



建國科技大學

資通安全維護計畫

第1.0版

113年12月26日 頒行



| 資通安全維護計畫 |  |      |      |    |     |
|----------|--|------|------|----|-----|
| 文件編號     |  | 機密等級 | 內部使用 | 版次 | 1.0 |

## 目 錄

|                                    |   |
|------------------------------------|---|
| 壹、依據及目的.....                       | 1 |
| 貳、適用範圍.....                        | 1 |
| 參、核心業務及重要性：.....                   | 1 |
| 一、核心業務重要性及說明.....                  | 1 |
| 二、非核心業務及說明：.....                   | 2 |
| 肆、資通安全政策及目標一、資通安全政策.....           | 2 |
| 伍、資通安全推動組織.....                    | 2 |
| 陸、專職人力及經費配置.....                   | 2 |
| 一、專職人力及資源之配置.....                  | 2 |
| 二、經費之配置.....                       | 3 |
| 柒、資訊及資通系統之盤點與風險評估.....             | 3 |
| 捌、資通安全防護及控制措施.....                 | 4 |
| 一、資訊及資通系統之管理.....                  | 4 |
| 二、存取控制與加密機制管理.....                 | 4 |
| 三、作業與通訊安全管理.....                   | 4 |
| 四、系統獲取、開發及維護.....                  | 4 |
| 五、業務持續運作演練.....                    | 4 |
| 六、執行資通安全健診.....                    | 4 |
| 七、資通安全防護設備.....                    | 4 |
| 玖、資通安全事件通報、應變及演練相關機制.....          | 4 |
| 壹拾、資通安全情資之評估及因應.....               | 5 |
| 一、資通安全情資之分類評估.....                 | 5 |
| 二、資通安全情資之因應措施.....                 | 5 |
| 壹拾壹、資通系統或服務委外辦理之管理.....            | 6 |
| 壹拾貳、資通安全教育訓練.....                  | 6 |
| 壹拾參、本校所屬人員辦理業務涉及資通安全事項之考核機制.....   | 6 |
| 壹拾肆、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..... | 6 |
| 一、資通安全維護計畫之實施.....                 | 6 |
| 二、資通安全維護計畫實施情形之稽核機制與改善精進.....      | 7 |
| 三、資通安全維護計畫之持續精進及績效管理.....          | 7 |
| 壹拾伍、資通安全維護計畫實施情形之提出.....           | 7 |
| 壹拾陸、相關法規、程序及表單.....                | 7 |
| 一、相關法規及參考文件.....                   | 7 |
| 二、附件表單.....                        | 8 |

| 資通安全維護計畫 |  |      |      |    |     |
|----------|--|------|------|----|-----|
| 文件編號     |  | 機密等級 | 內部使用 | 版次 | 1.0 |

### 壹、依據及目的

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。

### 貳、適用範圍

本計畫適用範圍涵蓋本校所有單位。參、核心業務及重要性

### 參、核心業務及重要性：

#### 一、核心業務重要性及說明

本校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 |
|---------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------|
| 校園網路維運  | 學術網路維運系統                    | <input type="checkbox"/> 為主管機關指定之關鍵基礎設施<br><input checked="" type="checkbox"/> 為主管機關核定資通安全責任等級 C 級機關所涉業務<br><input type="checkbox"/> 為本校依組織法執掌，足認為重要者 | 影響機關業務運作(相依性)：影響本校各資訊系統服務的提供與使用。                                                         | 24小時      |
| 教學務資訊管理 | 教學務資訊系統(包含教務系統、學務系統及數位學習系統) | <input type="checkbox"/> 為主管機關指定之關鍵基礎設施<br><input checked="" type="checkbox"/> 為主管機關核定資通安全責任等級 C 級機關所涉業務<br><input type="checkbox"/> 為本校依組織法執掌，足認為重要者 | 影響機關業務運作(相依性)：影響本校各資訊服務相關聯授權系統的資訊提供與服務。<br>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。 | 24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。

| 個人資料檔案安全維護計畫 |  |      |      |    |     |
|--------------|--|------|------|----|-----|
| 文件編號         |  | 機密等級 | 內部使用 | 版次 | 1.0 |

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。  
最大可容忍中斷時間單位以小時計。

## 二、非核心業務及說明：

本校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 |
|----------------|---------------------------------|-----------|
| 學校首頁系統         | 學校全球資訊網無法即時提供服務與訊息公告，將影響機關校譽    | 24 小時     |
| 電子郵件系統(教職員、學生) | 電子郵件無法即時提供寄收信件服務，將影響機關行政效率      | 24 小時     |
| 電子公文系統         | 電子公文無法即時送達機關與機關內之公文交換，將影響機關行政效率 | 48 小時     |
| 人會總系統          | 人事/會計/出納系統無法提供請款銷帳服務，將影響機關行政效率  | 48 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一、資通安全政策

依本校「資通安全政策」如附件一施行。

## 伍、資通安全推動組織

依本校「資通安全暨個人資料保護推動委員會設置辦法」如附件二，成立資通安全暨個人資料保護推動委員會。

## 陸、專職人力及經費配置

### 一、專職人力及資源之配置

1. 本校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 C 級，最低應設置資通安全專職人員 1 人，其職責如下，本校現有資通安全專責人員名單及職掌應列冊，並適時更新。

(1) 資通安全管理面業務，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、內部資通安全稽核及教育訓練等業務之推動。

| 個人資料檔案安全維護計畫 |  |      |      |    |     |
|--------------|--|------|------|----|-----|
| 文件編號         |  | 機密等級 | 內部使用 | 版次 | 1.0 |

- (2) 資通系統安全管理業務，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，負責資通安全監控管理機制、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。
2. 本校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，並提升校內資通安全專業人員之資通安全管理能力。本校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。
  - (1) 資安專職人員總計應持有 1 張以上資通安全專業證照。
  - (2) 資通安全專職人員每年至少接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練。
4. 本校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，並視需要實施人員輪調，建立人力備援制度。
5. 本校校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，應考量本校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。
2. 各單位於規劃資通系統建置時，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，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長或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與風險評估

遵循本校資訊安全管理系統(ISMS)之資訊資產管理與資訊安全風險管理程序辦理。

| 個人資料檔案安全維護計畫 |  |      |      |    |     |
|--------------|--|------|------|----|-----|
| 文件編號         |  | 機密等級 | 內部使用 | 版次 | 1.0 |

#### 捌、資通安全防護及控制措施

本校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

遵循本校資訊安全管理系統(ISMS)之資訊處理作業辦法要求辦理。

##### 二、存取控制與加密機制管理

遵循本校資訊安全管理系統(ISMS)之存取控制作業辦法要求辦理。

##### 三、作業與通訊安全管理

遵循本校資訊安全管理系統(ISMS)之網路通訊管理作業辦法

與實體與環境安全管理作業辦法之要求辦理。

##### 四、系統獲取、開發及維護

遵循本校資訊安全管理系統(ISMS)之應用系統開發及維護作業辦法與應用系統資料處理暨程式存取控制作業辦法之要求辦理。

##### 五、業務持續運作演練

遵循本校資訊安全管理系統(ISMS)之業務持續運作管理程序要求辦理。

##### 六、執行資通安全健診

本校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

遵循本校資訊安全管理系統(ISMS)之網路通訊管理作業辦法與檔案及設備之安全控制作業辦法之要求辦理。

#### 玖、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，本校訂定資通安全事件通報、應變及演練相關機制，詳本校資訊安全管理系統(ISMS)之資通安全事件管理程序。

| 個人資料檔案安全維護計畫 |  |      |      |    |     |
|--------------|--|------|------|----|-----|
| 文件編號         |  | 機密等級 | 內部使用 | 版次 | 1.0 |

#### 壹拾、資通安全情資之評估及因應

本校接獲資通安全情資，應評估該情資之內容，並視其對本校之影響、本校可接受之風險及本校之資源，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

本校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

本校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。

| 個人資料檔案安全維護計畫 |  |      |      |    |     |
|--------------|--|------|------|----|-----|
| 文件編號         |  | 機密等級 | 內部使用 | 版次 | 1.0 |

(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。

#### 壹拾壹、資通系統或服務委外辦理之管理

本校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，監督其資通安全維護情形。並遵循本校資訊安全管理系統(ISMS)之委外管理作業辦法之要求辦理。

#### 壹拾貳、資通安全教育訓練

本校資通安全教育訓練應遵循本校資訊安全管理系統(ISMS)之教育訓練管理程序要求辦理。

#### 壹拾參、本校所屬人員辦理業務涉及資通安全事項之考核機制

本校所屬人員之平時考核或聘用，依據建國科技大學教職員工獎懲實施辦法，及本校各相關規定辦理之。

#### 壹拾肆、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

##### 一、資通安全維護計畫之實施

為落實本安全維護計畫，使本校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，應與本校之資通安全政策、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。

| 個人資料檔案安全維護計畫 |  |      |      |    |     |
|--------------|--|------|------|----|-----|
| 文件編號         |  | 機密等級 | 內部使用 | 版次 | 1.0 |

## 二、資通安全維護計畫實施情形之稽核機制與改善精進

本校稽核機制之實施、稽核改善報告與改善精進作為，應遵循本校資訊安全管理系統(ISMS)之內部稽核及矯正預防管理程序要求辦理。

## 三、資通安全維護計畫之持續精進及績效管理

1. 本校之資通安全推動小組每年至少召開一次資訊安全管理審查會議，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. 應依循本校資訊安全管理系統(ISMS)之管理審查辦法要求辦理。
3. 持續改善機制之管理審查應留下相關紀錄並應予保存，以作為管理審查執行之證據。

## 壹拾伍、資通安全維護計畫實施情形之提出

本校依據本法第 16 條之規定，應向上級或監督機關(教育部)，提出資通安全維護計畫實施情形，使其得瞭解本校之年度資通安全計畫實施情形。

## 壹拾陸、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
6. 資訊安全政策
7. 資通安全風險管理程序
8. 業務持續運作管理程序
9. 資通安全事件管理程序
10. 存取控制作業辦法
11. 資安相關人事作業辦法
12. 資訊處理作業辦法
13. 資訊資產風險評鑑作業辦法
14. 實體與環境安全管理作業辦法
15. 委外管理作業辦法
16. 應用系統開發及維護作業辦法
17. 應用系統資料處理暨程式存取控制作業辦法

| 個人資料檔案安全維護計畫 |  |      |      |    |     |
|--------------|--|------|------|----|-----|
| 文件編號         |  | 機密等級 | 內部使用 | 版次 | 1.0 |

18. 網路通訊管理作業辦法

19. 檔案及設備之安全控制作業辦法

## 二、附件表單

1. 資通安全各資訊服務申請單
2. 資通安全認知宣導及教育訓練簽到表
3. 資通安全維護計畫實施情形
4. 內部稽核查核表
5. 內部稽核報告
6. 矯正預防措施紀錄單