

教育部 函

機關地址：10051臺北市中山南路5號

聯絡人：林文信

電話：02-7712-9092

受文者：國立暨南國際大學

發文日期：中華民國107年12月14日

發文字號：臺教資(四)字第1070215157號

速別：速件

密等及解密條件或保密期限：

附件：原函影本、資通安全責任等級分級彙整表(特定非公務機關)、資通安全責任等級分級彙整表(公務機關)、資通安全維護計畫(範本)、資通安全維護計畫範本參考附件、公務機關資通安全事件通報及應變管理程序(範本)、特定非公務機關資通安全事件通報及應變管理程序(範本)、資通安全事件通報單、02-1_教育體系資通安全維護計畫(A級適用)、02-1_教育體系資通安全維護計畫(B級適用)、02-1_教育體系資通安全維護計畫(C級適用)、學校資通安全事件通報及應變管理程序

主旨：函轉行政院有關資通安全管理法及其子法，行政院定自108年1月1日施行(如附件)，請查照並轉知所屬或監督之公務機關。

說明：

一、依據行政院107年12月5日院臺護字第1070217128B號函辦理。

二、有關原函說明二資通安全責任等級，本部提報說明如下：

(一)A級：本部、國立大學附設醫院(醫學中心)及常設試務機構。

(二)B級：本部所屬機關、國家教育研究院、國家圖書館、公立大專校院、國立大學附設醫院(區域醫院或地區醫院)、財團法人高等教育評鑑中心基金會。

(三)C級：本部其他所屬機構、國家運動訓練中心、及有維運自行或委外開發核心資通系統「公立高級中等以下學校」或特定非公務機關。

(四)D級：配合資訊資源向上集中計畫，核心資通系統由其上級或監督

總收文 107/12/17



機關兼辦或代管或未維運資通系統「公立高級中等以下學校」或特定非公務機關。

(五)E級：其他分校、分部或大學附屬各級學校，全部資通業務由其本校兼辦或代管者，或財團法人全部資通業務由其上級機關兼辦或代管者。

三、請各單位依上開責任等級及資通安全責任等級分級辦法附表應辦事項，函復資通安全管理法施行後預計可配置之資安專職（責）人力數，並說明人員類別，俾利本部彙辦。

四、請各單位訂定「資通安全維護計畫」及「資通安全事件通報及應變程序」，於明(108)年1月31日前送本部彙整審查，說明如下：

(一)資通安全維護計畫各單位可參考「教育體系資通安全維護計畫（範本）」修正。

(二)資通安全事件通報及應變程序，學校可參考「學校資通安全事件通報及應變管理程序(範本)」修正；公務機關及財團法人請參考行政院範本修正。

五、請各機關、學校於108年3月31日前依「公務機關所屬人員資通安全事項獎懲辦法」規定修正內部平時考核規定。

本：部屬機關(構)及國家運動訓練中心、各公立大學校院、各國立專科學校、國立臺灣大學醫學院附設醫院、國立陽明大學附設醫院、國立成功大學醫學院附設醫院、國立台北護理學院附設醫院、大學甄選入學委員會、大學考試入學分發委員會、身心障礙學生升學大專校院甄試委員會、技專校院招生委員會聯合會、財團法人技專校院入學測驗中心基金會、心理與教育測驗研究發展中心、財團法人教育部接受捐助獎學基金會、財團法人大學入學考試中心基金會、財團法人私立學校興學基金會、財團法人高等教育評鑑中心基金會、財團法人中華幼兒教育發展基金會、財團法人台灣省中小學校教職員福利文教基金會、財團法人國民教育測驗與評量中心教育基金會、財團法人高等教育國際合作基金會、財團法人蔣經國國際學術交流基金會、財團法人社教文化基金會、財團法人臺灣省童軍文教基金會、財團法人吳健雄學術基金會

副本：臺灣學術網路區域網路中心、各直轄市及縣市教育網路中心

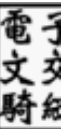
107/12/17
09:53:02

行政院 函

地址：10058臺北市忠孝東路1段1號
傳真：02-23973457
聯絡人：王詠萱02-33566500#8207
電子信箱：yswang@ey.gov.tw

受文者：教育部

發文日期：中華民國107年12月5日
發文字號：院臺護字第1070217128B號
速別：普通件
密等及解密條件或保密期限：
附件：如說明(1070217128B-0-0.xlsx、1070217128B-0-1.xlsx、1070217128B-0-2.docx、1070217128B-0-3.docx、1070217128B-0-4.docx、1070217128B-0-5.docx、1070217128B-0-6.doc)



主旨：中華民國107年6月6日制定公布之「資通安全管理法」及107年11月21日訂定發布之「資通安全管理法施行細則」、「資通安全責任等級分級辦法」、「資通安全事件通報及應變辦法」、「特定非公務機關資通安全維護計畫實施情形稽核辦法」、「資通安全情資分享辦法」、「公務機關所屬人員資通安全事項獎懲辦法」，本院定自108年1月1日施行，請查照並轉知所屬或監督之公務機關及所管特定非公務機關。



說明：

一、依「資通安全管理法」第23條、「資通安全管理法施行細則」第13條、「資通安全責任等級分級辦法」第12條、「資通安全事件通報及應變辦法」第21條、「特定非公務機關資通安全維護計畫實施情形稽核辦法」第10條、「資通安全情資分享辦法」第11條及「公務機關所屬人員資通安全事項獎懲辦法」第7條規定辦理。

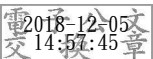
二、為確保資通安全管理法順利施行，請各機關配合依下列事



項辦理相關整備工作：

- (一)各機關依「資通安全責任等級分級辦法」第3條第2項至第5項規定及「資通安全責任等級分級彙整表」(如附件1)填表說明，填復自身、所屬或監督之公務機關及所管之特定非公務機關(不含關鍵基礎設施提供者)之資通安全責任等級，等級提交機關於本(107)年12月15日前送本院核定，等級核定機關於108年1月2日前送本院備查。
- (二)請各機關(不含關鍵基礎設施提供者)於本年12月31日前完成「資通安全維護計畫」及「資通安全事件通報及應變程序」訂定事宜(範本詳附件2)，並請各上級或監督機關協助彙整及審視所屬(轄)公務機關資通安全維護計畫，於108年2月28日前送本院備查。
- (三)請各公務機關於108年3月31日前依「公務機關所屬人員資安全事項獎懲辦法」規定修正內部平時考核規定。

正本：總統府、國家安全會議、立法院、司法院、考試院、監察院、各部會行總處署、省政府、各直轄市政府、各縣市政府、各直轄市議會、各縣市議會

副本：  2018-12-05 14:57:45

資通安全維護計畫

目 錄

壹、 依據及目的	3
貳、 適用範圍	3
參、 核心業務及重要性	3
一、 核心業務及重要性：	4
二、 非核心業務及說明：	5
肆、 資通安全政策及目標	5
一、 資通安全政策	6
二、 資通安全目標	6
三、 資通安全政策及目標之核定程序	7
四、 資通安全政策及目標之宣導	7
五、 資通安全政策及目標定期檢討程序	7
伍、 資通安全推動組織	7
一、 資通安全長	8
二、 資通安全推動小組	8
陸、 專職(責)人力及經費配置	10
一、 專職(責)人力及資源之配置	10
二、 經費之配置	11
柒、 資訊及資通系統之盤點	12
一、 資訊及資通系統盤點	12
二、 機關資通安全責任等級分級	13
捌、 資通安全風險評估	13
一、 資通安全風險評估	13
二、 核心資通系統及最大可容忍中斷時間	14
玖、 資通安全防護及控制措施	14
一、 資訊及資通系統之管理	15

二、存取控制與加密機制管理.....	16
三、作業與通訊安全管理.....	19
四、系統獲取、開發及維護.....	23
五、業務持續運作演練	24
六、執行資通安全健診	24
七、資通安全防護設備	24
壹拾、資通安全事件通報、應變及演練相關機制	25
壹拾壹、資通安全情資之評估及因應	25
一、資通安全情資之分類評估.....	25
二、資通安全情資之因應措施.....	26
壹拾貳、資通系統或服務委外辦理之管理	27
一、選任受託者應注意事項.....	27
二、監督受託者資通安全維護情形應注意事項.....	28
壹拾參、資通安全教育訓練	28
一、資通安全教育訓練要求.....	29
二、資通安全教育訓練辦理方式.....	29
壹拾肆、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	29
壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制	30
一、資通安全維護計畫之實施.....	30
二、資通安全維護計畫實施情形之稽核機制	30
三、資通安全維護計畫之持續精進及績效管理.....	31
壹拾陸、資通安全維護計畫實施情形之提出	32
壹拾柒、相關法規、程序及表單	32
一、相關法規及參考文件.....	32
二、附件表單	33

壹、依據及目的

範例一：

本計畫依據資通安全管理法第 10 條及施行細則第 6 條訂定。

範例二：

本計畫依據下列法規訂定：

- 一、資通安全管理法第 10 條及其施行細則第 6 條。
- 二、其他業務法規名稱。

貳、適用範圍

範例一：

本計畫適用範圍涵蓋本○全機關。

範例二：

本計畫適用範圍除本○全機關外，另包含(請依實際情形列出適
其他機關名稱)機關。

參、核心業務及重要性

撰寫說明：

- 本章重點在揭示組織之核心業務，並說明核心業務失效時對國人日常生活、社會經濟、政府功能之影響。
- 機關核心業務請依據資通安全管理法施行細則第 7 條規定及政府機關組織法列示。
- 資安責任等級為 A 級及 B 級機關如已進行業務營運衝擊分析，亦可援引敘明。
- 另為進行資通安全事件等級判定，機關仍應針對輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等非核心業務進行盤點，並列出最大可容忍中斷時間。

● 範例如下：

範例：

一、核心業務及重要性：

本機關之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
		☐ 為主管機關指定之關鍵基礎設施 ☐ 為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 ☐ 為本機關依組織法執掌，足認為重要者	財務損失： 民眾生命財產損失： 經濟發展受阻： 影響其他機關業務運作(相依性)： 違反法遵義務： 機關信譽： 其他：	
全國公務人員人事管理(範例)	全國公務人員人事管理系統	☐ 為主管機關指定之關鍵基礎設施 ☒ 為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 ☐ 為本機關依組織法執掌，足認為重要者	違反法遵義務:依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依受罰。	4 小時

各欄位定義：

1. 核心業務名稱：請參考資通安全管理法施行細則第 7 條之規定列示。
2. 作業名稱：該項業務內各項作業程序的名稱。
3. 重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。

4. 最大可容忍中斷時間單位以小時計。

二、非核心業務及說明：

本機關之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
公文交換 (範例)	電子公文無法即時送達機關，影響機關行政效率	○小時
其他-非屬上開業務範疇及核心業務者 (範例)	影響機關行政效率	○小時

各欄位定義：

1. 業務名稱：公務機關之非核心業務至少應包含輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等。(請依機關實際情形列出)
2. 作業名稱：該項業務內各項作業程序的名稱。
3. 說明：說明該業務之內容。
4. 最大可容忍中斷時間單位以小時計。

肆、資通安全政策及目標

撰寫說明：

- 本章包含政策內容、目標、核定程序、宣導程序、定期檢討程序等節，機關如已有規定及程序者，可直接引述內部文件編號及名稱。
- 本章經參考行政院及所屬各機關資訊安全管理規範之「壹、資訊安全政策制定及評估」一節，提供範本如下，機關得參酌本範本修改為機關適用之文件，內容可著重一般同仁應遵守之原則性規定。

一、資通安全政策

為使本機關業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

1. 應建立資通安全風險管理機制，定期因應內外資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 應強固核心資通系統之韌性，確保機關業務持續營運。
4. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本機關同仁之資通安全意識，本機關同仁亦應確實參與訓練。
5. 針對辦理資通安全業務有功人員應進行獎勵。
6. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
7. 禁止多人共用單一資通系統帳號。
8.

二、資通安全目標

（請各機關自行訂定資通安全目標，目標宜有量化與質化型指標，以下僅例示內容供參）

（一）量化型目標

1. 核心資通系統可用性達 99.99% 以上。（中斷時數/總運作時數 ≤ 0.1%）
2. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
3. 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5% 及 2%。
4.

(二) 質化型目標：(請視實際需要填列)

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免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。
2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。
3. 提升人員資安防護意識、有效偵測與預防外部攻擊等.....

三、資通安全政策及目標之核定程序

資通安全政策由本機關○○單位簽陳資通安全長核定。

四、資通安全政策及目標之宣導

1. 本機關之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。
2. 本機關應每年向利害關係人(例如 IT 服務供應商、與機關連線作業有關單位)進行資安政策及目標宣導，並檢視執行成效。

五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於資通安全管理審查會議中檢討其適切性。

伍、資通安全推動組織

撰寫說明：

- 本章至少包含資通安全長(特定非公務機關可為資通安全管理代表)、資通安全推動小組之組成及分工職掌等內容。機關規模較大者，亦可於資通安全長(資通安全管理代理)下設置資通安全指導小組及資通安全推動小組，分別負責資通安全規劃及推動作業。機關針對資通安全推動組織如已有規定及程序者，可直接引述內部文件編號及名稱。
- 本章參考行政院及所屬各機關資訊安全管理規範之「貳、資訊

安全組織及權責」一節，提供範本如下，機關得參酌本範本修改為機關適用之文件。

範本：

一、資通安全長

(針對特定非公務機關，資通安全長可改為資通安全管理代表)

依本法第 11 條之規定，本機關訂定○長（副首長或適當人員¹）為資通安全長，負責督導機關資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。
2. 資通安全責任之分配及協調。
3. 資通安全資源分配。
4. 資通安全防護措施之監督。
5. 資通安全事件之檢討及監督。
6. 資通安全相關規章與程序、制度文件核定。
7. 資通安全管理年度工作計畫之核定
8. 資通安全相關工作事項督導及績效管理。
9. 其他資通安全事項之核定。

二、資通安全推動小組

(一) 組織

為推動本機關之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各業務部門主管/副主管以上之人員代表成立資通安全推動小組²，其任務包括：

1. 跨部門資通安全事項權責分工之協調。

¹ 考量資通安全推動時常涉及機關內相關資源調動及分配等事項，故資通安全長由機關首長指派副首長擔任，如機關首長指派適當人員擔任資通安全長時，該人員應具有足夠權責、資源、權限、相當資歷、經驗及資安專業之人員兼任為宜，使資通安全相關業務得以順利推展。

² 資通安全推動小組成員由機關之資通安全長召集組成，依資通安全長之指示，負責協助或與機關內之相關單位合作推動機關內部之資通安全業務，如機關未成立資通安全推動小組，相關業務則應由資通安全長責承相關資通安全權責人員辦理之。

2. 應採用之資通安全技術、方法及程序之協調研議。
3. 整體資通安全措施之協調研議。
4. 資通安全計畫之協調研議。
5. 其他重要資通安全事項之協調研議。

(二) 分工及職掌(以下為例示規定，請各機關依實際情形列出分工與職掌)

本機關之資通安全推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項，本機關資通安全推動小組分組人員名單及職掌應列冊，並適時更新之³：

1. 策略規劃組：

- (1) 資通安全政策及目標之研議。
- (2) 訂定機關資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。
- (3) 依據資通安全目標擬定機關年度工作計畫。
- (4) 傳達機關資通安全政策與目標。
- (5) 其他資通安全事項之規劃。

2. 資安防護組：

- (1) 資通安全技術之研究、建置及評估相關事項。
- (2) 資通安全相關規章與程序、制度之執行。
- (3) 資訊及資通系統之盤點及風險評估。
- (4) 資料及資通系統之安全防護事項之執行。
- (5) 資通安全事件之通報及應變機制之執行。
- (6) 其他資通安全事項之辦理與推動。

3. 績效管理組：

- (1) 辦理資通安全內部稽核。
- (2) 每半年(每年)定期召開資通安全管理審查會議，提報資通安全

³ 各公務機關應製作「資通安全推動小組成員及分工表」，說明小組成員及相關職掌，格式可參附件：資通安全推動小組成員及分工表。

事項執行情形。

陸、專職(責)人力及經費配置

撰寫說明：

- 本章至少包含資安人員配置、訓練及證照，以及資通安全經費或資源之規劃及配置等內容，機關如已有規定及程序者，可直接引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

範本如下：

一、專職(責)人力及資源之配置

1. 本機關依資通安全責任等級分級辦法之規定，屬資通安全責任等級○級，最低應設置資通安全專職(責)人員○人，其分工如下，本機關現有資通安全專責人員名單及職掌應列冊，並適時更新⁴。

(以下分工供例示參考，請機關考量實務需求列出)

- (1) 資通安全管理面業務 1 人，負責推動資通系統防護需求分級、資通安全管理系統導入及驗證、內部資通安全稽核、機關資安治理成熟度評估及教育訓練等業務之推動。
 - (2) 資通系統安全管理業務 1 人，負責資通系統分級及防護基準、安全性檢測、業務持續運作演練等業務之推動。
 - (3) 資通安全防護業務 1 人，負責資通安全監控管理機制、政府組態基準導入，資通安全防護設施建置及資通安全事件通報及應變業務之推動。
 - (4) 資通安全管理法法遵事項業務 1 人，負責本機關對所屬公務務機關或所管特定非公務機關之法遵義務執行事宜。
2. 本機關之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本機關之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關

⁴ 各公務機關應製作「資通安全專職人員分工表」，說明專職人員及相關職掌，格式可參附件：資通安全推動小組成員及分工表。

- (構)提供顧問諮詢服務。
3. 資安專職(責)人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定⁵。
 - (1) 資安專職(責)人員總計應持有○張以上資通安全專業證照⁶。
 - (2) 資安專職(責)人員總計應持有○張以上資通安全職能評量證書⁷。
 4. 本機關負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定⁸，並視需要實施人員輪調，建立人力備援制度。
 5. 本機關之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。
 6. 專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

二、經費之配置

1. 資通安全推動小組於規劃配置相關經費及資源時，應考量本機關之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源⁹。
2. 各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。
3. 各單位如有資通安全資源之需求，應配合機關預算規劃期程向資通安全推動小組提出¹⁰，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長(資通安全管理代表)核定後，進行相關之建置。
4. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

⁵ 各機關應依據其資通安全責任等級分級辦法所規範之資通安全專責人員、認知與訓練之要求，配置適當之資源於資安人員專業職能之培養。

⁶ 視各機關之資通安全責任等級之分級要求。

⁷ 視各機關之資通安全責任等級之分級要求。

⁸ 格式可參附件：資通安全保密同意書。

⁹ 為有效建置機關之資通安全風險防護機制，公務機關應投入相當之資源，故機關之資通安全推動小組於資源規劃或編制預算時，應考量機關之責任等級、資通安全政策及目標。

¹⁰ 各機關可填具資通安全需求申請單，格式可參附件：資通安全需求申請單。

柒、資訊及資通系統之盤點

撰寫說明：

- 本章至少包含資訊及資通系統之分類及盤點之程序，並應包含標示核心資通系統及相關資產之要求。機關如已有規定及程序者，可直接引述內部文件編號及名稱。
- 本章經參考行政院及所屬各機關資訊安全管理規範之「捌、資訊資產之安全管理」一節，提供範本如下，機關得參酌本範本修改為機關適用之文件。

範本如下：

一、資訊及資通系統盤點

1. 本機關每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為資訊資產、軟體資產、實體資產、支援服務資產等(分類僅供參考，機關可依實際情形調整)。
2. 資訊及資通系統資產項目如下(供參)：
 - (1) 資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。
 - (2) 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。
 - (3) 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。
 - (4) 支援服務資產：相關基礎設施級其他機關內部之支援服務，如電力、消防等。
 - (5) ...(如人員資料：)
3. 本機關每年度應依資訊及資通系統盤點結果¹¹，製作「資訊及資

¹¹ 為使公務機關能依其所屬之資通安全責任等級之分級，執行相關之資通安全防護措施，公務機關應先進行機關內部之資訊及資通系統資產之盤點，使其能依據其所擁有之資訊或資通系統依據資通安全責任等級分級辦法進行風險評估。

通系統資產清冊」¹²，欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級。

4. 資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。核心資通系統及相關資產，並應加註標示。
5. 各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新資產清冊。

二、機關資通安全責任等級分級

本機關因持有全國性民眾個人資料檔案，並負責全國性民眾務之資通系統之推運，為資通安全責任等級 A 級機關。

(請機關依資通安全責任等級分級辦法規定自行修改內容)

捌、資通安全風險評估

撰寫說明：

- 本章至少包含風險評估、風險因應等節，機關如已有規定及程序者，可直引述內部文件編號及名稱。
- 本章參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」。
- 機關得參酌本範本修改為機關適用之文件。

範本如下：

一、資通安全風險評估

1. 本機關應每年針對資訊及資通系統資產進行風險評估。
2. 執行風險評估時應參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」，並依其中之「詳細風險評鑑方法」進行風險評估之工作。
3. 本機關應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外

¹² 參資訊系統風險評鑑參考指引附件詳細風險評鑑空白表單之資訊資產表。

開發之資通系統防護需求分級。

二、核心資通系統及最大可容忍中斷時間

核心資通系統	資訊資產	最大可容忍中斷時間	核心資通系統主要功能
○○○網站 (範例)	1. 網站前台主機計 3 台 2. 網站後台主機計 1 台 3. 負載平衡伺服器 4. 網路交換器(型號) (提供該網站網路服務之網路設備均需列出)	○小時	提供民眾申辦○○○服務

最大可容忍中斷時間以小時計。

玖、資通安全防護及控制措施

撰寫說明：

- 本章為機關因應資通安全風險，採取之安全防護及控制措施。
- 機關得參酌本範本修改為機關適用之文件。
- 針對需導入 CNS27001 之機關，因其標準中已有相關之規定及程序，僅需針對資通安全責任等級分級辦法中應辦事項列出防護及控制措施。
- 需導入 CNS27001 之機關範本如下：

本機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施，由於本機關核心資通系統已通過(導入)CNS27001 驗證，全機關之防護及控制措施詳如 CNS27001 資通安全管理系統

文件。

(請機關確認現有程序及標準書內容，需滿足以下範本中「未導入 CNS27001 機關之資通安全防護及控制措施」建議內容，如各機關對於非核心系統有不同的管理規定，可加以說明。)

- 針對未導入 CNS27001 之機關，本範例中參考資安治理成熟度評審作業面向，CNS27002 中控制措施之作業規範，提示原則性之準則(Standards)規範，請各依機關視實際情形增修，並針對各項準則定出相關程序(Procedures)文件。

- 不需導入 CNS27001 之機關範本如下：

本機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施如下：

一、資訊及資通系統之管理

(一) 資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。
2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。
3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。
4.其餘可參考 CNS 27002 編號 8.資產管理等相關內容。

(二) 資訊及資通系統之使用

1. 本機關同仁使用資訊及資通系統前應經其管理人授權。
2. 本機關同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 本機關同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。

4. 非本機關同仁使用本機關之資訊及資通系統，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。
5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。
6.其餘可參考 CNS 27002 編號 8.資產管理等相關內容。

(三) 資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。
2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。
3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。
4.其餘可參考 CNS 27002 編號 11.2.7 設備汰除或再使用之保全等相關內容。

二、存取控制與加密機制管理

(一) 網路安全控管

1. 本機關之網路區域劃分如下：(請機關視實際情形增列)
 - (1) 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。
 - (2) 非軍事區(DMZ)：放置機關對外服務伺服器之區段。
 - (3) 內部區域網路 (Local Area Network, LAN)：機關內部單位人員及內部伺服器使用之網路區段。
2. 外部網路、非軍事區及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。
3. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。
4. 對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時

間、存取時間以及採取的行動，均應予確實記錄。

5. 本機關內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

6. 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

7. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

8. 網域名稱系統(DNS)防護

(1) 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

(2) DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

(3) DNS 伺服器應設定指向 GSN Cache DNS。(公務機關適用)

(4) 內部主機位置查詢應指向機關內部 DNS 伺服器。

9. 無線網路防護

(1) 機密資料原則不得透過無線網路及設備存取、處理或傳送。

(2) 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

(3) 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

(4) 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

10.其餘可參考 CNS 27002 編號 9.1.2 對網路及網路服務之存取，以及國家資通安全會報「網路架構規劃參考指引」、「無線網路安全參考指引」等相關內容。

(二) 資通系統權限管理

1. 本機關之資通系統應設置通行碼管理，通行碼之要求需滿足：

(1) 通行碼長度 8 碼以上。

(2) 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以

上。

- (3) 使用者每 90 天應更換一次通行碼。
2. 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。
3. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。
4.其餘可參考 CNS 27002 編號 9.2.1 使用者註冊及註銷、編號 9.2.2 使用者存取權限之配置等相關內容。

(三) 特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。
2. 資通系統之特權帳號不得共用。
3. 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。
4. 資通系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。
5. 資通系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。
6.其餘可參考 CNS 27002 編號 9.2.3 具特殊存取權限之管理等相關內容。

(四) 加密管理

1. 本機關之機密資訊於儲存或傳輸時應進行加密。
2. 本機關之加密保護措施應遵守下列規定：
 - (1) 應落實使用者更新加密裝置並備份金鑰。
 - (2) 應避免留存解密資訊。
 - (3) 一旦加密資訊具遭破解跡象，應立即更改之。
 - (4) ...
3.其餘可參考 CNS 27002 編號 9.2.4 使用者之秘密鑑別資訊的管理、編號 9.3.1 秘密鑑別資訊之使用等相關內容。

三、作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本機關之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。
 - (1) 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。
 - (2) 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。
 - (3) 確實執行網頁惡意軟體掃描。
 - (4) …
2. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。
3. 使用者不得私自使用已知或有嫌疑惡意之網站。
4. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。
5.其餘可參考 CNS 27002 編號 12.2.1 防範惡意軟體之控制措施等相關內容。

(二) 遠距工作之安全措施

1. 本機關資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。
2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。
3. 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。
 - (1) 提供適當通訊設備，並指定遠端存取之方式。
 - (2) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。
 - (3) 進行遠距工作時之安全監視。
 - (4) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

4.其餘可參考 CNS 27002 編號 6.2.2 遠距工作等相關內容。

(三) 電子郵件安全管理

1. 本機關人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。
2. 電子郵件系統管理人應定期進行電子郵件帳號清查。
3. 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。
4. 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。
5. 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。
6. 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。
7. 使用者應確保電子郵件傳送時之傳遞正確性。
8. 使用者使用電子郵件時，應注意電子簽章之要求事項。
9. 本機關應定期舉辦(或配合上級機關舉辦)電子郵件社交工程演練，並檢討執行情形。
10.其餘可參考 CNS 27002 編號 13.2.3 電子傳輸等相關內容。

(四) 確保實體與環境安全措施

1. 資料中心及電腦機房之門禁管理
 - (1) 資料中心及電腦機房應進行實體隔離。
 - (2) 機關人員或來訪人員應申請及授權後方可進入資料中心及電腦機房¹³，資料中心及電腦機房管理者並應定期檢視授權人員之名單。
 - (3) 人員進入管制區應配戴身分識別之標示，並隨時注意身分不明或可疑人員。

¹³ 未具進出管制區權限之人員來訪時，應填具進出登記表，格式可參附件：管制區域人員進出登記表。

- (4) 僅於必要時，得准許外部支援人員進入資料中心及電腦機房。
- (5) 人員及設備進出資料中心及電腦機房應留存記錄。
- (6) …

2. 資料中心及電腦機房之環境控制

- (1) 資料中心及電腦機房之空調、電力應建立備援措施。
- (2) 資料中心及電腦機房之溫濕度管控範圍為：
- (3) 資料中心及電腦機房應安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全引發之危險。
- (4) 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。
- (5) …

3. 辦公室區域之實體與環境安全措施

- (1) 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
- (2) 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。
- (3) 機密性及敏感性資訊，不使用或下班時應該上鎖。
- (4) 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。
- (5) 顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。
- (6) 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。
- (7) …

4.其餘可參考 CNS 27002 編號 11.1 保全區域、編號 11.2 設備等相關內容。

(五) 資料備份

- 1. 重要資料及核心資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

2. 本機關應每季確認核心資通系統資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通系統。
3. 敏感或機密性資訊之備份應加密保護。
4.其餘可參考 CNS 27002 編號 12.3 備份、編號 17.2 多重備援等相關內容。

(六) 媒體防護措施

1. 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
2. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。
3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。
4. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。
5.其餘可參考 CNS 27002 編號 8.3 媒體處置等相關內容。

(七) 電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
3. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
4. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
5. 下班時應關閉電腦及螢幕電源。
6. 如發現資安問題，應主動循機關之通報程序通報。
7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

8.其餘可參考 CNS 27002 編號 11.2 設備等相關內容。

(八) 行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。
2. 機敏會議或場所不得攜帶未經許可之行動設備進入
3.其餘可參考參考 CNS 27002 編號 6.2.1 行動裝置政策、政府行動化安全防護規劃報告及行動裝置資安防護參考指引。

(九) 即時通訊軟體之安全管理

1. 使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。
2. 使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求：
 - (1) 用戶端應有身分識別及認證機制。
 - (2) 訊息於傳輸過程應有安全加密機制。
 - (3) 應通過經濟部工業局訂定行動化應用軟體之中級檢測項目。
 - (4) 伺服器端之主機設備及通訊紀錄應置於我國境內。
 - (5) 伺服器通訊紀錄 (log) 應至少保存六個月。
 - (6) 伺服器主機每年辦理二次弱點掃描及一次滲透測試，且不能出現中風險以上之弱點。
3.其餘可參考行政院及所屬機關使用即時通訊軟體安全管理要點。

四、系統獲取、開發及維護

(有維護、自行或委外開發資通系統機關適用)

1. 本機關之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十中資通系統防護基準，並注意下列事項：
 - (1) 開發過程請依安全系統發展生命週期 (Secure Software Development Life Cycle, SSDLC) 納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。

- (2) 於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。
 - (3) 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。
 - (4) 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。
2.其餘可參考 CNS 27002 編號 14.系統獲取、開發及維護等相關內容。

五、業務持續運作演練

(有核心資通系統之 C 級機關適用)

本機關應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。

六、執行資通安全健診

(C 級機關適用)

1. 本機關每二年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：
 - (1) 網路架構檢視。
 - (2) 網路惡意活動檢視。
 - (3) 使用者端電腦惡意活動檢視。
 - (4) 伺服器主機惡意活動檢視。
 - (5) 安全設定檢視。

七、資通安全防護設備

1. 本機關應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。
2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

壹拾、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本機關應訂定資通安全事件通報、應變及演練相關機制，詳資通安全事件通報應變程序¹⁴。

壹拾壹、資通安全情資之評估及因應

撰寫說明：

- 本章為機關接受情資後應採取之評估及因應措施，其內容包括情資分類及情資因應。機關如已有對應之規定及程序者，可直引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

範本如下：

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、資通安全情資之分類評估

本機關接受資通安全情資後，應指定資通安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(二) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動

¹⁴ 各機關應另訂定資通安全事件通報及應變程序。

且證據明確等內容，屬入侵攻擊情資。

(三) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之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，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(四) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、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等內容，屬涉及核心業務、核心資通系統之情資。

二、資通安全情資之因應措施

本機關於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一) 資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(二) 入侵攻擊情資

由資通安全專職(責)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三) 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

(四) 涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資

評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

壹拾貳、資通系統或服務委外辦理之管理

撰寫說明：

- 本章為機關辦理資通系統或服務委外時應注意之事項，其內容包括委外前之選任及委外後之監督。資安法施行細則第4條中除已規範應注意事項外，機關亦可參考最新版本之《資訊作業委外安全參考指引》調整相關內容，並於資訊委外各階段，訂定具體安全需求。機關如已有對應之規定及程序者，可直引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

範本如下：

本機關委外辦理資通系統之建置、維運或資通服務之提供時，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。

一、選任受託者應注意事項

1. 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¹⁵。
2. 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。
3. 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。
4. 受託業務涉及國家機密者，應考量受託業務所涉及國家機密之機密等級內容，於招標公告、招標文件及契約中，註明受託者辦理該項業務人員及可能接觸該國家機密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。(得視情形刪去)
5. 前點適任性查核得在必要範圍內就下列事項查核，查核前應經

¹⁵ 委外單位之管理措施是否完善，可視其人員資格是否具有相關證照、訓練或認證（如 ISO 27001、CISSP、SSCP、各資安教育訓練單位所辦之課程等）做為參考。

當事人書面同意：(得視情形刪去)

- (1) 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者。
- (2) 曾任公務人員因違反相關安全保密規定，受懲戒處分、記過以上行政懲處者。
- (3) 曾受到外國政府、大陸地區或香港、澳門官方之利誘、脅迫，從事不利國家安全或重大利益情事者。
- (4) 其他與國家機密保護相關之具體項目。

二、監督受託者資通安全維護情形應注意事項

1. 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第三方安全性檢測證明；涉及利用非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。
2. 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。
3. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
4. 受託者應採取之其他資通安全相關維護措施¹⁶。
5. 本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¹⁷。

壹拾參、資通安全教育訓練

撰寫說明：

- 本章為機關辦理資通安全教育訓練事宜，其內容教育訓練之要求及辦理方式。機關如已有對應之規定及程序者，可直引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

¹⁶ 公務機關與委外廠商簽訂契約時，應審查契約中保密條款，並要求委外廠商之業務執行人員簽署委外廠商執行人員保密切結書、保密同意書，格式可參附件：委外廠商執行人員保密切結書、保密同意書。

¹⁷ 稽核項目可參委外廠商查核項目表。

範本如下：

一、資通安全教育訓練要求

1. 本機關依資通安全責任等級分級屬○級，資安及資訊人員每年至少○名人員接受○○小時以上之資安專業課程訓練或資安職能訓練。
2. 本機關之一般使用者與主管，每人每年接受○小時以上之一般資通安全教育訓練。

二、資通安全教育訓練辦理方式

1. 承辦單位應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫¹⁸，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄¹⁹。
2. 本機關資通安全認知宣導及教育訓練之內容得包含：(請視實際情形增列)
 - (1) 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。
 - (2) 資通安全法令規定。
 - (3) 資通安全作業內容。
 - (4) 資通安全技術訓練。
3. 員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。
4. 資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

壹拾肆、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

本機關所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、(請填寫機關內部獎懲辦法及名稱)，及本

¹⁸ 格式可參附件：年度資通安全教育訓練計畫。

¹⁹ 公務機關辦理教育訓練時，參加人員應簽名留存紀錄，格式可參附件：資通安全認知宣導及教育訓練簽到表。

機關各相關規定辦理之。

壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制

撰寫說明：

- 本章為機關資通安全維護計畫實施情形之績效管理及持續精進機制，其內容包括維護計畫之實施、稽核及管理審查會議。機關如已有對應之規定及程序者，可直引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

範本如下：

一、資通安全維護計畫之實施

為落實本安全維護計畫，使本機關之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本機關之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、資通安全維護計畫實施情形之稽核機制

(一) 稽核機制之實施

1. 資通安全推動小組應定期(至少每年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。
2. 辦理稽核前資通安全推動小組應擬定資通安全稽核計畫²⁰並安排稽核成員，稽核計畫應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²¹、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。
3. 辦理稽核時，資通安全推動小組應於執行稽核前○○日，通知受稽單位，並將稽核期程、稽核項目紀錄表²²及稽核流程等相關資訊提供受稽單位。

²⁰ 格式可參附件：資通安全稽核計畫。

²¹ 格式可參附件：稽核委員聘任同意暨保密切結書。

²² 格式可參附件：稽核項目紀錄表

4. 本機關之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告²³中，並提供給受稽單位填寫辦理情形。
5. 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。
6. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼）。

(二) 稽核改善報告

1. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。
2. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。
3. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。
4. 機關應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。
5. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

三、資通安全維護計畫之持續精進及績效管理

1. 本機關之資通安全推動小組應於○○月(每年至少一次)召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
2. 管理審查議題應包含下列討論事項：
 - (1) 過往管理審查議案之處理狀態。
 - (2) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

²³ 格式可參附件：稽核結果及改善報告。

- (3) 資通安全維護計畫內容之適切性。
 - (4) 資通安全績效之回饋，包括：
 - A. 資通安全政策及目標之實施情形。
 - B. 資通安全人力及資源之配置之實施情形。
 - C. 資通安全防護及控制措施之實施情形。
 - D. 內外部稽核結果。
 - E. 不符合項目及矯正措施。
 - (5) 風險評鑑結果及風險處理計畫執行進度。
 - (6) 重大資通安全事件之處理及改善情形。
 - (7) 利害關係人之回饋。
 - (8) 持續改善之機會。
3. 持續改善機制之管理審查應做成改善績效追蹤報告²⁴，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾陸、資通安全維護計畫實施情形之提出

本機關依據本法第 11(16,17)條之規定，應於○○月前向上級或監督機關(中央目的事業主管機關)，提出資通安全維護計畫實施情形²⁵，使其得瞭解本機關之年度資通安全計畫實施情形。

壹拾柒、相關法規、程序及表單

一、相關法規及參考文件

- 1. 資通安全管理法
- 2. 資通安全管理法施行細則
- 3. 資通安全責任等級分級辦法
- 4. 資通安全事件通報及應變辦法
- 5. 資通安全情資分享辦法

²⁴ 格式可參附件：改善績效追蹤報告。

²⁵ 資通安全維護計畫實施情形之內容，包含上開定期評估、稽核機制、缺失之消除或改正及機關辦理資通安全計畫之相關實施事項，參附件：資通安全維護計畫實施情形。

6. 公務機關所屬人員資通安全事項獎懲辦法
7. 資訊系統風險評鑑參考指引
8. 政府資訊作業委外安全參考指引
9. 無線網路安全參考指引
10. 網路架構規劃參考指引
11. 行政裝置資安防護參考指引
12. 政府行動化安全防護規劃報告
13. 安全軟體發展流程指引
14. 安全軟體設計指引
15. 安全軟體測試指引
16. 資訊作業委外安全參考指引
17. 本機關資通安全事件通報及應變程序

二、附件表單

1. 資通安全推動小組成員及分工表
2. 資通安全保密同意書
3. 資通安全需求申請單
4. 資訊及資通系統資產清冊
5. 風險評估表
6. 風險類型暨風險對策參考表
7. 管制區域人員進出登記表
8. 委外廠商執行人員保密切結書、保密同意書
9. 委外廠商查核項目表
10. 年度資通安全教育訓練計畫
11. 資通安全認知宣導及教育訓練簽到表
12. 資通安全維護計畫實施情形
13. 資通安全稽核計畫

14. 稽核項目紀錄表
15. 稽核結果紀錄表
16. 稽核委員聘任同意保密切結書
17. 稽核結果及改善報告
18. 改善績效追蹤報告

資通安全維護計畫範本參考附件

目 次

1. 資通安全推動小組成員及分工表.....	1
2. 資通安全保密同意書	2
3. 資通安全需求申請單	3
4. 管制區域人員進出登記表	4
5. 委外廠商執行人員保密切結書、保密同意書	5
6. 委外廠商查核項目表	9
7. 年度資通安全教育訓練計畫	14
8. 資通安全認知宣導及教育訓練簽到表	16
9. 資通安全維護計畫實施情形	17
10. 資通安全稽核計畫	20
11. 稽核項目紀錄表	22
12. 稽核委員聘任同意暨保密切結書	23
13. 稽核結果及改善報告	25
14. 改善績效追蹤報告	26

1. 資通安全推動小組成員及分工表

○○○（機關名稱）資通安全推動小組成員及分工表

編號：○○

製表日期：106 年○○月○○日

單位職級	名稱	職掌事項	分機	備註 (代理人)
EX：資訊 室 專員	王○○	資通安全事件通報	○○	王○○

資通安全長¹：陳○○

註：陳核層級請機關依需求調整

¹ 特定非公務機關部分，可能是資通安全管理代表等相關資通安全負責人。

2. 資通安全保密同意書

○○○（機關名稱）資通安全保密同意書

編號：○○

立同意書人____○○○____於民國____○○____年____○○____月____○○____日起於____○○____任職，因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

- 一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。
- 二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。
- 三、遵守其他本單位資通安全相關之法令及規定。
- 四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：____○○○____(簽章)

身份證字號：____○○○____

服務機關：____○○____

機關首長：____○○○____

中 華 民 國 年 月 日

3. 資通安全需求申請單

○○○（機關名稱）資通安全需求申請單

編號：○○

申請單位	○○部門	申請日期	106 年○○月○○日
申請項目	☒ 軟體 ☐ 硬體 ☐ 其他	項目名稱	○○防毒軟體
申請數量	1	需用日期	106 年○○月○○日
申請類別	☒ 新購 ☐ 升級	使用設備	☒ 主機 ☐ 使用者電腦 ☐ 其他
安裝單位	資訊室	安裝位置	機房
用途說明	防毒軟體更新		
申請人	○○○	單位主管	○○○
資通安全推動小組	☒ 可採購 ☐ 不可採購	說明：	
資通安全推動小組承辦人員	○○○	資通安全長 ²	○○○

註：陳核層級請機關依需求調整

² 特定非公務機關部分，可能是資通安全管理代表等相關資通安全負責人。

4. 管制區域人員進出登記表

○○○（機關名稱）管制區域人員進出登記表

編號：○○

製表日期：106 年○○月○○日

編號	姓名	單位	配同人員	日期	進入時間	離開時間	事由	權限	進出設備	攜帶物品
1	王○○	○○室	陳○○	106.3.1	8：00	9：00	借用電腦設備	普	手提電腦	手機

承辦人員：陳○○

單位主管：林○○

註：陳核層級請機關依需求調整

5. 委外廠商執行人員保密切結書、保密同意書

○○○（機關名單）委外廠商執行人員保密切結書

立切結書人_____（簽署人姓名）等，受_____（廠商名稱）委派至_____（機關名稱，以下稱機關）處理業務，謹聲明恪遵機關下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

- 一、未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。
- 二、未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。
- 三、經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。
- 四、廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。
- 五、機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。
- 六、本保密切結書不因立切結書人離職而失效。
- 七、立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：

姓名及簽章	身分證字號	聯絡電話及戶籍地址
_____	_____	_____
_____	_____	_____

立切結書人所屬廠商：

廠商名稱及蓋章

廠商負責人姓名及簽章

廠商聯絡電話及地址

填表說明：

- 一、廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結機關網路者為限）及經常到機關洽公之業務人員皆須簽署本切結書。
- 二、廠商駐點服務人員、專責維護人員及經常到機關洽公之業務人員每年簽署本切結書乙次。

中 華 民 國 年 月 日

○○○（機關名單）委外廠商執行人員保密同意書

茲緣於簽署人_____（簽署人姓名，以下稱簽署人）參與_____（廠商名稱，以下稱廠商）得標_____（機關名稱）（以下稱機關）資通業務委外案_____（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

- 第一條 簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。
- 第二條 簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。
- 第三條 簽署人在下述情況下解除其所應負之保密義務：
- 原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。
- 原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。
- 原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。
- 第四條 簽署人若違反本同意書之規定，機關得請求簽署人及其任職之廠商賠償機關因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。
- 第五條 簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。
- 第六條 本同意書一式叁份，機關、簽署人及_____（廠商）各執存一份。

簽署人姓名及簽章：

身分證字號：

聯絡電話：

戶籍地址：

所屬廠商名稱及蓋章：

所屬廠商負責人姓名及簽章：

所屬廠商地址：

中 華 民 國 年 月 日

6. 委外廠商查核項目表

○○○（機關名單）委外廠商查核項目表

編號：○○

填表日期：○○○年○○月○○日

查核人員：○○○

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	■	□	□	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	■	□	□	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	■	□	□	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	■	□	□	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	■	□	□	將資安訊息公告於布告欄。
2.設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	■	□	□	指派副首長擔任資安長。
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	■	□	□	有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3 是否訂定組織之資通安全責任分工？	■	□	□	機關內部訂有資安責任分工組織。
3.配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	■	□	□	有訂定人員錄用之安全評估措施
	3.2 是否符合組織之需求配置專業資安人力？	■	□	□	機關依規定配置資安人員2人。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	3.3 是否具備相關專業資安證照或認證？	■	□	□	專業人員具備ISO27001之證照
	3.4 是否配置適當之資源？	□	■	□	機關並未投入足夠資安資源。
4.資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	■	□	□	依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？	■	□	□	資產依規定指定管理者及使用者。
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	■	□	□	資訊訂有分級處理之作業規範。
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	■	□	□	已進行風險評估及擬定相應之控制措施。
5.資通安全管理措施之實施情況	5.1 人員進入重要實體區域是否訂有安全控制措施？	■	□	□	機房訂有門禁管制措施。
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	■	□	離職人員之權限未刪除。
	5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	□	■	□	對於進出人員並未監督其活動。
	5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	■	□	□	按時檢測機房物理面之情況。
	5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	■	□	□	依規定定期檢查並按時提供同仁安全設備之使用運轉。
	5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	□	■	□	並未陪同或監視第三方支援人員。
	5.7 重要資訊處理設施是否有特別保護機制？	□	■	□	對於核心系統主機並未設置特別保護機制。
	5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	■	□	□	定期檢查物理面之風險。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.9 電源之供應及備援電源是否作安全上考量？	■	□	□	有設置備用電源。
	5.10 通訊線路及電纜線是否作安全保護措施？	□	■	□	電纜線老舊，並未設有安全保護措施。
	5.11 設備是否定期維護，以確保其可用性及完整性？	■	□	□	設備按期維護。
	5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？	■	□	□	訂有相關之保護措施。
	5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	■	□	□	攜帶式設備訂有保護措施。
	5.14 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	■	□	□	設備報廢前均有進行資料清除程序。
	5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	□	■	□	人員下班後並未將機敏性公文妥善存放。
	5.16 系統開發測試及正式作業是否區隔在不同之作業環境？	■	□	□	系統開發測試與正式作業區隔。
	5.17 是否全面使用防毒軟體並即時更新病毒碼？	■	□	□	按時更新病毒碼。
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	■	□	□	定期進行相關系統之病毒掃瞄。
	5.19 是否定期執行各項系統漏洞修補程式？	■	□	□	定期進行漏洞修補。
	5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	■	□	□	系統設有檢查之機制。
	5.21 重要的資料及軟體是否定期作備份處理？	■	□	□	有定期做備份處理。
	5.22 備份資料是否定期回復測試，以確保備份資料之有效性？	■	□	□	備份資料均有測試。
	5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	■	□	□	均有設加密之保護措施。
	5.24 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	■	□	□	訂有可攜式媒體之管理程序。
	5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	■	□	□	訂有使用者存取權限註冊及註銷之作業程序。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	☐	☒	☐	未定期檢視使用者存取權限。
	5.27 通行碼長度是否超過 6 個字元(建議以 8 位或以上為宜)？	☒	☐	☐	通行碼符合規定。
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	☒	☐	☐	通行碼符合規定。
	5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	☒	☐	☐	依規定訂定適當之存取權限。
	5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	☒	☐	☐	對於特定網路有訂定相關之控制措施。
	5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	☒	☐	☐	有針對行動式電腦訂定管理政策。
	5.32 重要系統是否使用憑證作為身份認證？	☒	☐	☐	針對重要系統設有身份認證。
	5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	☒	☐	☐	系統更新後相關措施仍有效。
	5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	☒	☐	☐	可即時取得系統弱點並採取應變措施。
6.訂定資通安全事件通報及應變之程序及機制	5.1 是否建立資通安全事件發生之通報應變程序？	☒	☐	☐	有訂定通報應變程序。
	5.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	☒	☐	☐	同仁及委外廠商均知悉通報應變程序，並定期宣導。
	5.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	☒	☐	☐	有留存相關紀錄。
7.定期辦理資通安全認知宣導及教育訓練	7.1 是否定期辦理資通安全認知宣導？	☒	☐	☐	有定期辦理宣導。
	7.2 是否對同仁進行資安評量？	☒	☐	☐	按期進行資安評量。
	7.3 同仁是否依層級定期舉辦資通安全教育訓練？	☒	☐	☐	有定期辦理教育訓練。
	7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	☒	☐	☐	同仁均瞭解單位之資通安全政策及目標。
8.資通安全維護	8.1 是否設有稽核機制？	☒	☐	☐	訂有稽核機制。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
計畫實施情形之精進改善機制	8.2 是否訂有年度稽核計畫？	■	□	□	有訂定年度稽核計畫。
	8.3 是否定期執行稽核？	■	□	□	有按期執行稽核。
	8.4 是否改正稽核之缺失？	■	□	□	訂有稽核後之缺失改正措施。
9.資通安全維護計畫及實施情形之績效管考機制	10.1 是否訂定安全維護計畫持續改善機制？	■	□	□	有訂定持續改善措施。
	10.2 是否追蹤過去缺失之改善情形？	■	□	□	有追蹤缺失改善之情形。
	10.3 是否定期召開持續改善之管理審查會議？	■	□	□	定期召開管理審查會議。

單位主管：陳○○

資通安全長³：林○○

註：陳核層級請機關依需求調整

³ 特定非公務機關部分，可能是其資安代表，或單位之資安負責人員。

7. 年度資通安全教育訓練計畫

○○○（機關名單）○○○年度資通安全教育訓練計畫

壹、依據

○○○（機關名稱）之資通安全維護計畫辦理。

貳、目的

為精進所屬人員之資通安全意識及職能，並敦促該等人員得以瞭解並執行（本機關）之資通安全維護計畫，以強化（本機關）之資通安全管理能量，爰要求該等人員應接受資通安全之教育訓練，爰擬定本教育訓練計畫。

參、實施範圍（各機關自行定義）

本機關所屬人員：

人員類別	人數
資通安全專責人員	○○
一般人員	○○
主管人員	○○
共計	○○

肆、訓練項目（各機關自行定義）

人員類別	訓練課程 ⁴	時數
資通安全專責人員	電子郵件安全 ○○	○○

⁴ 可參考行政院國家資通安全會報技術服務中心之資安職能課程項目，網址：
<https://www.nccst.nat.gov.tw/Capacity?lang=zh>

資訊人員	資訊系統風險管理 ○○	
一般人員	資訊安全通識 ○○	○○
主管人員	○○	○○

伍、訓練期程（各機關自行定義）

由各機關自行排定教育訓練期程。

陸、訓練方式（各機關自行定義）

由各機關自行決定教育訓練方式(實體課程、線上課程...)。

8. 資通安全認知宣導及教育訓練簽到表

○○○（機關名單）資通安全認知宣導及教育訓練 簽到表

編號：○○○

課程名稱：資安宣導課程-案例分享、資安防護重點及社交工程等

時 間：107 年○○月○○日 8：00－9：00

地 點：會議室

單 位	職 稱	姓 名	簽 名
人事室	專員	○○○	

9. 資通安全維護計畫實施情形

○○○（機關名單）資通安全維護計畫實施情形

編號：○○

本機關(單位)之業務因涉及全國性民眾個人資料檔案之持有及處理，經主管機關核定後本單位之資通安全責任等級為A級，依資通安全管理法第12條之規定，向鈞部（院）提出本（107）年度資通安全維護計畫實施情形、執行成果及相關說明如下表所示：

實施項目	實施內容	實施情形說明 (下列內容為範例，請機關依自身情形填寫對應的說明，並提供證明，如計畫、程序、記錄或相關公文等)
1. 核心業務及其重要性	1.1 核心業務及重要性盤點	本機關核心業務及重要性詳參資通安全維護計畫（詳附件，下同）。
2. 資通安全政策及目標之訂定	2.1 資通安全政策訂定及核定	本機關已訂定資通安全政策，詳參資通安全維護計畫，並經資安長核定（詳公文附件）。
	2.2 資通安全目標之訂定	本機關已訂定資通安全目標，詳參資通安全維護計畫。
	2.3 資通安全政策及目標宣導	本機關為推動資通安全政策，已定期向同仁及利害關係人進行宣達。
	2.4 資通安全政策及目標定期檢視	本機關已定期召開資通安全管理審查會議中檢討資通安全政策及目標之適切性（詳會議記錄）。
3. 設置資通安全推動組織	3.1 設定資通安全長	本機關已指定○○長為資通安全長，其職掌詳參資通安全維護計畫。
	3.2 設置資通安全推動小組	本機關已設置資通安全推動小組，其組織、分工及職常詳參資通安全維護計畫。
4. 專責人力及經費之配置	4.1 專職(責)人員配置	本機關依規定配置資通安全專職人員四人，並具備資通安全專業證照及資通安全職能評量證書各四張。另因其

		業務內容將涉及機密性資料，故已進行相關安全評估。
	4.2 經費之配置	本機關今年視需求已合理分資安經費，資安經費佔資訊經費之○○%。
5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	本機關已於今年○月盤點本機關之資訊、資通系統，建立資產目錄。
	5.2 機關資通安全責任等級分級	本機關依資通安全責任等級分級辦法，為資通安全責任等級 A 級機關。
6. 資通安全風險評估	6.1 資通安全風險評估	本機關已於今年○月完成本機關之資訊、資通系統及相關資產之風險分析評估及處理。
	6.2 資通安全風險之因應	本機關已依資通安全風險評估之結果擬定對應之資通安全防護及控制措施。
7. 資通安全防護及控制措施	7.1 資通安全防護及控制措施	本機關已依依安全維護計畫辦理，詳附件資料。(導入 CNS27001 機關)
	7.1 資訊及通系統之保管	本機關已依依安全維護計畫辦理，詳附件資料。(以下為未導入 CNS27001 機關之範例)
	7.2 存取控制與加密機制管理	本機關已依依安全維護計畫辦理。
	7.3 作業及通訊安全管理	本機關已依依安全維護計畫辦理。
	7.4 系統獲取、開發及維護	本機關已依依安全維護計畫辦理。
	7.5 執行資通安全健診	本機關已依依安全維護計畫辦理。
8. 資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制	本機關已依規定訂定資通安全事件通報應變程序。(詳附件)
	8.2 資通安全事件通報、應變及演練	本機關已依規定進行資通安全事件通報。 本機關已依規定於今年○、○月辦理社交工程演練，並於○月辦理通報應變演練。
9. 資通安全情資之評估及因應機制	9.1 資通安全情資之分類評估	本機關接受情資後，已進行分類評估。
	9.2 資通安全情資之因應措施	本機關已接受情資之分類，採取對應

		之因應措施。
10. 資通系統或服務委外辦理之管理	10.1 選任受託者應注意事項	本機關資通系統或服務委外辦理時，已將選任受託者應注意事項加入招標文件中。
	10.2 監督受託者資通安全維護情形應注意事項	本機關已依規定監督受託者資通安全維護情形，客製他資通系統開發者，已要求其出具安全性檢測證明....(請機關依實際情形列出)。
11. 資通安全教育訓練	11.1 資通安全教育訓練要求	本機關人員已規定進行資通安全教育訓練。
	11.2 辦理資通安全教育訓練	本機關已於今年○月辦理資通安全教育訓練。
12. 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	12.1 訂定考核機制並進行考核	本機關已建立考核機制，並已依規定進行平時及年終考核。
13. 資通安全維護計畫及實施情形之持續精進及績效管理機制	13.1 資通安全維護計畫之實施	本機關已依規定訂定各階文件、流程、程序或控制措施，據以實施並保存相關之執行成果記錄。
	13.2 資通安全維護計畫實施情形之稽核機制	本機關已依規定辦理內部稽核。
	13.3 資通安全維護計畫之持續精進及績效管理	本機關已依規定辦理內部召開管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
其他說明		

單位主管：陳○○

資通安全長：陳○○

註：陳核層級請機關依需求調整

10. 資通安全稽核計畫

○○○（機關名單）○○年度資通安全稽核計畫

壹、依據⁵

- 一、○○○（單位名稱）之資通安全維護計畫辦理。（內部稽核用）
- 二、資通安全管理法第十三條規定辦理。（稽核所屬機關用）
- 三、……（請機關自行列出依據）

貳、目的

為瞭解本機關資通安全維護計畫執行之有效性，爰擬定本稽核計畫，執行稽核作業。

參、稽核期程

- （各機關自行定義）
- 由各機關自行排定稽核期程。

肆、稽核團隊成員

- （各機關自行定義）
- 由各機關自行考量稽核之需求，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，稽核團隊人數原則為3至7人。

伍、稽核範圍

- （各機關自行定義）
- 全機關

陸、稽核項目及內容

- （各機關自行定義）
- 依據各機關安全維護之內容，並參考國際資訊安全管理標準 ISO 27001:2013、國際資訊技術服務管理標準 ISO 20000、「個人資料保護法」、「個人資料保護法施行細則」、「政府機關(構)資通安全責任等級分級作業規定」或「資訊系統分級與資安防護基準作業規定」等，以及其他相關規定，由各機關自行定義當年度之稽核項目、內容及執行方式。
- 一、核心業務及其重要性：（內容由各機關自行定義）
- 二、資通安全政策及目標：（內容由各機關自行定義）

⁵ 各機關可依執行稽核之類別填列適當之依據。

- 三、資通安全推動組織：(內容由各機關自行定義)
- 四、專責人力及經費之配置：(內容由各機關自行定義)
- 五、公務機關資通安全長之配置：(內容由各機關自行定義)
- 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：(內容由各機關自行定義)
- 七、資通安全風險評估：(內容由各機關自行定義)
- 八、資通安全防護及控制措施：(內容由各機關自行定義)
- 九、資通安全事件通報、應變及演練相關機制：(內容由各機關自行定義)
- 十、資通安全情資之評估及因應機制：(內容由各機關自行定義)
- 十一、資通系統或服務委外辦理之管理措施：(內容由各機關自行定義)
- 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：(內容由各機關自行定義)
- 十三、資通安全維護計畫及實施情形之持續精進及績效管理機制：(內容由各機關自行定義)

柒、改善作業

(各機關自行定義)

由各機關自行評估對於稽核結果表現優良者是否給予行政獎勵，並針對缺失或待改善項目者研擬後續追蹤方式及頻率(如將前次稽核結果納入本次稽核範圍中追蹤辦理情形及進度)。

11. 稽核項目紀錄表

○○○（單位名稱）稽核項目紀錄表

稽核日期：○○○年○○月○○日

稽核範圍：全機關

受稽核單位	稽核項目	稽核結果	備註
EX：總務科	資產盤點	☒ 符合 ☐ 不符合 ☐ 不適用	經驗證其資產項目表，按規定進行資產盤點，各項資產均依規定建檔並指派責任人。
EX：人事室	權限控管	☐ 符合 ☒ 不符合 ☐ 不適用	可使用高權限登入 A 網站，提供一般同仁進行課程報到作業外，亦可查詢所有同仁之個人資料。
		☒ 符合 ☐ 不符合 ☐ 不適用	
		☒ 符合 ☐ 不符合 ☐ 不適用	
		☒ 符合 ☐ 不符合 ☐ 不適用	
		☒ 符合 ☐ 不符合 ☐ 不適用	
附註			
受稽核人員：王○○			受稽核單位主管：黃○○

註：陳核層級請機關依需求調整

12. 稽核委員聘任同意暨保密切結書

○○○（機關名稱）○○○（計畫名稱）

稽核委員聘任同意暨保密切結書

本人_____（以下簡稱甲方）為協助○○○（以下簡稱乙方）執行「○○○」（以下簡稱本計畫），接受乙方之邀請，擔任 107 年資安稽核團隊之稽核委員，特立書同意事項如下：

- 一、 甲方應遵守國家機密保護法、個人資料保護法、行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、著作權法及其他相關法令之規定，並對因執行本計畫或因執行本計畫之機會所知悉之機密資訊負有保密義務；且上開各義務不因甲方與乙方或與技服中心間，就本年度擔任稽核委員相關事宜之法律關係解除、終止或完成而失其效力。
- 二、 甲方就因執行本計畫或因執行本計畫之機會，所知悉或接觸之乙方、受稽機關或其他第三人之機密資訊，除因執行本計畫所必須，且事先經乙方書面同意者，或法律另有明文規定外，不得有下列行為：
 - （一）全部或一部重製或留存上開機密資訊；
 - （二）以任何方式向任何第三人揭露上開機密資訊之全部或一部；
 - （三）以任何方式使任何第三人知悉、持有或使用上開機密資訊之全部或一部；
 - （四）以任何方式使自己或任何第三人就上開機密資訊之全部或一部取得任何權利；
 - （五）揭露、公開或使用上開機密資訊之全部或一部。
- 三、 甲方因執行本計畫所製作之報告、文件或其他產出，其智慧財產權及其他權利均歸屬乙方所有。
- 四、 甲方與受稽機關有下列情形之一者，就與該受稽機關之稽核相關事宜，應主動迴避，或事先以書面告知乙方，以確認是否得免予迴避：
 - （一）甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人，與受稽機關間，有財產上或非財產上利益之利害關係者；
 - （二）甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬，與受稽機關或其負責人間現有或於過去兩年間曾有僱傭、承攬、委任、代理或其他類似之關係者；
 - （三）甲方或其現任職或於過去兩年內曾任職之機關，於民國 105 年至本次稽核期間，曾為受稽機關進行與受稽事項相關之顧問輔導者。
- 五、 前條所稱財產上利益，係指動產、不動產、現金、有價證券、債權、其他財產上權

本文件之智慧財產權屬行政院資通安全處擁有。

利、具有經濟價值或得以金錢交易取得之利益；所稱非財產上利益，係指有利於甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人於受稽機關或其關聯機關之任用、陞遷、調動及其他人事措施。

- 六、 有其他情形足認甲方有不能公正執行職務之虞，經受稽機關敘明理由，並由乙方作成迴避決定者，甲方應迴避之。
- 七、 甲方有第四條各款情形之一，而未自行迴避，亦未事先以書面告知乙方相關情事，並經乙方書面同意免予迴避者，乙方得終止本契約，甲方應返還已收取之報酬，如乙方，因此認有必要對受稽核機關重為全部或一部稽核，或受有其他不利益時，甲方並應賠償乙方因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。
- 八、 甲方如違反第二條或就相關事宜涉及其他不法情事，將移送司法機關處理；如致乙方、受稽機關，遭受任何不利益，或受第三人法律上請求或訴追者，甲方應賠償乙方、受稽機關，因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。
- 九、 甲方應公正執行職務，並應避免使人誤認推薦特定廠商、產品或服務；且處理稽核相關事務或出席會議，應親自為之。

此 致

○○○（機關名稱）；

受稽機關

立 同 意 書 人

姓 名： （簽章）

身 份 證 字 號：

中 華 民 國 年 月 日

13. 稽核結果及改善報告

○○○（機關名稱）稽核結果及改善報告

稽核範圍	全機關			
稽核日期	107 年 00 月 00 日			
審查日期	107 年 00 月 00 日			
改善措施				
編號	稽核缺失或待改善稽核項目	改善措施	改善期程規劃	相關證明資料
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

單位主管：陳○○

資通安全長：陳○○

註：陳核層級請機關依需求調整

14. 改善績效追蹤報告

○○○（機關名單）改善績效追蹤報告

編號：○○

製表日期：○○○○

稽核發現			
稽核日期	<u>106</u> 年 <u>10</u> 月 <u>20</u> 日 <u>08</u> 時		受稽核單位 ○○○
稽核區域	■ <u>電腦機房</u> <u>委外業務之監督措施</u> <u>自動備份系統之安全措施</u>		
缺失或待改善項目與內容	待改善項目：電腦機房所設置之預備電源設備老舊。 缺失項目：委外廠商未定期為保養相關設備。		
影響範圍評估	將影響電腦機房之運作及相關非核心系統之線上服務之提供。		
發生原因分析	未落實監督委外廠商管理之責任。		
改善措施成效追蹤			
改善措施		預計成效	執行情況
管理面	定期進行委外廠商承辦人員之教育訓練，已落實對委外廠商之監督責任。	要求委外廠商每季進行保養，並提供相關保養紀錄。	已與委外廠商接洽。
技術面			

人力面			
資源面	更新相關電腦機房設備，並確保備份設備及機制運作效果。	電腦機房電源設備更新，並採用不斷電系統，於停電時可維持 12 小時運作。	已進行採購作業。
作業程序			
其他			
績效管考			
改善措施確認	☒ 合格／完成 ☐ 待追蹤(追蹤期限：_____年_____月_____日) ☐ 不合格(說明：_____)		
經費需求或編列執行金額	○○○萬元。	經費執行情形	已進行相關電腦機房設備更新採購，共執行○○萬元。
預定完成日期	<u>106</u> 年 <u>11</u> 月 <u>20</u> 日	實際完成日期	<u>106</u> 年 <u>11</u> 月 <u>20</u> 日
完成進度或情形說明	定期檢視委外廠商之監督維護責任。		
改善成效考核			
後續成效追蹤			
資通安全推動小組	○○○	資通安全長 ⁶	○○○

註：陳核層級請機關依需求調整

⁶ 特定非公務機關部分，可能是資通安全管理代表等相關資通安全負責人。

公務機關資通安全事件通報及應變管理程序

(範本)

目錄

壹、 目的.....	2
貳、 適用範圍.....	2
參、 責任.....	2
肆、 事件通報窗口及緊急處理小組.....	2
伍、 通報程序.....	3
陸、 應變程序.....	5
柒、 資安事件後之復原、鑑識、調查及改善機制.....	6
捌、 紀錄留存及管理程序之調整.....	6
玖、 演練作業.....	7

壹、目的

〇〇〇(以下簡稱本機關(請依需求替換為本部、本局、本府…。等，下同))為遵照資通安全管理法第 14 條及本機關資安全維護計畫之規定，建立本機關資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序(以下稱本管理程序)。

貳、適用範圍

發生於本機關之事件，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者。

參、責任

- 一、本機關所屬人員於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。
- 二、本機關應於資通安全事件發生前，確保所屬或監督之公務機關及所管之特定非公務機關是否制定及落實資通安全事件通報及應變管理程序，並依規定指定其知悉資通安全事件之通報以及完成應變作業後之結案登錄方式。
- 三、本機關應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變管理程序，並於知悉資通安全事件後向本機關進行通報，於完成事件之通報及應變程序後，依本機關指示提供相關之紀錄或資料。
- 四、本機關應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依上級或監督機關及行政院指定之方式進行結案登錄作業，並送交調查、處理及改善報告。
- 五、本機關應於資通安全事件發生前，確認所管之非公務機關資通安全事件通報之方式，並於知悉其資通安全事件後，依規定向行政院通報(本項僅中央目的事業主管機關適用)

肆、事件通報窗口及緊急處理小組

- 一、本機關之資通安全事件通報窗口及聯繫專線為：（各機關自行定義）
- 二、本機關應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。
- 三、本機關所屬人員發現資通安全事件後，應立即向所屬單位主管及本機關之

通報窗口通報。

- 四、本機關應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。
- 五、負責事件處理之單位(該事件發生之單位)權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。
- 六、事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立緊急處理小組，立即協助進行處理；接獲本機關所屬機關或受託廠商所通報之資通安全事件時，亦同。
- 七、緊急處理小組成員由資通安全長指派機關之資通安全相關技術人員擔任，或亦得由其他機關資通安全相關技術人員或外部專家擔任之。
- 八、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

本機關之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

1. 事件涉及核心業務或關鍵基礎設施業務之資訊與否。
2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。
3. 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。
4. 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。
5. 事件其他足以影響資通安全事件等級之因素。

(二)除事件之等級外，權責人員或緊急處理小組亦應對資通安全事件之影響範圍、損害程度及本機關因應之能力進行評估。

(三)本機關權責人員或緊急處理小組於完成資通安全事件等級之判斷及相關評估後，應盡速報資通安全長核准。

(四)除因網路或電力中斷等事由，致無法依上級或監督機關及行政院所指定或

認可之方式通報外，應於知悉資通安全事件後一小時內上級或監督機關及行政院所指定或認可之方式，進行事件通報。

- (五)本機關因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於知悉資通安全事件後一小時內以電話或其他適當方式，將該次資安事件應通報之內容及無法通報依規定方式通報之事由，分別告知所屬之上級或監督機關及行政院，並於事由解除後，依原方式補行通報。
- (六)資通安全事件等級如有變更，權責人員或緊急應變小組應告知通報窗口，使其續行通報作業。
- (七)本機關於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向本機關之權責人員或窗口，以指定之方式進行通報。
- (八)本機關於知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，權責人員或緊急處理小組應於知悉資通安全事件後一小時內，將該事件依上級機關或行政院所指訂或認可之方式，通知該機關。
- (九)本機關執行通報應變作業時，得視情形向直屬上級機關或直轄市、縣（市）政府（機關自行視其位階自行修改請求對象）提出技術支援或其他協助之需求。

二、接獲自身、所屬（監督）機關或所管特定非公務機關通報之評估作業程序

- (一)本機關之權責人員或緊急處理小組，於接獲所屬（監督）機關或所管特定非公務機關之資通安全事件通報後，應於以下時限內，完成資通安全事件通報等級及相關事項之審核：
 - 1. 通報為第一級或第二級之資通安全事件，於接獲通報後八小時內。
 - 2. 通報為第三級或第四級之資通安全事件，於接獲通報後二小時內。
- (二)本機關之權責人員或緊急處理小組進行本條第一項之審核過程中，得請求通報之公務或特定非公務機關提供級別判斷所需之資料或紀錄。
- (三)本機關於必要時得依據審核之結果，逕行變更資通安全事件之等級，並應於決定變更後一小時內，將審核結果及級別變更之決定通知行政院，並提供做成決定所依據之相關資訊。
- (四)本機關於知悉所管特定非公務機關發生第三級或第四級之資通安全事件或收受所管特定非公務機關之第三級或第四級資通安全事件通報後，應於完成審核後一小時內依行政院指定或認可之方式通知行政院。（本項係中央目的事業主管機關適用）

(五)本機關於知悉所管特定非公務機關發生第一級或第二級之資通安全事件或收受所管特定非公務機關之第一級或第二級資通安全事件通報後，應依行政院指定或認可之方式，定期彙整相關資訊送交行政院。(本項係中央目的事業主管機關適用)

三、對所屬或所管特定非公務機關之協助

本機關之所屬機關或特定非公務機關知悉資通安全事件，向本機關為通報時，本機關資通安全長應視必要性於以下時限內，決定是否組成緊急處理小組，以協助隸屬本機關之所屬機關或特定非公務機關執行通報及應變程序，並視情形提供必要之支援或協助：

1. 通報為第一級或第二級之資通安全事件，於完成複核後二小時內。
2. 通報為第三級或第四級之資通安全事件，於接獲通報後一小時內。

陸、應變程序

一、事件發生前之防護措施規劃

本機關應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

二、損害控制機制

(一)負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄

1. 資安事件之衝擊及損害控制作業。
2. 資安事件所造成損害之復原作業。
3. 資安事件相關鑑識及其他調查作業。
4. 資安事件之調查與處理及改善報告之方式。
5. 資安事件後續發展及與其他事件關聯性之監控。
6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。
7. 其他資通安全事件應變之相關事項。

(二)對於第一級、第二級資通安全事件，本機關應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本機關應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

- (三)本機關完成通報及應變程序之辦理後，應依所隸屬之上級機關或行政院所指定或認可之方式進行結案登錄。
- (四)本機關於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。
- (六)本機關於接獲特定非公務機關之損害控制、復原與事件之調查及處理作業完成通知後，應依行政院所指定或認可之方式進行結案登錄。(本項係中央目的事業主管機關適用)

柒、資安事件後之復原、鑑識、調查及改善機制

- 一、本機關完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。
- 二、資通安全事件調查、處理及改善報告應包括以下項目：
 - (一)事件發生、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)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。
 - (六)前款措施之預定完成時程及成效追蹤機制。
- 三、本機關應向所隸屬之上級機關及行政院提出前項之報告，以供監督與檢討。
- 四、本機關指示隸屬於本機關之所屬機關或特定非公務機關提出第二項報告之期限，若其逾期未提出，本機關除應使其盡速提出外，並應為其他必要之監督及指示。

捌、紀錄留存及管理程序之調整

- 一、本機關應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「資安事件通報紀錄單」上留存完整之紀錄，該文件並應經承辦之權責人員、資通安全長簽核。
- 二、本機關於完成資通安全事件之通報及應變程序後，應依據「資安事件通報紀錄單」之內容及實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

玖、演練作業

- 一、本機關應每年依資通安全事件通報應變辦法之規定辦理社交工程演練、資通安全事件通報及應變演練，並於完成後一個月內，將執行情形及成果報告¹送交主管機關。(本項適用總統府、中央一級機關及中央一級機關之直屬機關(構)及直轄市、縣(市)政府、縣(市)議會)
- 二、本機關應配合總統府、中央一級機關及中央一級機關之直屬機關(構)及直轄市、縣(市)政府(請機關視情形擇一)依資通安全事件通報應變辦法之規定所辦理之社交工程演練、資通安全事件通報及應變演練。(本項適用總統府、中央一級機關及中央一級機關之直屬機關(構)及直轄市、縣(市)政府、縣(市)議會外之公務機關)
- 三、本機關應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：
 - (一)社交工程。
 - (二)資安事件通報及應變
 - (三)網路攻防
 - (四)情境演練
 - (五)其他資安演練

¹ 參錯誤! 找不到參照來源。。

特定非公務機關資通安全事件通報及應變管理程序 (範本)

目錄

壹、 目的.....	2
貳、 適用範圍.....	2
參、 責任.....	2
肆、 事件通報窗口及緊急處理小組.....	2
伍、 通報程序.....	3
陸、 應變程序.....	4
柒、 資安事件後之復原、鑑識、調查及改善機制.....	5
捌、 紀錄留存及管理程序之調整.....	5
玖、 演練作業.....	5

壹、目的

〇〇〇(以下簡稱本機關(請依需求替換為本公司、本基金會…。等，下同))為遵照資通安全管理法第 18 條及本機關資安全維護計畫之規定，建立本機關資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序(以下稱本管理程序)。

貳、適用範圍

發生於本機關之事件，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者。

參、責任

- 一、本機關所屬人員於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。
- 二、本機關應於資通安全事件發生前，確保同仁及權責人員熟悉資通安全事件之通報及完成應變作業程序。
- 三、本機關應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變管理程序，並於知悉資通安全事件後向本機關進行通報，於完成事件之通報及應變程序後，依本機關指示提供相關之紀錄或資料。
- 四、本機關應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依依中央目的事業主管機關指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

肆、事件通報窗口及緊急處理小組

- 一、本機關之資通安全事件通報窗口及聯繫專線為：（各機關自行定義）
- 二、本機關應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。
- 三、本機關所屬人員發現資通安全事件後，應立即向所屬單位主管及本機關之通報窗口通報。
- 四、本機關應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

- 五、負責事件處理之單位(該事件發生之單位)權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。
- 六、事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向資通安全管理代表報告，由資通安全管理代表成立緊急處理小組，立即協助進行處理；接獲受託廠商所通報之資通安全事件時，亦同。
- 七、緊急處理小組成員由資通安全管理代表指派機關之資通安全相關技術人員擔任，或亦得聘任外部專家擔任之。
- 八、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

本機關之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

1. 事件涉及核心業務或關鍵基礎設施業務之資訊與否。
2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。
3. 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。
4. 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。
5. 事件其他足以影響資通安全事件等級之因素。

(二)除事件之等級外，權責人員或緊急處理小組亦應對資通安全事件之影響範圍、損害程度及本機關因應之能力進行評估。

(三)本機關權責人員或緊急處理小組於完成資通安全事件等級之判斷及相關評估後，應盡速報資通安全管理代表核准。

(四)除因網路或電力中斷等事由，致無法依中央目的事業主管機關所指定或認可之方式通報外，應於知悉資通安全事件後一小時內依中央目的事業主管機關所指定或認可之方式，進行事件通報。

(五)本機關因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於知悉資通安全事件後一小時內以電話或其他適當方式，將該次資安事件應

通報之內容及無法通報依規定方式通報之事由，分別告知所屬之中央目的事業主管機關，並於事由解除後，依原方式補行通報。

- (六)資通安全事件等級如有變更，權責人員或緊急應變小組應告知通報窗口，使其續行通報作業。
- (七)本機關於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向本機關之權責人員或窗口，以指定之方式進行通報。
- (八)本機關執行通報應變作業時，得視情形向中央目的事業主管機關提出技術支援或其他協助之需求。

陸、應變程序

一、事件發生前之防護措施規劃

本機關應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

二、損害控制機制

- (一)負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄
 - 1. 資安事件之衝擊及損害控制作業。
 - 2. 資安事件所造成損害之復原作業。
 - 3. 資安事件相關鑑識及其他調查作業。
 - 4. 資安事件之調查與處理及改善報告之方式。
 - 5. 資安事件後續發展及與其他事件關聯性之監控。
 - 6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。
 - 7. 其他資通安全事件應變之相關事項。
- (二)對於第一級、第二級資通安全事件，本機關應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本機關應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。
- (三)本機關完成通報及應變程序之辦理後，應依中央目的事業主管機關所指定或認可之方式進行結案登錄。

- (四)本機關於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

柒、資安事件後之復原、鑑識、調查及改善機制

一、本機關完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

二、資通安全事件調查、處理及改善報告應包括以下項目：

- (一)事件發生、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)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。
- (六)前款措施之預定完成時程及成效追蹤機制。

三、本機關應向中央目的事業主管機關提出前項之報告，以供監督與檢討。

捌、紀錄留存及管理程序之調整

- 一、本機關應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「資安事件通報紀錄單」上留存完整之紀錄，該文件並應經承辦之權責人員、資通安全管理代表簽核。
- 二、本機關於完成資通安全事件之通報及應變程序後，應依據「資安事件通報紀錄單」之內容及實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

玖、演練作業

- 一、本機關應於每年年初訂定社交工程演練、資通安全事件通報及應變演練計畫，並於每年12月底前完成組織內部之資通安全演練作業¹。(本項適用總統府、中央一級機關及中央一級機關之直屬機關(構)及直轄市、縣(市)政府、縣(市)議會)

¹ 參錯誤! 找不到參照來源。。

二、本機關應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：

(一)網路攻防

(二)情境演練

(三)其他資安演練

資通安全事件通報單

政府機關(構)應至國家資通安全通報應變網站 (<http://www.ncert.nat.gov.tw>) 通報資安事件，若因故無法上網填報，可先填具本通報單以傳真或郵寄方式傳送至國家資通安全會報政府資通安全組，惟待網路連線恢復後仍需上網補登通報。

傳真專線：(02)27331655

郵寄地址：台北市大安區 106 富陽街 116 號

諮詢專線：(02)27339922

注意事項

1. 「☒」為必填項目。
2. 請依通報之資安「事件分類」填寫通報單，並依事件類別回傳通報單內容。
3. 事件通報的部分請回傳 P1-P3，事件通報並結案的部分請根據事件分類回傳對應的頁碼(網頁攻擊 P1-P7、非法入侵 P1-P3,P8-P10、阻斷服務 P1-P3,P11-P12、設備異常 P1-P3,P13-P14、其他 P1-P3,P15-P17)

◎填報時間：____年____月____日____時____分

STEP1.請填寫事件相關基本資料

一、發生資通安全事件之機關(機構)聯絡資料：

- ◎機關(機構)名稱：_____◎主管機關名稱：_____
- ◎通報人：_____◎電話：_____傳真：_____
- ◎電子郵件信箱：_____
- ◎是否代其他機關(構)通報：☐是，該單位名稱_____ ☐否
- ◎資安監控中心(SOC)：☐無 ☐機關自行建置
- ☐委外建置，該廠商名稱_____
- ◎資安維護廠商：_____

STEP2.請詳述事件發生過程

二、事件發生過程：

- ◎事件發生時間：____年____月____日____時____分
- ◎事件分類與異常狀況：(事件分類為單選項；異常狀況為複選項)
- ☐網頁攻擊
- ☐網頁置換 ☐惡意留言 ☐惡意網頁 ☐釣魚網頁
- ☐網頁木馬 ☐網站個資外洩
- ☐非法入侵
- ☐系統遭入侵 ☐植入惡意程式 ☐異常連線 ☐發送垃圾郵件
- ☐資料外洩
- ☐阻斷服務(DoS/DDoS)
- ☐服務中斷 ☐效能降低

○設備問題

☐設備毀損 ☐電力異常 ☐網路服務中斷 ☐設備遺失

○其他：_____

◎事件說明及影響範圍：

◎是否影響其他政府機關(構)或重要民生設施運作：☐是 ☐否

◎此事件通報來源：☐自行發現 ☐警訊通知，發布編號：_____

STEP3.評估事件影響等級

三、事件影響等級：

◎請分別評估資安事件造成之機密性、完整性以及可用性衝擊：

資安事件影響等級為機密性、完整性及可用性衝擊最嚴重者(數字最大者)

—機密性衝擊：(單選)

- ☐國家機密資料遭洩漏(4 級)
- ☐密級或敏感公務資料遭洩漏(3 級)
- ☐核心業務(含關鍵資訊基礎設施)一般資料遭洩漏(2 級)
- ☐非核心業務一般資料遭洩漏(1 級)
- ☐無資料遭洩漏(無需通報)

—完整性衝擊：(單選)

- ☐關鍵資訊基礎設施系統或資料遭嚴重竄改(4 級)
- ☐核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改(3 級)
- ☐非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改(2 級)
- ☐非核心業務系統或資料遭竄改(1 級)
- ☐無系統或資料遭竄改(無需通報)

—可用性衝擊：(單選)

- ☐關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作(4 級)
- ☐核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(3 級)
- ☐非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(2 級)
- ☐非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常

運作(1 級)

☐無系統或設備運作受影響(無需通報)

Step4.評估是否需要外部支援

四、期望支援項目：

☒是否需要支援：

☐是（請續填期望支援內容） ☐否（免填期望支援內容）

期望支援內容：（請勿超過 200 字）

Step5.請填寫機關緊急應變措施-網頁攻擊(請回傳 P1-P7)

五、完成損害控制與復原：

◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

☐ 已保存遭入侵主機事件紀錄檔〈單選〉

〈☐1 個月 ☐1-6 個月 ☐6 個月以上 ☐其他_____〉

☐ 已保存防火牆紀錄〈單選〉

〈☐1 個月 ☐1-6 個月 ☐6 個月以上 ☐其他_____〉

☐ 已保存網站日誌檔〈單選〉

〈☐1 個月 ☐1-6 個月 ☐6 個月以上 ☐其他_____〉

☐ 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共_____個

☐ 其他保留資料或資料處置說明【如未保存資料亦請說明】

◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)，經分析已保存之紀錄，是否發現下列異常情形：

☐ 異常連線行為【請列出異常 IP 與異常連線原因，如：存取後台管理頁面】

☐ 異常帳號使用【請列出帳號並說明帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

☐ 清查網頁目錄內容，網站內存在未授權之程式/檔案【請說明程式名稱或路徑、檔名】

☐ 網站資料庫內容遭竄改

☐ 發現資料外洩情況【如：異常打包資料，請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

☐ 影響評估說明補充【請填寫補充說明】

◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於

「應變措施補充說明」欄位說明)因應分析結果，執行處置措施：

- ☐ 移除未授權存在之惡意網頁/留言/檔案，共____筆(必填)
【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】

- ☐ 將異常外部連線 IP 列入阻擋清單(必填)【請說明設定阻擋之資訊
設備與阻擋之 IP，如無須阻擋，請填寫「無」】

- ☐ 停用/刪除異常帳號(必填)【請說明停用/刪除之帳號，如無須刪
除，請填寫「無」】

- ☐ 移除網站外洩資料
- ☐ 通知事件相關當事人，並依內部資安通報作業向上級呈報
- ☐ 暫時中斷受害主機網路連線行為至主機無安全性疑慮
- ☐ 已向搜尋引擎提供者申請移除庫存頁面〈複選〉
《☐Google☐Yahoo☐Yam(蕃薯藤) ☐Bing☐Hinet
☐其他搜尋引擎提供者_____》
- ☐ 修改網站程式碼，並檢視其他網站程式碼，完成日期_____
- ☐ 重新建置作業系統與作業環境，完成日期_____
- ☐ 應變措施補充說明【請填寫補充說明】

STEP6.資安事件結案作業-網頁攻擊(請回傳 P1-P7)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計_____臺；伺服器總計_____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址 (Web-URL) (無；可免填)：_____

◎作業系統名稱、版本：

☐Windows 系列 ☐Linux 系列 ☐其他作業平台 版本：_____

◎已裝置之安全機制：

☐防火牆 ☐防毒軟體 ☐入侵偵測系統 ☐入侵防禦系統 ☐其他：_____

◎受害系統是否通過資安管理認證(ISMS)：☐是 ☐否

◎事件發生原因〈單選〉

〈☐作業系統漏洞☐弱密碼☐應用程式漏洞☐網站設計不當

☐人為疏失☐設定錯誤☐系統遭入侵☐其他_____〉

◎請簡述事件處理情況：_____

◎補強措施〈複選〉

I. 補強系統/程式安全設定

☐ 已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密碼等)(**必填**)

☐ 已完成評估變更受害主機中所有帳號之密碼(含本機管理者) (**必填**)

☐ 已完成檢視/更新受害主機系統與所有應用程式至最新版本(包含網站編輯管理程式，如：FrontPage) (**必填**)【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

☐ 關閉網路芳鄰功能

☐ 設定 robots.txt 檔，控制網站可被搜尋頁面

☐ 已針對所有需要特殊存取權限之網頁加強身分驗證機制【請說明機制名稱或類別】

☐ 限制網站主機上傳之附件檔案類型【請說明附檔名】

-
- ☐ 限制網頁存取資料庫的使用權限，對於讀取資料庫資料的帳戶身分及權限加以管制
 - ☐ 限制連線資料庫之主機 IP
 - ☐ 關閉 WebDAV(Web Distribution Authoring and Versioning)

II. 資安管理與教育訓練

- ☐ 重新檢視機關網路架構適切性
- ☐ 機關內部全面性安全檢測
- ☐ 加強內部同仁資安教育訓練
- ☐ 修正內部資安防護計畫

◎其他相關安全處置【請填寫其他安全處置】

◎完成修復時間：____年____月____日____時____分

Step5.請填寫機關緊急應變措施-非法入侵(請回傳 P1-P3、P8-P10)

五、完成損害控制與復原：

◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

- ☐ 已保存遭受害主機事件紀錄檔〈單選〉
〈☐1 個月 ☐1-6 個月 ☐6 個月以上 ☐其他_____〉
- ☐ 已保存防火牆紀錄〈單選〉
〈☐1 個月 ☐1-6 個月 ☐6 個月以上 ☐其他_____〉
- ☐ 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共_____個
- ☐ 其他保留資料或資料處置說明【如未保存資料亦請說明】

◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)經分析已保存之紀錄，是否發現下列異常情形：

- ☐ 異常連線行為【請列出異常 IP 與異常連線，如：存取後台管理頁面】

- ☐ 異常帳號使用【請列出帳號並說帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

- ☐ 發現資料外洩情況【如：異常打包資料，請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

- ☐ 影響評估補充說明【請填寫補充說明】

◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)因應分析結果，執行處置措施：

- ☐ 移除未授權存在之惡意網頁/留言/檔案/程式，共_____筆(必填)
【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】

- ☐ 將可疑 IP/Domain Name 列入阻擋清單(必填)【請說明設定阻擋之

資訊設備與阻擋之 IP，如無須阻擋，請填寫「無」】

- ☐ 停用/刪除異常帳號(必填)【請說明停用/刪除之帳號，如無須移除，請填寫「無」】

- ☐ 中斷受害主機網路連線行為至主機無安全性疑慮
- ☐ 重新建置作業系統與作業環境，完成日期_____
- ☐ 惡意程式樣本送交防毒軟體廠商，共_____個
- ☐ 應變措施補充說明【請填寫補充說明】

Step6.資安事件結案作業-非法入侵(請回傳 P1-P3、P8-P10)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計_____臺；伺服器總計_____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址（Web-URL）(無；可免填)：_____

◎作業系統名稱、版本：

☐Windows 系列 ☐Linux 系列 ☐其他作業平台 版本：_____

◎已裝置之安全機制：

☐防火牆 ☐防毒軟體 ☐入侵偵測系統 ☐入侵防禦系統 ☐其他：_____

◎受害系統是否通過資安管理認證(ISMS)：☐是 ☐否

◎事件發生原因〈單選〉

〈☐社交工程☐作業系統漏洞☐弱密碼☐應用程式漏洞☐網站設計不當
☐系統遭入侵☐其他_____〉【請說明事件調查情況】

◎補強措施〈複選〉

I. 補強系統/程式安全設定〈複選〉

- ☐ 已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密

碼等) (必填)

☐ 已完成評估變更受害主機中所有帳號密碼之必要性(含本機管理者) (必填)

☐ 已完成檢視/更新受害主機系統與所有應用程式至最新版本(必填)

【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

☐ 關閉郵件伺服器 Open Relay 功能

☐ 關閉網路芳鄰功能

II. 資安管理與教育訓練(複選)

☐ 重新檢視機關網路架構適切性

☐ 機關內部全面性安全檢測

☐ 加強內部同仁資安教育訓練

☐ 修正內部資安防護計畫

◎其他相關安全處置【請填寫其他安全處置】

◎已解決時間：____年____月____日____時____分

Step5.請填寫機關緊急應變措施-阻斷服務(DoS/DDoS) (請回傳 P1-P3、P11-P12)

五、完成損害控制與復原：

◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

☐ 已保存遭入侵主機事件檢視器〈單選〉

〈☐1 個月 ☐1-6 個月 ☐6 個月以上 ☐其他_____〉

☐ 已保存防火牆紀錄〈單選〉

〈☐1 個月 ☐1-6 個月 ☐6 個月以上 ☐其他_____〉

☐ 已保存受攻擊主機封包紀錄(☐10 分鐘 ☐10-30 分鐘 ☐30-60 分鐘)

☐ 其他保留資料或資料處置說明【如未保存資料亦請說明】

◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)

☐ 攻擊來源 IP 數量_____個

☐ 確認遭攻擊主機用途【請說明主機用途】

☐ 影響評估補充說明

◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)

☐ 阻擋攻擊來源 IP(必填)【請說明設定阻擋之資訊設備與阻擋之 IP，如無須阻擋，請填寫「無」】

☐ 調整網路頻寬

☐ 聯繫網路服務提供業者(ISP)_____(請提供 ISP 業者名稱)，請其協助進行阻擋

☐ 應變措施補充說明【請填寫補充說明】

Step6.資安事件結案作業-阻斷服務(DoS/DDoS) (請回傳 P1-P3、P11-P12)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計_____臺；伺服器總計_____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址（Web-URL）（無；可免填）：_____

◎作業系統名稱、版本：

☐Windows 系列 ☐Linux 系列 ☐其他作業平台 版本：_____

◎已裝置之安全機制：

☐防火牆 ☐防毒軟體 ☐入侵偵測系統 ☐入侵防禦系統 ☐其他：_____

◎受害系統是否通過資安管理認證(ISMS)：☐是 ☐否

◎補強措施〈複選〉

I. 補強系統/程式安全設定〈複選〉

☐ 限制同時間單一 IP 連線

☐ DNS 主機停用外部遞迴查詢

☐ 已完成檢視/移除主機/伺服器不必要服務功能(必填)【請說明服務功能名稱，如無須移除，請填寫「無」】

☐ 已完成檢視/更新受害主機系統與所有應用程式至最新版本(必填)
【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

II. 資安管理與教育訓練〈複選〉

☐ 重新檢視機關網路架構適切性

☐ 修正內部資安防護計畫

◎其他相關安全處置【請填寫其他安全處置】

◎已解決時間：____年____月____日____時____分

Step5.請填寫機關緊急應變措施-設備異常(請回傳 P1-P3、P13-P14)

◎保留受害期間之相關設備紀錄資料

- ☐ 其他保留資料或資料處置說明【如未保存資料亦請說明】

◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)

- ☐ 評估設備影響情況

〈☐無資料遭損毀

☐資料損毀，但可由備份檔案還原

☐資料損毀，且資料無法復原

☐資料損毀，僅可復原部分資料____%〉

- ☐ 遺失設備存放資料性質說明

〈個人敏感性資料、機密性資料、非機敏性資料，請說明內容〉

- ☐ 影響評估補充說明

◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)

- ☐ 毀損資料/系統已恢復正常運作

- ☐ 完成系統復原測試

- ☐ 通知事件相關當事人，並依內部資安通報作業向上級呈報【如遺失設備存有敏感資料，此選項為必填】

- ☐ 應變措施補充說明【請填寫補充說明】

Step6.資安事件結案作業-設備異常(請回傳 P1-P3、P13-P14)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計____臺；伺服器總計____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址（Web-URL）（無；可免填）：_____

◎作業系統名稱、版本：

☐Windows 系列 ☐Linux 系列 ☐其他作業平台 版本：_____

◎已裝置之安全機制：

☐防火牆 ☐防毒軟體 ☐入侵偵測系統 ☐入侵防禦系統 ☐其他：_____

◎受害系統是否通過資安管理認證(ISMS)：☐是 ☐否

◎事件發生原因〈單選〉

〈☐設定錯誤☐設備毀損☐系統遭入侵☐電力供應異常☐人為疏失
☐其他_____〉【請說明事件調查情況】

◎補強措施〈複選〉

I. 補強系統/程式安全設定

☐檢視資訊設備使用年限

II. 資安管理與教育訓練〈複選〉

☐重新檢視機關網路架構適切性

☐機關內部全面性安全檢測

☐加強內部同仁資安教育訓練

☐修正內部資安防護計畫

◎其他相關安全處置【請填寫其他安全處置】

◎已解決時間：____年____月____日____時____分

Step5.請填寫機關緊急應變措施-其他(請回傳 P1-P3、P15-P17)

◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

- ☐ 已保存遭入侵主機事件檢視器〈單選〉
〈☐1 個月 ☐1-6 個月 ☐6 個月以上 ☐其他_____〉
- ☐ 已保存防火牆紀錄〈單選〉
〈☐1 個月 ☐1-6 個月 ☐6 個月以上 ☐其他_____〉
- ☐ 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共____個
- ☐ 其他保留資料或資料處置說明【如未保存資料亦請說明】

◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)經分析已保存之紀錄，是否發現下列異常情形：

- ☐ 異常連線行為【請列出異常 IP 與異常連線原因，如：存取後台管理頁面】

- ☐ 異常帳號使用【請列出帳號並說明帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

- ☐ 發現資料外洩情況【如：異常打包資料，請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

- ☐ 影響評估補充說明【請填寫補充說明】

◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)

- ☐ 移除未授權存在之惡意網頁/留言/檔案/程式，共____筆(必填)
【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】

- ☐ 將可疑 IP/Domain Name 列入阻擋清單(必填)【請說明設定阻擋之資訊設備與阻擋之 IP，如無須阻擋，請填寫「無」】

- ☐ 停用/刪除異常帳號(必填)【請說明停用/刪除之帳號，如無須移除，請填寫「無」】

- ☐ 暫時中斷受害主機網路連線行為至主機無安全性疑慮
- ☐ 重新建置作業系統與作業環境，完成日期_____
- ☐ 惡意程式樣本送交防毒軟體廠商，共__個
- ☐ 應變措施補充說明【請填寫補充說明】

Step6.資安事件結案作業-其他(請回傳 P1-P3、P15-P17)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計_____臺；伺服器總計_____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址 (Web-URL) (無；可免填)：_____

◎作業系統名稱、版本：

☐Windows 系列 ☐Linux 系列 ☐其他作業平台 版本：_____

◎已裝置之安全機制：

☐防火牆 ☐防毒軟體 ☐入侵偵測系統 ☐入侵防禦系統 ☐其他：_____

◎受害系統是否通過資安管理認證(ISMS)：☐是 ☐否

◎事件發生原因〈單選〉

〈☐社交工程☐作業系統漏洞☐弱密碼☐應用程式漏洞

☐網站設計不當☐人為疏失☐設定錯誤☐設備毀損

☐系統遭入侵☐電力供應異常☐其他_____〉【請說明事件調查情況】

◎補強措施〈複選〉

I. 補強系統/程式安全設定〈複選〉

- ☐ 已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密碼等) (必填)

☐ 已完成評估變更受害主機中所有帳號密碼之必要性(含本機管理

者) (必填)

☐ 已完成檢視/更新受害主機系統與所有應用程式至最新版本(必填)

【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

☐ 關閉網路芳鄰功能

II. 資安管理與教育訓練(複選)

☐ 重新檢視機關網路架構適切性

☐ 機關內部全面性安全檢測

☐ 加強內部同仁資安教育訓練

☐ 修正內部資安防護計畫

◎其他相關安全處置【請填寫其他安全處置】

◎已解決時間：____年____月____日____時____分

○○○（單位名稱）資通安全事件調查、處理及改善報告範本

通 報 部 門		事 件 發 生 時 間	
完 成 通 報 時 間		結 案 登 錄 時 間	
通 報 事 件 等 級	☒ 一級 ☐ 二級 ☐ 三級 ☐ 四級		
事 件 歸 類 （請參酌應變紀錄）	☐ 網頁攻擊 ☒ 非法入侵 ☐ 阻斷服務 ☐ 設備問題 ☐ 其他：		
事 件 等 級 判 斷 依 據			
事 件 說 明			
原 因 肇 因			
調 查 經 過			
復 原 作 業			
改 善 措 施			

備 註			
權 責 人 員		資 通 安 全 長	

資通安全演練成果報告

編號：○○○

製表日期：○○○年○○月○○日

演練單位：人事室		演練時間：○○○年○○月○○日下午○○時○○分至○○○年○○月○○日下午○○時○○分
實施單位：稽核小組		
演練項目		演練情況概述
1.	EX：社交工程演練	寄發社交工程信件，造成人員電腦中毒的通報應變。
2.	...	...
演練結果		
合格項目	EX：依規定進行通報。	
不合格項目	EX：未依規定與受影響之其他機關聯繫。	
待改善項目	EX：通報紀錄單填寫不完整。	
其他	...	
演練結果檢討與待改善事項		
(由各單位自行填寫)		

資通安全維護計畫

目 錄

壹、 依據及目的	3
貳、 適用範圍	3
參、 核心業務及重要性	3
一、 核心業務及重要性：	4
二、 非核心業務及說明：	5
肆、 資通安全政策及目標	5
一、 資通安全政策	6
二、 資通安全目標	6
三、 資通安全政策及目標之核定程序	7
四、 資通安全政策及目標之宣導	7
五、 資通安全政策及目標定期檢討程序	7
伍、 資通安全推動組織	7
一、 資通安全長	8
二、 資通安全推動小組	9
陸、 專職(責)人力及經費配置	10
一、 專職(責)人力及資源之配置	10
二、 經費之配置	11
柒、 資訊及資通系統之盤點	12
一、 資訊及資通系統盤點	12
二、 機關資通安全責任等級分級	13
捌、 資通安全風險評估	13
一、 資通安全風險評估	14
二、 核心資通系統及最大可容忍中斷時間	14
玖、 資通安全防護及控制措施	15
一、 資訊及資通系統之管理	16

二、存取控制與加密機制管理.....	17
三、作業與通訊安全管理.....	19
四、系統獲取、開發及維護.....	24
五、業務持續運作演練	25
六、執行資通安全健診	25
七、資通安全防護設備	25
壹拾、資通安全事件通報、應變及演練相關機制	26
壹拾壹、資通安全情資之評估及因應	26
一、資通安全情資之分類評估.....	26
二、資通安全情資之因應措施.....	27
壹拾貳、資通系統或服務委外辦理之管理	28
一、選任受託者應注意事項.....	28
二、監督受託者資通安全維護情形應注意事項.....	29
壹拾參、資通安全教育訓練	29
一、資通安全教育訓練要求.....	30
二、資通安全教育訓練辦理方式.....	30
壹拾肆、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	30
壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制	31
一、資通安全維護計畫之實施.....	31
二、資通安全維護計畫實施情形之稽核機制	31
三、資通安全維護計畫之持續精進及績效管理.....	32
壹拾陸、資通安全維護計畫實施情形之提出	33
壹拾柒、相關法規、程序及表單	33
一、相關法規及參考文件.....	33
二、附件表單	34

壹、依據及目的

範例一：

本計畫依據資通安全管理法第 10 條及施行細則第 6 條訂定。

範例二：

本計畫依據下列法規訂定：

- 一、資通安全管理法第 10 條及其施行細則第 6 條。
- 二、其他業務法規名稱。

貳、適用範圍

範例一：

本計畫適用範圍涵蓋本○全機關。

範例二：

本計畫適用範圍除本○全機關外，另包含(請依實際情形列出適
其他機關名稱)機關。

參、核心業務及重要性

撰寫說明：

- 本章重點在揭示組織之核心業務，並說明核心業務失效時對國人日常生活、社會經濟、政府功能之影響。
- 機關核心業務請依據資通安全管理法施行細則第 7 條規定及政府機關組織法列示。
- 資安責任等級為 A 級及 B 級機關如已進行業務營運衝擊分析，亦可援引敘明。
- 另為進行資通安全事件等級判定，機關仍應針對輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等非核心業務進行盤點，並列出最大可容忍中斷時間。

● 範例如下：

範例：

一、核心業務及重要性：

本機關之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
		☐ 為主管機關指定之關鍵基礎設施 ☐ 為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 ☐ 為本機關依組織法執掌，足認為重要者	財務損失： 民眾生命財產損失： 經濟發展受阻： 影響其他機關業務運作(相依性)： 違反法遵義務： 機關信譽： 其他：	
全國公務人員人事管理(範例)	全國公務人員人事管理系統	☐ 為主管機關指定之關鍵基礎設施 ☒ 為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 ☐ 為本機關依組織法執掌，足認為重要者	違反法遵義務：依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依受罰。	4 小時

各欄位定義：

1. 核心業務名稱：請參考資通安全管理法施行細則第 7 條¹之規定

¹一、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者。

列示。

2. 作業名稱：該項業務內各項作業程序的名稱。
3. 重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。
4. 最大可容忍中斷時間單位以小時計。

二、非核心業務及說明：

本機關之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
公文交換 (範例)	電子公文無法即時送達機關，影響機關行政效率	○小時
其他-非屬上開業務範疇及核心業務者 (範例)	影響機關行政效率	○小時

各欄位定義：

1. 業務名稱：公務機關之非核心業務至少應包含輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等。(請依機關實際情形列出)
2. 作業名稱：該項業務內各項作業程序的名稱。
3. 說明：說明該業務之內容。
4. 最大可容忍中斷時間單位以小時計。

肆、資通安全政策及目標

撰寫說明：

- 本章包含政策內容、目標、核定程序、宣導程序、定期檢討程序等節，機關如已有規定及程序者，可直接引述內部文件編號及名稱。
- 本章經參考行政院及所屬各機關資訊安全管理規範之「壹、資訊安全政策制定及評估」一節，提供範本如下，機關得參酌本

範本修改為機關適用之文件，內容可著重一般同仁應遵守之原則性規定。

一、資通安全政策

為使本機關業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

1. 應建立資通安全風險管理機制，定期因應內外資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 應強固核心資通系統之韌性，確保機關業務持續營運。
4. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本機關同仁之資通安全意識，本機關同仁亦應確實參與訓練。
5. 針對辦理資通安全業務有功人員應進行獎勵。
6. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
7. 禁止多人共用單一資通系統帳號。
8.

二、資通安全目標

（請各機關自行訂定資通安全目標，目標宜有量化與質化型指標，以下僅例示內容供參）

（一）量化型目標

1. 核心資通系統可用性達 99.99% 以上。（中斷時數/總運作時數 $\leq$ 0.1%）（可參考：確保本校關鍵業務系統資訊機房維運服務達全年上班時間 96.9% 以上之可用性，並確保：因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每年不得超過 8 次。因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長

不得超過 8 工作小時。)

2. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
3. 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5% 及 2%。
4.

(二) 質化型目標：(請視實際需要填列)

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免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。
2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。
3. 提升人員資安防護意識、有效偵測與預防外部攻擊等.....

三、資通安全政策及目標之核定程序

資通安全政策由本機關○○單位簽陳資通安全長核定。

四、資通安全政策及目標之宣導

1. 本機關之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。
2. 本機關應每年向利害關係人(例如 IT 服務供應商、與機關連線作業有關單位)進行資安政策及目標宣導，並檢視執行成效。

五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於資通安全管理審查會議中檢討其適切性。

伍、資通安全推動組織

撰寫說明：

- 本章至少包含資通安全長(特定非公務機關可為資通安全管理代

表)、資通安全推動小組之組成及分工職掌等內容。機關規模較大者，亦可於資通安全長(資通安全管理代理)下設置資通安全指導小組及資通安全推動小組，分別負責資通安全規劃及推動作業。機關針對資通安全推動組織如已有規定及程序者，可直接引述內部文件編號及名稱。

- 本章參考行政院及所屬各機關資訊安全管理規範之「貳、資訊安全組織及權責」一節，提供範本如下，機關得參酌本範本修改為機關適用之文件。

範本：

一、資通安全長

(針對特定非公務機關，資通安全長可改為資通安全管理代表)

依本法第 11 條之規定，本機關訂定○長（副首長或適當人員²）為資通安全長，負責督導機關資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。
2. 資通安全責任之分配及協調。
3. 資通安全資源分配。
4. 資通安全防護措施之監督。
5. 資通安全事件之檢討及監督。
6. 資通安全相關規章與程序、制度文件核定。
7. 資通安全管理年度工作計畫之核定
8. 資通安全相關工作事項督導及績效管理。
9. 其他資通安全事項之核定。

² 考量資通安全推動時常涉及機關內相關資源調動及分配等事項，故資通安全長由機關首長指派副首長擔任，如機關首長指派適當人員擔任資通安全長時，該人員應具有足夠權責、資源、權限、相當資歷、經驗及資安專業之人員兼任為宜，使資通安全相關業務得以順利推展。

二、資通安全推動小組

(一) 組織

為推動本機關之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各業務部門主管/副主管以上之人員代表成立資通安全推動小組³，其任務包括：

1. 跨部門資通安全事項權責分工之協調。
2. 應採用之資通安全技術、方法及程序之協調研議。
3. 整體資通安全措施之協調研議。
4. 資通安全計畫之協調研議。
5. 其他重要資通安全事項之協調研議。

(二) 分工及職掌(以下為例示規定，請各機關依實際情形列出分工與職掌)

本機關之資通安全推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項，本機關資通安全推動小組分組人員名單及職掌應列冊，並適時更新之⁴：

1. 策略規劃組：

- (1) 資通安全政策及目標之研議。
- (2) 訂定機關資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。
- (3) 依據資通安全目標擬定機關年度工作計畫。
- (4) 傳達機關資通安全政策與目標。
- (5) 其他資通安全事項之規劃。

2. 資安防護組：

- (1) 資通安全技術之研究、建置及評估相關事項。

³ 資通安全推動小組成員由機關之資通安全長召集組成，依資通安全長之指示，負責協助或與機關內之相關單位合作推動機關內部之資通安全業務，如機關未成立資通安全推動小組，相關業務則應由資通安全長責承相關資通安全權責人員辦理之。

⁴ 各公務機關應製作「資通安全推動小組成員及分工表」，說明小組成員及相關職掌，格式可參附件：資通安全推動小組成員及分工表。

- (2) 資通安全相關規章與程序、制度之執行。
- (3) 資訊及資通系統之盤點及風險評估。
- (4) 資料及資通系統之安全防護事項之執行。
- (5) 資通安全事件之通報及應變機制之執行。
- (6) 其他資通安全事項之辦理與推動。

3. 績效管理組：

- (1) 辦理資通安全內部稽核。
- (2) 每半年(每年)定期召開資通安全管理審查會議，提報資通安全事項執行情形。

陸、專職(責)人力及經費配置

撰寫說明：

- 本章至少包含資安人員配置、訓練及證照，以及資通安全經費或資源之規劃及配置等內容，機關如已有規定及程序者，可直接引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

範本如下：

一、專職(責)人力及資源之配置

1. 本機關依資通安全責任等級分級辦法之規定，屬資通安全責任等級○級，最低應設置資通安全專職(責)人員 4 人，其分工如下，本機關現有資通安全專責人員名單及職掌應列冊，並適時更新⁵。

(以下分工供例示 A 級單位參考，請機關考量實務需求列出)

- (1) 資通安全管理面業務 1 人，負責推動資通系統防護需求分級、資通安全管理系統導入及驗證、內部資通安全稽核、機關資安治理成熟度評估及教育訓練等業務之推動。
- (2) 資通系統安全管理業務 1 人，負責資通系統分級及防護基準、

⁵ 各公務機關應製作「資通安全專職人員分工表」，說明專職人員及相關職掌，格式可參附件：資通安全推動小組成員及分工表。

安全性檢測、業務持續運作演練等業務之推動。

- (3) 資通安全防護業務 1 人，負責資通安全監控管理機制、政府組態基準導入，資通安全防護設施建置及資通安全事件通報及應變業務之推動。
 - (4) 資通安全管理法法遵事項業務 1 人，負責本機關對所屬公務務機關或所管特定非公務機關之法遵義務執行事宜。
2. 本機關之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本機關之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。
 3. 資安專職(責)人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定⁶。
 - (1) 資安專職(責)人員總計應持有 4 張以上資通安全專業證照⁷。
 - (2) 資安專職(責)人員總計應持有 4 張以上資通安全職能評量證書⁸。
 4. 本機關負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定⁹，並視需要實施人員輪調，建立人力備援制度。
 5. 本機關之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。
 6. 專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

二、經費之配置

1. 資通安全推動小組於規劃配置相關經費及資源時，應考量本機關之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源¹⁰。

⁶ 各機關應依據其資通安全責任等級分級辦法所規範之資通安全專責人員、認知與訓練之要求，配置適當之資源於資安人員專業職能之培養。

⁷ 視各機關之資通安全責任等級之分級要求。

⁸ 視各機關之資通安全責任等級之分級要求。

⁹ 格式可參附件：資通安全保密同意書。

¹⁰ 為有效建置機關之資通安全風險防護機制，公務機關應投入相當之資源，故機關之資通安全推動小組於資源規劃或編制預算時，應考量機關之責任等級、資通安全政策及目標。

2. 各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。
3. 各單位如有資通安全資源之需求，應配合機關預算規劃期程向資通安全推動小組提出¹¹，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長(資通安全管理代表)核定後，進行相關之建置。
4. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

柒、資訊及資通系統之盤點

撰寫說明：

- 本章至少包含資訊及資通系統之分類及盤點之程序，並應包含標示核心資通系統及相關資產之要求。機關如已有規定及程序者，可直接引述內部文件編號及名稱。
- 本章經參考行政院及所屬各機關資訊安全管理規範之「捌、資訊資產之安全管理」一節，提供範本如下，機關得參酌本範本修改為機關適用之文件。

範本如下：

一、資訊及資通系統盤點

1. 本機關每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為資訊資產、軟體資產、實體資產、支援服務資產等(分類僅供參考，機關可依實際情形調整)。
2. 資訊及資通系統資產項目如下(供參)：
 - (1) 資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。
 - (2) 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦

¹¹ 各機關可填具資通安全需求申請單，格式可參附件：資通安全需求申請單。

作業系統等。

(3) 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。

(4) 支援服務資產：相關基礎設施及其他機關內部之支援服務，如電力、消防等。

(5) ...(如人員資料：)

3. 本機關每年度應依資訊及資通系統盤點結果¹²，製作「資訊及資通系統資產清冊」¹³，欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級。

4. 資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。核心資通系統及相關資產，並應加註標示。

5. 各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新資產清冊。

二、機關資通安全責任等級分級

本機關因持有全國性民眾個人資料檔案，並負責全國性民眾務之資通系統之推運，為資通安全責任等級 A 級機關。

(請機關依資通安全責任等級分級辦法規定自行修改內容)

A 級單位範例：

本機關屬公務機關，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，為資通安全等級分類 A 級機關。

捌、資通安全風險評估

撰寫說明：

- 本章至少包含風險評估、風險因應等節，機關如已有規定及程序者，可直引述內部文件編號及名稱。

¹² 為使公務機關能依其所屬之資通安全責任等級之分級，執行相關之資通安全防護措施，公務機關應先進行機關內部之資訊及資通系統資產之盤點，使其能依據其所擁有之資訊或資通系統依據資通安全責任等級分級辦法進行風險評估。

¹³ 參資訊系統風險評鑑參考指引附件詳細風險評鑑空白表單之資訊資產表。

- 本章參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」。
- 機關得參酌本範本修改為機關適用之文件。

範本如下：

一、資通安全風險評估

1. 本機關應每年針對資訊及資通系統資產進行風險評估。
2. 執行風險評估時應參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」，並依其中之「詳細風險評鑑方法」進行風險評估之工作。
3. 本機關應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外開發之資通系統防護需求分級。

二、核心資通系統及最大可容忍中斷時間

核心資通系統	資訊資產	最大可容忍中斷時間	核心資通系統主要功能
○○○網站 (範例)	1. 網站前台主機計 3 台 2. 網站後台主機計 1 台 3. 負載平衡伺服器 4. 網路交換器(型號) (提供該網站網路服務之網路設備均需列出)	○小時	提供民眾申辦○○○服務

最大可容忍中斷時間以小時計。

玖、資通安全防護及控制措施

撰寫說明：

- 本章為機關因應資通安全風險，採取之安全防護及控制措施。
- 機關得參酌本範本修改為機關適用之文件。
- 針對需導入 CNS27001 之機關，因其標準中已有相關之規定及程序，僅需針對資通安全責任等級分級辦法中應辦事項列出防護及控制措施。
- 需導入 CNS27001 者亦可導入其他具有同等或以上效果之系統或標準，或教育體系資通安全管理規範，。
- 需導入 CNS27001 之機關範本如下：

本機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施，由於本機關核心資通系統已通過(導入)CNS27001 驗證，全機關之防護及控制措施詳如 CNS27001 資通安全管理系統文件。

(請機關確認現有程序及標準書內容，需滿足以下範本中「未導入 CNS27001 機關之資通安全防護及控制措施」建議內容，如各機關對於非核心系統有不同的管理規定，可加以說明。)

- 針對未導入 CNS27001 之機關，本範例中參考資安治理成熟度評審作業面向，CNS27002 中控制措施之作業規範，提示原則性之準則(Standards)規範，請各依機關視實際情形增修，並針對各項準則定出相關程序(Procedures)文件。
- 不需導入 CNS27001 之機關範本如下：

本機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施如下：

一、資訊及資通系統之管理

(一) 資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。
2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。
3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。
4.其餘可參考 CNS 27002 編號 8.資產管理等相關內容，或可參考教育體系資通安全管理規範 A.8 資產管理等相關內容。

(二) 資訊及資通系統之使用

1. 本機關同仁使用資訊及資通系統前應經其管理人授權。
2. 本機關同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 本機關同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。
4. 非本機關同仁使用本機關之資訊及資通系統，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。
5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。
6.其餘可參考 CNS 27002 編號 8.資產管理等相關內容，或可參考教育體系資通安全管理規範 A.8 資產管理等相關內容。

(三) 資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。
2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。
3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，

或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

4.其餘可參考 CNS 27002 編號 11.2.7 設備汰除或再使用之保全等相關內容，或可參考教育體系資通安全管理規範 A.11.2.7 之內容。

二、存取控制與加密機制管理

(一) 網路安全控管

1. 本機關之網路區域劃分如下：(請機關視實際情形增列)
 - (1) 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。
 - (2) 非軍事區(DMZ)：放置機關對外服務伺服器之區段。
 - (3) 內部區域網路 (Local Area Network, LAN)：機關內部單位人員及內部伺服器使用之網路區段。
2. 外部網路、非軍事區及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。
3. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。
4. 對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。
5. 本機關內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。
6. 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。
7. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。
8. 網域名稱系統(DNS)防護
 - (1) 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。
 - (2) DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管

控機制。

(3) DNS 伺服器應設定指向 GSN Cache DNS。(公務機關適用)

(4) 內部主機位置查詢應指向機關內部 DNS 伺服器。

9. 無線網路防護

(1) 機密資料原則不得透過無線網路及設備存取、處理或傳送。

(2) 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

(3) 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

(4) 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

10.其餘可參考 CNS 27002 編號 9.1.2 對網路及網路服務之存取，以及國家資通安全會報「網路架構規劃參考指引」、「無線網路安全參考指引」等相關內容，或可參考教育體系資通安全管理規範 A.9.1.2 之內容。

(二) 資通系統權限管理

1. 本機關之資通系統應設置通行碼管理，通行碼之要求需滿足：

(1) 通行碼長度 8 碼以上。

(2) 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

(3) 使用者每 90 天應更換一次通行碼。

2. 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

4.其餘可參考 CNS 27002 編號 9.2.1 使用者註冊及註銷、編號 9.2.2 使用者存取權限之配置等相關內容，或可參考教育體系資通安全管理規範 A.9.1.2、A.9.2.2 之內容。

(三) 特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號

授權前應妥善審查其必要性，其授權及審查記錄應留存。

2. 資通系統之特權帳號不得共用。
3. 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。
4. 資通系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。
5. 資通系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。
6.其餘可參考 CNS 27002 編號 9.2.3 具特殊存取權限之管理等相關內容，或可參考教育體系資通安全管理規範 A.9.2.3 之內容。

(四) 加密管理

1. 本機關之機密資訊於儲存或傳輸時應進行加密。
2. 本機關之加密保護措施應遵守下列規定：
 - (1) 應落實使用者更新加密裝置並備份金鑰。
 - (2) 應避免留存解密資訊。
 - (3) 一旦加密資訊具遭破解跡象，應立即更改之。
 - (4) ...
3.其餘可參考 CNS 27002 編號 9.2.4 使用者之秘密鑑別資訊的管理、編號 9.3.1 秘密鑑別資訊之使用等相關內容，或可參考教育體系資通安全管理規範 A.9.2.4、A.9.3.1 之內容。

三、作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本機關之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。
 - (1) 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。
 - (2) 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

- (3) 確實執行網頁惡意軟體掃描。
- (4) ...
- 2. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。
- 3. 使用者不得私自使用已知或有嫌疑惡意之網站。
- 4. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。
- 5.其餘可參考 CNS 27002 編號 12.2.1 防範惡意軟體之控制措施等相關內容，或可參考教育體系資通安全管理規範 A.12.2.1 之內容。

(二) 遠距工作之安全措施

- 1. 本機關資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。
- 2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。
- 3. 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。
 - (1) 提供適當通訊設備，並指定遠端存取之方式。
 - (2) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。
 - (3) 進行遠距工作時之安全監視。
 - (4) 遠距工作終止時之存取權限撤銷，並應返還相關設備。
- 4.其餘可參考 CNS 27002 編號 6.2.2 遠距工作等相關內容，或可參考教育體系資通安全管理規範 A.6.2.2 之內容。

(三) 電子郵件安全管理

- 1. 本機關人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。
- 2. 電子郵件系統管理人應定期進行電子郵件帳號清查。
- 3. 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之

必要更新。

4. 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。
5. 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。
6. 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。
7. 使用者應確保電子郵件傳送時之傳遞正確性。
8. 使用者使用電子郵件時，應注意電子簽章之要求事項。
9. 本機關應定期舉辦(或配合上級機關舉辦)電子郵件社交工程演練，並檢討執行情形。
10.其餘可參考 CNS 27002 編號 13.2.3 電子傳輸等相關內容，或可參考教育體系資通安全管理規範 A.13.2.3(電子傳訊)之內容。

(四) 確保實體與環境安全措施

1. 資料中心及電腦機房之門禁管理

- (1) 資料中心及電腦機房應進行實體隔離。
- (2) 機關人員或來訪人員應申請及授權後方可進入資料中心及電腦機房¹⁴，資料中心及電腦機房管理者並應定期檢視授權人員之名單。
- (3) 人員進入管制區應配戴身分識別之標示，並隨時注意身分不明或可疑人員。
- (4) 僅於必要時，得准許外部支援人員進入資料中心及電腦機房。
- (5) 人員及設備進出資料中心及電腦機房應留存記錄。
- (6) ...

2. 資料中心及電腦機房之環境控制

- (1) 資料中心及電腦機房之空調、電力應建立備援措施。

¹⁴ 未具進出管制區權限之人員來訪時，應填具進出登記表，格式可參附件：管制區域人員進出登記表。

- (2) 資料中心及電腦機房之溫濕度管控範圍為：
- (3) 資料中心及電腦機房應安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全引發之危險。
- (4) 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。
- (5) ...

3. 辦公室區域之實體與環境安全措施

- (1) 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
- (2) 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。
- (3) 機密性及敏感性資訊，不使用或下班時應該上鎖。
- (4) 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。
- (5) 顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。
- (6) 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。
- (7) ...

4.其餘可參考 CNS 27002 編號 11.1 保全區域、編號 11.2 設備等相關內容，或可參考教育體系資通安全管理規範 A.11.1(安全區域)、A.11.2 之內容。

(五) 資料備份

- 1. 重要資料及核心資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。
- 2. 本機關應每季確認核心資通系統資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通系統。
- 3. 敏感或機密性資訊之備份應加密保護。
- 4.其餘可參考 CNS 27002 編號 12.3 備份、編號 17.2 多重備援

等相關內容，或可參考教育體系資通安全管理規範 A.12.3、
A.17.2 之內容。

(六) 媒體防護措施

1. 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
2. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。
3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。
4. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。
5.其餘可參考 CNS 27002 編號 8.3 媒體處置等相關內容，或可參考教育體系資通安全管理規範 A.8.3(媒體處理)之內容。

(七) 電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
3. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
4. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
5. 下班時應關閉電腦及螢幕電源。
6. 如發現資安問題，應主動循機關之通報程序通報。
7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。
8.其餘可參考 CNS 27002 編號 11.2 設備等相關內容，或可參考教育體系資通安全管理規範 A.11.2 之內容。

(八) 行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。
2. 機敏會議或場所不得攜帶未經許可之行動設備進入
3.其餘可參考參考 CNS 27002 編號 6.2.1 行動裝置政策、政府行動化安全防護規劃報告及行動裝置資安防護參考指引，或可參考教育體系資通安全管理規範 A.6.2.1 之內容。

(九) 即時通訊軟體之安全管理

1. 使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。
2. 使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求：
 - (1) 用戶端應有身分識別及認證機制。
 - (2) 訊息於傳輸過程應有安全加密機制。
 - (3) 應通過經濟部工業局訂定行動化應用軟體之中級檢測項目。
 - (4) 伺服器端之主機設備及通訊紀錄應置於我國境內。
 - (5) 伺服器通訊紀錄 (log) 應至少保存六個月。
 - (6) 伺服器主機每年辦理二次弱點掃描及一次滲透測試，且不能出現中風險以上之弱點。
3.其餘可參考行政院及所屬機關使用即時通訊軟體安全管理要點。

四、系統獲取、開發及維護

(有維護、自行或委外開發資通系統機關適用)

1. 本機關之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十中資通系統防護基準，並注意下列事項：
 - (1) 開發過程請依安全系統發展生命週期 (Secure Software Development Life Cycle, SSDLC) 納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。
 - (2) 於資通系統開發前，設計安全性要求，包含機敏資料存取、用

戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。

(3) 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

(4) 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

2.其餘可參考 CNS 27002 編號 14.系統獲取、開發及維護等相關內容，或可參考教育體系資通安全管理規範 A.14 之內容。

五、業務持續運作演練

(有核心資通系統之 C 級機關適用)

本機關應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。

六、執行資通安全健診

(C 級機關適用)

1. 本機關每二年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：

- (1) 網路架構檢視。
- (2) 網路惡意活動檢視。
- (3) 使用者端電腦惡意活動檢視。
- (4) 伺服器主機惡意活動檢視。
- (5) 安全設定檢視。

七、資通安全防護設備

1. 本機關應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。
2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

壹拾、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本機關應訂定資通安全事件通報、應變及演練相關機制，詳資通安全事件通報應變程序¹⁵。

壹拾壹、資通安全情資之評估及因應

撰寫說明：

- 本章為機關接受情資後應採取之評估及因應措施，其內容包括情資分類及情資因應。機關如已有對應之規定及程序者，可直引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

範本如下：

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、資通安全情資之分類評估

本機關接受資通安全情資後，應指定資通安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(二) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動

¹⁵ 各機關應另訂定資通安全事件通報及應變程序。

且證據明確等內容，屬入侵攻擊情資。

(三) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之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，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(四) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、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等內容，屬涉及核心業務、核心資通系統之情資。

二、資通安全情資之因應措施

本機關於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一) 資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(二) 入侵攻擊情資

由資通安全專職(責)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三) 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

(四) 涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資

評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

壹拾貳、資通系統或服務委外辦理之管理

撰寫說明：

- 本章為機關辦理資通系統或服務委外時應注意之事項，其內容包括委外前之選任及委外後之監督。資安法施行細則第4條中除已規範應注意事項外，機關亦可參考最新版本之《資訊作業委外安全參考指引》調整相關內容，並於資訊委外各階段，訂定具體安全需求。機關如已有對應之規定及程序者，可直引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

範本如下：

本機關委外辦理資通系統之建置、維運或資通服務之提供時，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。

一、選任受託者應注意事項

1. 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¹⁶。
2. 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。
3. 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。
4. 受託業務涉及國家機密者，應考量受託業務所涉及國家機密之機密等級內容，於招標公告、招標文件及契約中，註明受託者辦理該項業務人員及可能接觸該國家機密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。(得視情形刪去)
5. 前點適任性查核得在必要範圍內就下列事項查核，查核前應經

¹⁶ 委外單位之管理措施是否完善，可視其人員資格是否具有相關證照、訓練或認證（如 ISO 27001、CISSP、SSCP、各資安教育訓練單位所辦之課程等）做為參考。

當事人書面同意：(得視情形刪去)

- (1) 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者。
- (2) 曾任公務人員因違反相關安全保密規定，受懲戒處分、記過以上行政懲處者。
- (3) 曾受到外國政府、大陸地區或香港、澳門官方之利誘、脅迫，從事不利國家安全或重大利益情事者。
- (4) 其他與國家機密保護相關之具體項目。

二、監督受託者資通安全維護情形應注意事項

1. 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第三方安全性檢測證明；涉及利用非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。
2. 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。
3. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
4. 受託者應採取之其他資通安全相關維護措施¹⁷。
5. 本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¹⁸。

壹拾參、資通安全教育訓練

撰寫說明：

- 本章為機關辦理資通安全教育訓練事宜，其內容教育訓練之要求及辦理方式。機關如已有對應之規定及程序者，可直引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

¹⁷ 公務機關與委外廠商簽訂契約時，應審查契約中保密條款，並要求委外廠商之業務執行人員簽署委外廠商執行人員保密切結書、保密同意書，格式可參附件：委外廠商執行人員保密切結書、保密同意書。

¹⁸ 稽核項目可參委外廠商查核項目表。

範本如下：

一、資通安全教育訓練要求

1. 本機關依資通安全責任等級分級屬 A 級，資安及資訊人員每年至少 4 名人員接受 12 小時以上之資安專業課程訓練或資安職能訓練。
2. 本機關之一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。

二、資通安全教育訓練辦理方式

1. 承辦單位應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫¹⁹，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄²⁰。
2. 本機關資通安全認知宣導及教育訓練之內容得包含：(請視實際情形增列)
 - (1) 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。
 - (2) 資通安全法令規定。
 - (3) 資通安全作業內容。
 - (4) 資通安全技術訓練。
3. 員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。
4. 資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

壹拾肆、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

本機關所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、(請填寫機關內部獎懲辦法及名稱)，及本

¹⁹ 格式可參附件：年度資通安全教育訓練計畫。

²⁰ 公務機關辦理教育訓練時，參加人員應簽名留存紀錄，格式可參附件：資通安全認知宣導及教育訓練簽到表。

機關各相關規定辦理之。

壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制

撰寫說明：

- 本章為機關資通安全維護計畫實施情形之績效管理及持續精進機制，其內容包括維護計畫之實施、稽核及管理審查會議。機關如已有對應之規定及程序者，可直引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

範本如下：

一、資通安全維護計畫之實施

為落實本安全維護計畫，使本機關之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本機關之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、資通安全維護計畫實施情形之稽核機制

(一) 稽核機制之實施

1. 資通安全推動小組應定期(至少每年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。
2. 辦理稽核前資通安全推動小組應擬定資通安全稽核計畫²¹並安排稽核成員，稽核計畫應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²²、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。
3. 辦理稽核時，資通安全推動小組應於執行稽核前○○日，通知受稽單位，並將稽核期程、稽核項目紀錄表²³及稽核流程等相關資訊提供受稽單位。

²¹ 格式可參附件：資通安全稽核計畫。

²² 格式可參附件：稽核委員聘任同意暨保密切結書。

²³ 格式可參附件：稽核項目紀錄表

4. 本機關之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告²⁴中，並提供給受稽單位填寫辦理情形。
5. 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。
6. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼）。

(二) 稽核改善報告

1. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。
2. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。
3. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。
4. 機關應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。
5. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

三、資通安全維護計畫之持續精進及績效管理

1. 本機關之資通安全推動小組應於○○月(每年至少一次)召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
2. 管理審查議題應包含下列討論事項：
 - (1) 過往管理審查議案之處理狀態。
 - (2) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

²⁴ 格式可參附件：稽核結果及改善報告。

- (3) 資通安全維護計畫內容之適切性。
 - (4) 資通安全績效之回饋，包括：
 - A. 資通安全政策及目標之實施情形。
 - B. 資通安全人力及資源之配置之實施情形。
 - C. 資通安全防護及控制措施之實施情形。
 - D. 內外部稽核結果。
 - E. 不符合項目及矯正措施。
 - (5) 風險評鑑結果及風險處理計畫執行進度。
 - (6) 重大資通安全事件之處理及改善情形。
 - (7) 利害關係人之回饋。
 - (8) 持續改善之機會。
3. 持續改善機制之管理審查應做成改善績效追蹤報告²⁵，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾陸、資通安全維護計畫實施情形之提出

本機關依據本法第 11(16,17)條之規定，應於○○月前向上級或監督機關(中央目的事業主管機關)，提出資通安全維護計畫實施情形²⁶，使其得瞭解本機關之年度資通安全計畫實施情形。

壹拾柒、相關法規、程序及表單

一、相關法規及參考文件

- 1. 資通安全管理法
- 2. 資通安全管理法施行細則
- 3. 資通安全責任等級分級辦法
- 4. 資通安全事件通報及應變辦法
- 5. 資通安全情資分享辦法

²⁵ 格式可參附件：改善績效追蹤報告。

²⁶ 資通安全維護計畫實施情形之內容，包含上開定期評估、稽核機制、缺失之消除或改正及機關辦理資通安全計畫之相關實施事項，參附件：資通安全維護計畫實施情形。

6. 公務機關所屬人員資通安全事項獎懲辦法
7. 資訊系統風險評鑑參考指引
8. 政府資訊作業委外安全參考指引
9. 無線網路安全參考指引
10. 網路架構規劃參考指引
11. 行政裝置資安防護參考指引
12. 政府行動化安全防護規劃報告
13. 安全軟體發展流程指引
14. 安全軟體設計指引
15. 安全軟體測試指引
16. 資訊作業委外安全參考指引
17. 本機關資通安全事件通報及應變程序

二、附件表單

1. 資通安全推動小組成員及分工表
2. 資通安全保密同意書
3. 資通安全需求申請單
4. 資訊及資通系統資產清冊
5. 風險評估表
6. 風險類型暨風險對策參考表
7. 管制區域人員進出登記表
8. 委外廠商執行人員保密切結書、保密同意書
9. 委外廠商查核項目表
10. 年度資通安全教育訓練計畫
11. 資通安全認知宣導及教育訓練簽到表
12. 資通安全維護計畫實施情形
13. 資通安全稽核計畫

14. 稽核項目紀錄表
15. 稽核結果紀錄表
16. 稽核委員聘任同意保密切結書
17. 稽核結果及改善報告
18. 改善績效追蹤報告

學校資通安全事件通報及應變管理程序

(範本)

目錄

壹、 目的	2
貳、 適用範圍	2
參、 責任	2
肆、 事件通報窗口及緊急處理小組	2
伍、 通報程序	3
陸、 應變程序	4
柒、 重大(「4」、「3」級)資安事件後之復原、鑑識、調查及改善機制	5
捌、 紀錄留存及管理程序之調整	6
玖、 演練作業	6

壹、目的

〇〇〇(以下簡稱本校(請依需求替換為本中心、本小組…等，下同))為遵照資通安全管理法第 14 條及本校資通安全維護計畫之規定，建立資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序(以下稱本管理程序)。

貳、適用範圍

發生於本校之事件，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者。

參、責任

- 一、本校於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。
- 二、本中心(小組)應於資通安全事件發生前，確保所屬連線學校是否制定及落實資通安全事件通報及應變管理程序，並依規定指定其知悉資通安全事件之通報以及完成應變作業後之結案登錄方式。(連線學校不用填寫)
- 三、本校應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變管理程序，並於知悉資通安全事件後向本部進行通報，於完成事件之通報及應變程序後，依本校指示提供相關之紀錄或資料。
- 四、本校應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依教育部指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

肆、事件通報窗口及緊急處理小組

- 一、臺灣學術網路資通安全事件委託由臺灣學術網路危機處理中心之教育機構資安通報應變小組(簡稱通報應變小組)負責，聯繫資訊如下：

- (一) 聯絡電話：(07)525-0211
- (二) 網路電話：98400000
- (三) 電子郵件：service@cert.tanet.edu.tw

- 二、本校應至少指派二位以上資安聯絡人員，並於「教育機構資安通報應變平

台」(<https://info.cert.tanet.edu.tw>)登錄相關聯絡資料，如有異動亦應立即上網更新。

三、本校之資通安全事件通報窗口及聯繫專線為：**(各校自行定義)**

四、本校應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。

五、本校所屬人員知悉資通安全事件後，應立即至教育機構資安通報平台(<https://info.cert.tanet.edu.tw>)通報登錄資安事件細節、影響等級及支援申請等資訊。

六、本校應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

七、負責事件處理之單位(該事件發生之單位)權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。

八、事件經初步判斷認為可能屬重大(第「三」級、第「四」級)資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立緊急處理小組，立即協助進行處理；接獲本校所屬分校(機關)或受託廠商所通報之資通安全事件時，亦同。

九、緊急處理小組成員由資通安全長指派機關之資通安全相關技術人員擔任，或亦得由其他機關資通安全相關技術人員或外部專家擔任之。

十、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

本校之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

1. 事件涉及核心業務或關鍵基礎設施業務之資訊與否。
2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。
3. 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。

4.機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。

5.事件其他足以影響資通安全事件等級之因素。

(二)本校因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於確認資安事件條件成立後1小時內，與所隸屬區縣市網路中心及通報應變小組聯繫，先行提供該次資安事件應通報之內容及無法通報依規定方式通報之事由，並於事由解除後，依原方式補行通報。

(三)資通安全事件等級如有變更，本校權責人員或通報應變小組應告知通報單位，使其續行通報作業。

(四)本校於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向委託單位所屬之權責人員通知，以指定之方式進行通報。

(五)本校於知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，權責人員或通報應變小組應於知悉資通安全事件後一小時內，將該事件依教育部或行政院所指訂或認可之方式，通知該機關。

(六)本校執行通報應變作業時，得視情形向所隸屬區縣市網路中心人員提出技術支援或其他協助之需求。

二、接獲所屬連線學校通報之評估作業程序（連線學校不用填寫）

(一)本中心(小組)，於接獲所屬連線學校之資通安全事件通報後，應於以下時限內，完成資通安全事件通報等級及相關事項之審核：

1.通報為第一級或第二級之資通安全事件，於接獲通報後八小時內。

2.通報為第三級或第四級之資通安全事件，於接獲通報後二小時內。

(二)本中心(小組)進行本條第一項之審核過程中，得請求通報之提供級別判斷所需之資料或紀錄。

(三)本中心(小組)於必要時得依據審核之結果，逕行變更資通安全事件之等級，並應於決定變更後一小時內，將審核結果及級別變更之決定通知教育部，並提供做成決定所依據之相關資訊。

陸、應變程序

一、事件發生前之防護措施規劃

本校應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資

安事件之發生。

二、損害控制機制

(一)負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄

1. 資安事件之衝擊及損害控制作業。
2. 資安事件所造成損害之復原作業。
3. 重大(第「三」級、第「四」級)資安事件相關鑑識及其他調查作業。
4. 重大(第「三」級、第「四」級)資安事件之調查與處理及改善報告之方式。
5. 重大(第「三」級、第「四」級)資安事件後續發展及與其他事件關聯性之監控。
6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。
7. 其他資通安全事件應變之相關事項。

(二)對於第一級、第二級資通安全事件，本校應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本校應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

(三)本校完成資安事件處理後，須至教育機構資安通報平台填報資安事件處理辦法及完成時間。

(四)本校於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

柒、重大(第「三」級、第「四」級)資安事件後之復原、鑑識、調查及改善機制

一、本校若發生重大(第「三」級、第「四」級)資通安全事件時，於完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

二、重大(第「三」級、第「四」級)資通安全事件調查、處理及改善報告應包

括以下項目：

- (一)事件發生、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)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。
- (六)前款措施之預定完成時程及成效追蹤機制。

三、本校應向所隸屬之上級機關及教育部提出前項之報告，以供監督與檢討。

四、本中心(小組)指示所屬連線學校提出第二項報告之期限，若其逾期未提出，本中心(小組)除應使其盡速提出外，並應為其他必要之監督及指示。
(連線學校不用填寫)

捌、紀錄留存及管理程序之調整

- 一、本校應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「教育機構資安通報平台」上填報完整之紀錄，該平台事件通報應變紀錄由通報應變小組於年度彙整後，提交至本部資訊及科技教育司覆核備查。
- 二、本校於完成資通安全事件之通報及應變程序後，應依據實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

玖、演練作業

- 一、本校應配合教育部依資通安全事件通報應變辦法之規定所辦理之社交工程演練、資通安全事件通報及應變演練。
- 二、本校應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：
 - (一)社交工程。
 - (二)資安事件通報及應變
 - (三)網路攻防
 - (四)情境演練
 - (五)其他資安演練