. 違反第十六條第二項規定未執行資通安全維護計畫。 3. 違反第十八條規定未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報告。 4. 違反第十九條第一項未向中央目的事業主管機關通報資通安全事件。 5. 違反第十九條第三項未主動向司法機關通報資通安全事件。 |  |
| 1. 有下列情形之一者，由中央目的事業主管機關限期改正，限期未改正者，按次處新台幣二萬元以上二十萬元以下罰鍰： 2. 違反第十六條第一項未採行適當安全維護措施。 3. 違反第十九條第三項未妥善保全相關資料。 |  |
| 1. 非公務機關無正當理由違反本法第二十ㄧ條第四項規定者，由中央目的事業主管機關處新台幣二萬元以上二十萬元以下罰鍰。 |  |
| 1. 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前五條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。 | 為促使非公務機關之代表人、管理人或其他有代表權人重視機關內部之資通安全維護計畫之推動，進而投入人力與經費，爰明定其除能證明已盡防止義務者外，其應與該機關受同一額度罰鍰之處罰。參考個人資料保護法第五十條及營業秘密法第十三之四條之體例定之。 |
| 1. 本法所稱之罰鍰，由主管機關處罰之，並得於行政執行無效果時，移送法院強制執行。 | 為免非公務機關未依期繳納罰鍰，擬比照水利法第九十六條之規定，訂定未繳納罰鍰之後續處理方式，以資明確。 |
| **第六章 附則** | |
| 1. 公務機關應將其受理之資通安全通報事件傳輸至主管機關建置之公務機關資通安全情資分享平台＊。   前項通報事件傳輸之內容、程序及方法、情資之分析、分享、整合及其他應遵循事項，由主管機關定之。 | 1. 為增進與改善我國境內面對資通安全威脅與風險的應變能力與策略擬定，應建立相關資通安全情資分享機制，以促進相關政策、法令之修訂。 2. 有鑑於主管機關管理監督公務機關相關之資通安全環境，而中央目的事業主管機關監督管理目的事業相關之資通安全環境，因此以主管機關、中央目的事業主管機關為主要參與主體，參與並建立資通安全分享機制。 |
| 1. 中央各機關及直轄市、縣 (市) 政府應依法編列必要之人力與經費，確保有效推動資通安全政策相關事項。 | 一、為確保資通安全政策相關事項之有效推動，政府應匡列人力與經費。參考癌症防治法第十六條、[花東地區發展條例](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=A0030242)第十二條、[全民防衛動員準備法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=F0070013)第四十五條、[災害防救法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=D0120014)第四十三條及[核子事故緊急應變法](http://law.moj.gov.tw/LawClass/LawContentIf.aspx?PCODE=J0160056)第四十三條之體例定之。 |
| 1. 為提升資通安全，主管機關及中央目的事業主管機關應提供充分資源並整合民間力量，提升全民資通安全意識，並推動下列事項： 2. 資通安全專業人才之培育。 3. 資通安全科技之研發、整合、應用、產學合作及國際交流合作之推動。 4. 資通安全產品與管理系統之認驗證標準與體系之發展及推動。 5. 資通安全產業發展及推動。 | 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、軟體、設備、專業人才等。是以，政府應與民間共同提升全民資通安全意識，推動資通安全產業之發展，以利先進資通安全技術、軟體、設備、專業人才等之發展。參考癌症防治法第五條之體例定之。 |
| 1. 本法施行細則，由主管機關定之＊。 |  |
| 1. 本法自公布日施行。 |  |