國立嘉義特殊教育學校

資通安全維護計畫

版次：V1.4(四版)

中 華 民 國 113 年 2 月 6 日

資通安全維護計畫

文件制/修訂紀錄表

文件版本	修訂日期	修訂內容	修訂單位	修訂人	核定人 （資安長）
V1.0(初版)	108年11月27日	新擬訂文件	教務處	魏瑛慧	許碧雲
V1.1(一版)	109 年 10 月 19 日	依據臺教國署秘字第1090101289F 號文審查意見修正: 1.核心業務最大可容忍中斷時間為 24 小時。 2.非核心業務為 48 小時。	教務處	陸澤聿	許碧雲
V1.2(二版)	110 年 3 月 24 日	依據資通系統防護基準修正: 資通系統權限管理 1. 本校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)略以。 (3)使用者更換密碼時，至少不可以與前三次使用過之密碼相同。	教務處	陸澤聿	陳威銓
V1.3(三版)	112 年 8 月 21 日	依據資通安全責任等級 D 級之各機關應辦事項: 刪除內部稽核作業條文	教務處	陸澤聿	陳錫輝
V1.4(四版)	113 年 2 月 6 日	1.已向上集中或使用主管機關指定之資訊系統納入資通安全維護計畫之核心系統。 2.D 級機關維持稽核機制。	教務處	陸澤聿	陳錫輝

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、 核心業務及重要性.....1
二、 非核心業務及說明.....2
肆、 資通安全政策及目標.....3
一、 資通安全政策.....3
二、 資通安全目標.....3
三、 資通安全政策及目標之核定程序.....3
四、 資通安全政策及目標之宣導.....3
五、 資通安全政策及目標定期檢討程序.....4
伍、 資通安全推動組織.....4
一、 資通安全長.....4
二、 資通安全推動小組.....4
陸、 專職人力及經費配置.....5
一、 專職人力及資源之配置.....5
二、 經費之配置.....6
柒、資通安全防護及控制措施.....6
一、 存取控制與加密機制管理.....6
二、 作業與通訊安全管理.....7
捌、 資通安全事件通報、應變及演練相關機制.....9
玖、 資通安全情資之評估及因應.....9
一、 資通安全情資之分類評估.....9
二、 資通安全情資之因應措施.....9
壹拾、 資通安全教育訓練.....10
一、 資通安全教育訓練要求.....10
二、 資通安全教育訓練辦理方式.....10
壹拾壹、 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.....10
壹拾貳、 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.....11

一、 資通安全維護計畫之實施.....11
二、 資通安全維護計畫實施情形之稽核機制.....11
三、 資通安全維護計畫之持續精進及績效管理.....12
壹拾參、 資通安全維護計畫實施情形之提出 13
壹拾肆、 相關法規、程序及表單 13
一、 相關法規及參考文件.....13
二、 附件表單.....13

壹、依據及目的

依據資通安全管理法第 10 條及施行細則第 6 條訂定資通安全維護計畫，作為資訊安全推動之依循及應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫(以下簡稱本計畫)。為因應資通安全管理法及資通安全責任等級應辦事項要求，以符合法令規定並落實本計畫之資通作業安全。

貳、適用範圍

本計畫適用範圍涵蓋國立嘉義特殊教育學校(以下簡稱本校)全校。

參、核心業務及重要性

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	資通系統分級	管理單位
學務、教務、輔導業務	教育部特殊教育通報網(連外部系統網站)	為本機關依組織法執掌，足認為重要者。	影響校務運作	24 小時	中	上級主管機關
網域名稱解譯	網域名稱服務（向上集中）	為本校依組織法執掌，足認為重要者	影響校務運作	24 小時	中	成大向上集中團隊
學校對外資訊	全球資訊網（向上集中）	為本校依組織法執掌，足認為重要者	影響校務運作	24 小時	中	成大向上集中團隊
公務資訊傳遞	教育雲電子郵件(連外部系統網站)	為本校依組織法執掌，足認為重要者	影響校務運作	24 小時	中	上級主管機關

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(對外服務以小時，對內服務以工作小時計)。

5. IP：系統使用者連線 IP

6. 系統管理單位：實際管理單位(科室)

7. 系統管理人員：實際管理單位負責人

8. 系統維護廠商：負責維護廠商

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	電子公文無法及時送達機關，影響機關行政效率	48 小時
人事室差勤管理	影響人事業務進行	48 小時
校務基金管理	影響主計業務進行	48 小時
出納帳務管理	影響機關行政效率	48 小時
薪資作業管理	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(對外服務以小時，對內服務以工作小時計)。

5. IP：系統使用者連線 IP

6. 系統管理單位：實際管理單位(科)

7. 系統管理人員：實際管理單位負責人

8. 系統維護廠商：負責維護廠商

肆、資通安全政策及目標

一、 資通安全政策

為使本校業務順利運作，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：

(一)應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。

(二)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。

(三)應因應資通安全威脅情勢變化，鼓勵同仁積極參與資通安全教育訓練，以提高本校同仁之資通安全意識。

(四)建立資通安全防護(如：防火牆、防毒軟體)。

(五)勿開啟來路不明或無法明確辨識寄件人之電子郵件。

(六)禁止多人共用同一帳號。

(七)落實資通安全通報機制。

二、 資通安全目標

(一) 資安事件發生時，能於規定的時間，完成通報、應變及復原作業。

(二) 因應法令與技術之變動調整資通安全維護計畫內容，避免資通系統或資訊遭受未經授權侵害，以確保其機密性、完整性及可用性。

(三) 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。

三、 資通安全政策及目標之核定程序

資通安全政策由本校資訊業務承辦人簽陳資通安全長(校長)核定。

四、 資通安全政策及目標之宣導

資通安全政策及目標應透過適當的通知方式，向本校所有人員進行宣導，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檢討其適切性。

伍、資通安全推動組織

一、 資通安全長

依本法第 11 條之規定，本校由校長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

(一) 資通安全管理政策及目標之核定、核轉及督導。

(二) 資通安全責任之分配及協調。

(三) 資通安全資源分配。

(四) 資通安全防護措施之監督。

(五) 資通安全事件之檢討及監督。

(六) 資通安全相關規章、程序與制度文件核定。

(七) 資通安全維護計畫之核定。

二、 資通安全推動小組

(一)組織

為推動本校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處室主任、學部代表與相關業務人員成立資通安全推動小組，其任務包括：

1.跨業務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

本校之資通安全推動小組依資通安全長之指示負責下列事項,本校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：

1.資通安全政策及目標之研議。

2.訂定本校資通安全相關規章、程序與制度文件，並確保相關規章、程序與制度合乎法令及契約之要求。

3.傳達本校資通安全政策與目標。

4.資通安全相關規章、程序與制度之執行。

5.資料及資通系統之安全防護事項之執行

6.資通安全事件之通報及應變機制之執行。

7.其他資通安全事項之規劃與推動。

8.每年至少召開 1 次會議，確認資通安全事項執行情形。

陸、專職人力及經費配置

一、 專職人力及資源之配置

(一)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 D 級，最低應設置資通安全兼辦人員 1 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。

1.負責推動內部資通安全稽核及教育訓練等業務之推動。

2.負責資通安全防護設施建置、資通安全事件通報及應變業務之推動。

(二)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，並提升機關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，

得洽請縣政府資管科、相關學者專家或專業機關（構）提供顧問諮詢服務。

(三)本校負責重要資通設備之管理、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。

(四)本校之首長及各業務人員，應負責所屬業務資料之資通安全作業，防範不法及不當行為。

二、 經費之配置

(一)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。

(二)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[1]，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。

(三)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、資通安全防護及控制措施

本校依據自身資通安全責任等級之應辦事項,採行相關之防護及控制措施如下：

一、 存取控制與加密機制管理

(一)網路安全控管

1. 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。

2. 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。

3. 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。

4. 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。

5. 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) 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。

(3) 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。

(二) 資通系統權限管理

1. 本校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數字及符號二種以上。

(3) 使用者更換密碼時，至少不可以與前三次使用過之密碼相同。

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。

二、 作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本校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。

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。

(二)電子郵件安全管理

1.本機關人員使用教育部校園雲端電子郵件作為公務用電子郵件信箱。

2.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。

3.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。

4.使用者應確保電子郵件傳送時之傳遞正確性。

(三)確保實體與環境安全措施

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. 具有機密性或敏感性資訊的文件及可移除式媒體在不使用或不上班時，應妥善存放。

3. 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。

4. 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。

5. 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。

(四)電腦使用之安全管理

1.電腦超過 30 分鐘不使用時，應啟動螢幕保護功能。

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.如發現資安問題，應主動循機關之通報程序通報。

(五)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

捌、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。

玖、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。

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。

(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

由指定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。

壹拾、資通安全教育訓練

一、 資通安全教育訓練要求

本校依資通安全責任等級分級屬 D 級,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

(一)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,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。

(二)本校資通安全認知宣導及教育訓練之內容得包含:

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。

(三)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。

(四)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。

壹拾壹、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

本校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及本校各相關規定辦理之。

壹拾貳、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、 資通安全維護計畫之持續精進及績效管理

(一)稽核機制之實施:

1. 資通安全推動小組應定期或於系統重大變更或組織改造後執行一次內部考核作業，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. 資通安全推動小組應擬定資通安全內部考核計畫，內容應包括依據與目的、期間、重點領域、考核小組成員、保密義務、考核方式、基準與項目及受考核單位協助事項，並應將前次考核之結果納入範圍。

(二)本校之資通安全推動小組應定期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。

(三)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。

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：

(1) 資通安全政策及目標之實施情形。

(2) 資通安全人力及資源之配置之實施情形。

(3) 資通安全防護及控制措施之實施情形。

(4) 外部稽核結果。

(5) 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。

(四)持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾參、資通安全維護計畫實施情形之提出

本校依據資通安全管理法第 12 條之規定，向上級或監督機關提出資通安全維護計畫實施情形,使其得瞭解本機關之年度資通安全計畫實施情形。

壹拾肆、相關法規、程序及表單

一、 相關法規及參考文件

(一) 資通安全管理法

(二) 資通安全管理法施行細則

(三) 資通安全責任等級分級辦法

(四) 資通安全事件通報及應變辦法

(五) 公務機關所屬人員資通安全事項獎懲辦法

(六) 資訊系統風險評鑑參考指引

(七) 本機關資通安全事件通報及應變管理程序

二、 附件表單

(一)資通安全推動小組成員及分工表

(二)資通安全保密同意書

(三)資通安全需求申請表

(四)委外廠商執行人員保密切結書、保密同意書

附件表單(一) 資通安全推動小組成員及分工表

國立嘉義特殊教育學校

資通安全推動小組成員及分工表

編號：

製表日期： 112 年 9 月 1 日

單位職級	名稱	職掌事項	分機	備註 （代理人）
校長	陳錫輝	統籌資通安全推動	200	
秘書	張慧玉	資通安全事項規劃與推展	210	
教務主任	陳威銓	教師、學生資料管理	100	
學務主任	許嘉倩	學生、學務處人事資料管理	300	
總務主任	鍾惠如	資訊資產盤點管理	400	
實輔主任	潘思恩	學生輔導資料管理	600	
人事主任	曾威超	人事系統、教師權限管理	700	
主計主任	吳金霙	資訊與資安費用之審視	800	
設備組長	陸澤聿	資通安全事項規劃與推展	102	
幹事	林俊達	資通安全事件通報與處理	109	
學前國小部學部代表	黃家亮	資通安全事項規劃與推展	161	
國中部學部代表	林珠玉	資通安全事項規劃與推展	212	
高職部學部代表	魏瑛慧	資通安全事項規劃與推展	656	

附件表單(二)資通安全保密同意書-1

資通安全保密同意書（一般人員用）

本人_____自民國___年___月___日起，於_____服務，對於職務上所知悉或持有之機密資料、程式及檔案、媒體等，絕對保守機密，不任意對外洩漏，並能遵守個人資料保護法、國家機密保護法以及本府資訊安全管理要點等法令，如有違誤，願負法律上相關責任，離職後亦同。

具切結書人（簽章）：

戶籍地：

身分證字號：

中華民國　　年　　月　　日

附件表單(二)資通安全保密同意書-2

資通安全保密同意書（駐點人員用）

本人_____自民國___年___月___日起，於_____進行駐點服務，對於職務上所知悉或持有之機密資料、程式及檔案、媒體等，絕對保守機密，不任意對外洩漏，並能遵守個人資料保護法、國家機密保護法以及本府資訊安全管理要點等法令，如有違誤，願負法律上相關責任，離職後亦同。

具切結書人（簽章）：

戶籍地：

身分證字號：

中華民國　　年　　月　　日

附件表單(三)資通安全需求申請表

國立嘉義特殊教育學校
資通安全需求申請表

編號：

申請單位		申請日期	年　　月　　日
申請項目	□軟體 □硬體 □其他	項目名稱	
申請數量		需用日期	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		安裝位置	
用途說明			
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		機關首長(或資通安全管理代表)	

附件表單(四)委外廠商執行人員保密切結書、保密同意書

資通安全保密切結書（委外廠商用）

具切結人_____，於民國_____年參與「_____**案**」之規劃、設計或設備安裝，謹聲明恪遵契約之精神及規範如下：

一、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。

二、本保密切結書不因立切結書人離職而失效。

三、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。

具切結人：

姓名及簽章	身分證字號	聯絡電話	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
_____	_____	_____

說明：本切結書所蒐集之個人資料僅供本專案相關業務使用，並依個人資料保護法之相關規定，遵循本機關資通安全管理規範妥為保存。

中　華　民　國　　年　　月