亞東學校財團法人

亞東科技大學

資通安全維護計畫

Ver 1.0

機密等級：限閱

修訂日期：113年11月26日

文件版本	生效日期	制/修訂摘要說明	承辦人	審核人
V1.0	113/11/26	新擬訂資通安全維護計畫	柯正一	資訊安全委員會

目錄

壹、 依據及目的

本計畫依據下列法規訂定：

一、資通安全管理法施行細則第6條。

二、111年全國大專校院資安長會議紀錄。

三、教育部高等教育深耕計畫-主冊專章：資安強化。

貳、 適用範圍

本計畫適用範圍亞東科技大學(以下簡稱本校)所有單位。

參、 核心業務及重要性

一、 核心業務及重要性：

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
選課系統	選課系統	□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 ■為本校依組織法執掌，足認為重要者	機關信譽：影響學生權益與相關業務及運作。	24小時(工作時間)
網路報名系統	網路報名系統	□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 ■為本校依組織法執掌，足認為重要者	機關信譽：影響學生權益與相關業務及運作。	24小時(工作時間)

各欄位定義：

二、 非核心業務及說明：

本校非核心業務之資通系統、均遵守本校資訊安全規範，詳細情形請參閱「相關法規、程序及表單」。

肆、 資通安全政策及目標

一、資通安全政策

為確保本校所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規及標準之要求，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本校之業務需求，訂定「亞東學校財團法人亞東科技大學資通安全政策」以確保本校資訊安全。

二、資通安全目標

(一) 量化型目標

1. 資通系統或主機發生異常故障導致無法正常提供服務事件每年不超過3次。
2. 網路及資通系統服務維持全年度90%以上服務不中斷。
3. 每年至少進行一次資安內部稽核。
4. 每年應辦理2場以上資安教育訓練課程。

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安全委員會或資安長核定後公布實行。

四、資通安全政策及目標之宣導

每年透過電子信箱、網站公告等形式，向本校教職員宣導資通安全政策。

五、資通安全政策及目標定期檢討程序

本校每年定期召開資訊安全會員會會議，檢視資通安全維護計畫適切性。

伍、 資通安全推動組織

一、資通安全長

依「111年全國大專校院資安長會議」紀錄，明示私立大專校院得參照「國立大專校院資通安全維護作業指引」，本校訂定張浚

林副校長為本校資通安全長，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）資通安全相關規章與程序、制度文件核定。

（七）資通安全相關工作事項督導及績效管理。

（八）其他資通安全事項之核定。

二、資訊安全委員會

（一）組織

資訊安全委員會設委員若干人，以校長、副校長、主任秘書、圖資長、各學術及行政單位主管為當然委員，校長為召集人，並由校長指派資訊安全長，圖資長擔任執行秘書，得視需要另聘資安專家參與。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

本校之資訊安全委員會依下列分工進行責任分組，並依資通安全長及執行秘書之指示負責下列事項，本校資通安全組織名冊已列冊管理，並適時更新之：

1.資安推動小組：

(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.資安防護小組：

(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.資安稽核小組：

(1)辦理資通安全內部稽核。

(2)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、 專責人力及經費配置

一、專責人力及資源之配置

(一)本校依教育部高等教育深耕計畫，主冊：資安強化與「111年全國大專校院資安長會議」紀錄規定，參照屬資通安全責任等級 C 級非特定公務機關，最低應設置資通安全專責人員1人，其分工如下，

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、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，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. 資通安全管理法法遵事項業務1人，負責本校對所屬公務機關或所管特定非公務機關之法遵義務執行事宜。

(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足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

(三)資安專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。

(四)資安專責人員總計應持有1張以上資通安全專業證照。

(五)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。

(六)本校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。

(七)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

（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。

（三）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訊安全委員會提出，由資訊安全委員會視整體資通安全資源進行分配，並經資通安全長與召集人核定後，進行相關之建置。

（四）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、 資通系統及資訊之盤點

一、資通系統及資訊之盤點

（一）本校每年辦理資通系統及資訊資產盤點，依各單位管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為軟體、硬體、資料、通訊、文件、環境、人員等。

（二）資通系統及資訊資產項目如下：

1. 軟體：資通系統，如應用軟體、系統軟體、開發工具、客製化套裝軟體、APP及電腦作業系統等。

2. 硬體：包括具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備，如個人電腦、筆記型電腦、伺服器、智慧型手機、平板電腦、行動電話機、網路通訊設備（如網路交換器、無線網路分享器等）、無人機、虛擬實境設備、影像攝錄設備、印表機、投影機、可攜式設備、物聯網設備等。

3. 資料：資訊系統之相關資料與操作說明之電子紀錄等。

4. 通訊：網路設備、無線/有線網路、網路交換器、防火牆等。

5. 文件:資訊資產廠商維護合約、資通系統操作手冊等。

6. 環境:資訊資產放置實體環境或空間、電力系統及消防等支援設備。

7. 人員:資通系統開發維護管理人員、委外廠商等。

（三）本校每年度應依資訊及資通系統盤點結果，製作「資訊資產清冊盤點」，欄位應包含：資通類別、資訊資產編號、資產名稱、資產說明、數量、保管單位、使用單位、機密性、可用性、完整性、資產價值、是否為大陸廠牌。

（四）資通系統及資訊資產硬體設備應以財產標籤標示於設備明顯處，並載明財產編號、廠牌、型號等資訊。核心資通系統及相關資產，並應加註標示。

（五）各單位管理之資通系統或資訊資產如有異動，應通知各單位資安窗口更新資產清冊。

二、機關資通安全責任等級分級

本校依教育部高等教育深耕計畫，主冊：資安強化與「111年全國大專校院資安長會議」紀錄規定，參照屬資通安全責任等級C級非特定公務機關。

捌、 資通安全風險評估

一、資通安全風險評估

（一）本校應每年針對資訊資產進行風險評估。

（二）執行風險評估時應參考本校「ISMS-2-05-00_風險評鑑程序

書」與「ISMS-2-05-02_風險因子資料庫」進行風險評估之工作。

（三）本校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
選課系統	1.網站前台主機計1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）	24小時	提供學生選課服務
網路報名系統	1.網站前台主機計1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）	24小時	提供新生報名本校入學管道服務

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

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，由於本向核心資通系統已導入 ISO27001管理制度驗證，本校之防護及控制措施詳如 ISO27001資訊安全管理系統文件

一、資通系統及資訊之管理

（一）資通系統及資訊之保管

依本校「ISMS-2-04-00_資產管理程序書」規定實行。

（二）資通系統及資訊之使用

依本校「ISMS-2-04-00_資產管理程序書」規定實行。

（三）資通系統及資訊之刪除或汰除

依本校「ISMS-3-05-00_資訊資產異動作業說明書」規定實行。

二、存取控制與加密機制管理

（一）網路安全控管

依本校「ISMS-2-13-00_系統與網路安全管理程序書」規定實行。

（二）資通系統權限管理

依本校「ISMS-2-10-00_存取權限管理程序書」規定實行。

（三）特權帳號之存取管理

依本校「ISMS-2-10-00_存取權限管理程序書」規定實行。

（四）加密管理

依本校「ISMS-2-13-00_系統與網路安全管理程序書」與「ISMS-3-03-00_個人電腦暨可攜式儲存媒體作業說明」規定實行。

三、 作業與通訊安全管理

（一）防範惡意軟體之控制措施

依本校「ISMS-2-13-00_系統與網路安全管理程序書」規定實行。

（二）遠距工作之安全措施

依本校「ISMS-2-13-00_系統與網路安全管理程序書」規定實行。

（三）電子郵件安全管理

依本校「亞東學校財團法人亞東科技大學電子郵件信箱管理辦法」規定實行。

（四）確保實體與環境安全措施

依本校「ISMS-2-15-00_實體安全管理程序書」規定實行。

（五）資料備份

依本校「ISMS-3-01-00_備份與還原作業說明」規定實行。

（六）媒體防護措施

依本校「ISMS-3-03-00_個人電腦暨可攜式儲存媒體作業說明」規定實行。

（七）電腦使用之安全管理

依本校「ISMS-3-03-00_個人電腦暨可攜式儲存媒體作業說明」規定實行。

（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. 不得使用大陸廠牌行動設備用於公務行政使用。

（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) 即時通訊軟體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) 不得為大陸廠牌之即時通訊軟體。
(4) 伺服器端之主機設備及通訊紀錄不得置於大陸地區。

四、 系統獲取、開發及維護

依本校「ISMS-2-14-00_系統開發與維護管理程序書」規定實行。

五、 業務持續運作演練

本校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。

（一）執行資通安全健診

1. 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) 目錄伺服器設定及防火牆連線設定檢視。

（二）資通安全防護設備

1. 本校應建置防毒軟體、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. 資通系統設備應定期備份日誌紀錄，定期檢視執行成果，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，本校應訂定資通安全事件通報、應變及演練相關機制，詳見「ISMS-2-11-00_資安事件通報管理程序書」。

壹拾壹、 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，詳見「ISMS-2-13-00_系統與網路安全管理程序書」。

壹拾貳、 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，並監督其資通安全維護情形。

一、選任受託者應注意事項

（一） 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並禁止為大陸廠牌。

（二） 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。

（三） 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。

二、監督受託者資通安全維護情形應注意事項

（一） 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。

（二） 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用之補救措施。

（三） 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。

（四） 受託者應採取之其他資通安全相關維護措施。

（五） 本校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。

壹拾參、 資通安全教育訓練

一、 資通安全教育訓練要求

（一） 本校依教育部高等教育深耕計畫，主冊：資安強化與「111年全國大專校院資安長會議」紀錄規定，參照屬資通安全責任等級C級非特定公務機關，資安專責人員每年至少接受12小時以上之資安專業課程訓練或資安職能訓練。

（二） 資安專責以外資訊人員每2年至少接受3小時以上之資安專業課程訓練。

（三） 本校之一般人員與主管，每人每年接受3小時以上之資訊安全通識教育訓練。

二、 資通安全教育訓練辦理方式

（一） 資安推動小組應於每年年初，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. 資訊安全通識認知。
4. 資通安全作業內容。
5. 資通安全技術訓練。

（三） 員工報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

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

本校非所屬公務機關，不適用之。

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

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。

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. 資安稽核小組應定期（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. 辦理稽核前資通稽核小組應擬定資通安全稽核計畫並安排稽核成員，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、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，稽核小組應於執行稽核至少前一週，通知受稽核單位，並將稽核期程、目標評量統計表及稽核流程等相關資訊提供受稽單位。

4. 本校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. 本校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

（一）本校之資訊安全委員會應於每年至少召開一次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。

（二）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：

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。

（三）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。

壹拾陸、 資通安全維護計畫實施情形之提出

本校依教育部高等教育深耕計畫-主冊專章：資安強化與「111年全國大專校院資安長會議」紀錄規定，應於每年向本校資訊安全委員會報告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

（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） 亞東學校財團法人亞東科技大學資訊安全委員會組織章程

（六） 亞東學校財團法人亞東科技大學資訊安全事件處理辦法

（七） 亞東學校財團法人亞東科技大學校園網路使用規定

（八） 亞東科技大學資通安全維護計畫

（九） 亞東學校財團法人亞東科技大學個人資料保護安全管理要點

（十） 亞東學校財團法人亞東科技大學個人資料檔案安全維護計畫

（十一） 亞東學校財團法人亞東科技大學電子郵件信箱管理辦法

（十二） ISMS-1-01-00_資通安全政策

（十三） ISMS-2-01-00_資通安全組織程序書

（十四） ISMS-2-02-00_資通安全實施程序書

（十五） ISMS-2-03-00_文件與紀錄管理程序書

（十六） ISMS-2-04-00_資產管理程序書

（十七） ISMS-2-05-00_風險評鑑程序書

（十八） ISMS-2-06-00_內部稽核管理程序書

（十九） ISMS-2-07-00_矯正管理程序書

（二十） ISMS-2-08-00_人力資通安全管理程序書

（二十一） ISMS-2-09-00_委外管理程序書

（二十二） ISMS-2-10-00_存取權限管理程序書

（二十三） ISMS-2-11-00_資安事件通報管理程序書

（二十四） ISMS-2-12-00_營運持續管理程序書

（二十五） ISMS-2-13-00_系統與網路安全管理程序書

（二十六） ISMS-2-14-00_系統開發與維護管理程序書

（二十七） ISMS-2-15-00_實體安全管理程序書

（二十八） ISMS-2-16-00_組織全景評鑑程序書

（二十九） ISMS-2-17-00_適用性聲明書

（三十） ISMS-3-01-00_備份與還原作業說明

（三十一） ISMS-3-02-00_帳號權限管理作業說明

（三十二） ISMS-3-03-00_個人電腦暨可攜式儲存媒體作業說明

（三十三） ISMS-3-04-00_營運持續演練計畫

（三十四） ISMS-3-05-00_資訊資產異動作業說明書

二、 附件表單

（一） ISMS-2-01-01_資通安全組織名冊

（二） ISMS-2-02-01_資訊安全管理系統目標評量統計表

（三） ISMS-2-03-01_文件管制一覽表

（四）　ISMS-2-03-02_外來文件管制表

（五）　ISMS-2-03-03_文件新增、變更或廢止申請單

（六）　ISMS-2-04-01_資產清冊暨風險評鑑表

（七）　ISMS-2-04-02_組態管理基準表

（八）　ISMS-2-05-01_風險評鑑報告

（九）　ISMS-2-05-02_風險因子資料庫

（十）　ISMS-2-06-01_資通安全稽核計畫

（十一）　ISMS-2-06-02_資通安全稽核報告

（十二）　ISMS-2-07-01_資通安全管理矯正措施單

（十三）　ISMS-2-07-02_資通安全稽核發現彙總表

（十四）　ISMS-2-08-01_保密協議書

（十五）　ISMS-2-10-01_帳號權限異動申請表

（十六）　ISMS-2-11-01_資通安全事件處理情形回覆單

（十七）　ISMS-2-12-01_營運衝擊分析表

（十八）　ISMS-2-12-02_資安事件緊急聯絡人

（十九）　ISMS-2-13-03_系統與網路檢查紀錄表

（二十）　ISMS-2-13-04_雲服務專案管理表

（二十一）ISMS-2-13-05_情資管理彙整表

（二十二）ISMS-2-14-01_應用系統作業申請單

（二十三）ISMS-2-15-01_人員進出機房登記表

（二十四）ISMS-2-15-02_設備進出紀錄表

（二十五）ISMS-2-15-03_機房環境例行性檢查紀錄表

（二十六）ISMS-2-16-01_組織全景評鑑表

（二十七）ISMS-3-01-01_備份測試查核表

（二十八）ISMS-3-01-02_備份機制明細表

（二十九）ISMS-3-02-01_存取權限審查表

（三十）　ISMS-3-03-01_個人資訊設備查核表

（三十一）ISMS-3-03-02_離職人員電腦帳號保留書

（三十二）ISMS-3-04-01_營運持續演練報告

（三十三）ISMS-3-04-02_演練排程表

（三十四）ISMS-3-04-03_演練規劃及執行表

（三十五）ISMS-3-05-01_資訊資產異動申請表