元智大學資通安全維護計畫

版本編號：1.0

訂定日期：112 年 09 月 20 日

元智大學資通安全維護計畫書

目錄

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全機關。

參、 核心業務及重要性

一、 核心業務及重要性：

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	防護需求分級
網路服務	對外、區域網路服務	□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 C 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	對外、校內網路中斷	■ hr	高
	DNS	□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 C 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	無法連線到指定主機、無法解析網址	■ hr	高
	DMZ	□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 C 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	server farm 網路中斷或安全防護等級降低	■ hr	高
	無線網路服務	□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 C 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	校園無線網路服務中斷	■ hr	高
電子郵件服務	AD 服務	□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 C 級機關所涉業	無法提供帳號密碼認證，所有依存之	■ hr	中

		務 ■為本校依組織法執掌，足認為重要者	服務之伺服器皆無法運作。		
	虛擬化儲存服務	□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 C 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	無法儲存大容量資料	■ hr	中
	前端/後端郵件服務	□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 C 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	無法提供電子郵件存取，造成內外聯絡管道中斷	■ hr	中
	SPAM 阻擋機制	□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 C 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	無法提供電子郵件存取，造成內外聯絡管道中斷	■ hr	中
首頁網站服務	電力支援 網路 虛擬伺服器服務	□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 C 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	WWW 網頁前端服務無法使用	■ hr	普
	電力支援 網路 虛擬伺服器服務 AD 服務	□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 C 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	WWW 網頁後端服務無法使用	■ hr	普
備份系統服務	備份系統	□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 C 級機關所涉業務 ■為本校依組織法執掌，足	無法提供自動備份服務	■ hr	普

		認為重要者			
行政教學務系統	資料庫管理	□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C級機關所涉業務 ■為本校依組織法執掌，足認為重要者	資料庫損毀，資訊系統無法運作	■ hr	普
	資訊系統運作	□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C級機關所涉業務 ■為本校依組織法執掌，足認為重要者	Web/用戶端操作系統發生異常，影響系統處理結果	■ hr	普

二、 非核心業務及說明如下表：

非核心業務	業務失效影響	最大可容忍中斷時間
系所及研究單位網頁	可能使系所及研究單位部分業務中斷	■ hr
用戶端服務	各處室行政及教職員無法使用網路及列印資料等服務	■ hr

肆、 資通安全政策及目標

一、 資通安全政策

為強化本校資訊安全管理，防止本校之資訊環境遭受內、外部的蓄意或意外之威脅及受未經授權之存取、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，以供全校同仁共同遵循：

(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) 確保經授權之使用者當需要時能使用資訊及資通系統。
(四) 符合法令與法規要求。
(五) 評估各種人為或天然災害之影響，訂定核心資通系統之復原計畫，以確保核心業務可持續運作。
(六) 應強固核心資通系統之韌性，確保本校業務持續營運。
(七) 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本校同仁之資通安全意識，本校同仁亦應確實參與訓練。
(八) 落實人員辦理業務涉及資通安全事項之相關懲處。
(九) 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
(十) 禁止多人共用單一資通系統帳號。

二、 資通安全目標

(一) 量化型目標

1.確保機房維運服務達全年上班時間 97%以上之可用性。

2.確保全年度未發生 4 級資通安全事件。

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 10%及 6%。

4.依員工之職務及責任符合資通安全管理法教育訓練時數要求，且執行率須達 100%。

(二) 質化型目標

1.加強內部控制，防止未經授權之不當存取，以確保資訊資產受適當的保護

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.確保所有資訊安全意外事故或可疑之安全弱點，都應依循適當之通報機制向上反映，並予以適當調查及處理。

(三) 資通安全政策及目標之核定程序

本校依「元智大學資通安全暨個人資料保護推動委員會組織辦法」,每學年審議全校資訊發展策略與方案、資通安全政策與目標，通過後再送行政會議審議並由校長核定。

(四) 資通安全政策及目標之宣導。

資通安全政策及目標得以書面、電子郵件（E-MAIL)、公告於網站、或其他等方式公告周知向所有人員、利害關係人（例如 IT 服務供應商）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每年定期審查，如遇組織、業務、法令或環境等因素之更迭，予以適當修訂之。

伍、 資通安全推動組織

依本校「元智大學資通安全暨個人資料保護推動委員會組織辦法」成立資通安全暨個人資料保護推動委員會及工作小組，負責相關業務推動。

陸、 專職（責）人力及經費配置

一、 專職（責）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 C 級，最低應設置資通安全專職人員 1 人，負責統籌資安業務，其負責工作如下：

1.資通安全管理面業務：負責推動資通系統防護需求等級、資通安全系統導入及驗證、內容資通安全稽核、機構資安置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.資通安全防護業務：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：負責本校資通安全管理法法遵義務執行事宜。

(二) 本校之承辦單位（圖書資訊服務處）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，並提升本校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) 資安專職（責）人員專業職能之培養（如證書、證照、培訓記錄等)，應依據資通

安全責任等級分級辦法之規定，持有各 1 張資通安全專業證照及資通安全職能評量證書。

(四) 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。

(五) 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。

(六) 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。

(七) 依資通安全管理法要求，應配置資安專職人員 1 名，本校目前配置資安人力，屬兼任資安業務，為符合法規要求，未來將積極爭取專職人力配置名額，更希望上級主管機關能給予預算支援，以符合法令規定之人力配置要求。

二、 經費之配置

(一) 本校預算委員會於規劃配置相關經費及資源時，應考量本校之資訊發展策略與方案；及資通安全政策與目標，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，應配合本校預算規劃期程向預算委員會提出，視整體資通安全資源進行分配，並經核定後，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、 資訊及資通系統之盤點

一、 資訊及資通系統盤點

(一) 每年至少辦理 1 次資訊及資通系統資產盤點，詳「資訊資產管理程序書」，依資訊及資通系統盤點結果，製作「資訊資產清單」。

(二) 依「資通安全責任等級分級辦法」C 級公務機關應辦事項規定，及附表九「資通系統防護需求分級原則」要求，每年至少辦理 1 次評估自行或委外開發之資通系統防護需求分級。

(三) 資訊及資通系統重要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。

(四) 每年至少進行 1 次「資訊資產清單」、「資通系統清冊」覆核，以更新及確保資訊資產清單的正確性及完整性。

二、 機關資通安全責任等級分級

本校因維運自行或委外開發之資通系統，應屬資通安全等級分類 C 級機關。

捌、 資通安全風險評估

為建立資訊安全管理制度風險評鑑與管理規範，提供本校資訊流程之權責單位、保管單位，以及使用單位，共同遵行之風險評鑑標準，有效執行風險控管，預防資訊安全事件之威脅，訂定風險評鑑與管理程序。

請參考本校「風險評鑑與管理程序書」。

玖、 資通安全防護及控制措施

依據前章資通安全風險評估結果，以及資通安全責任等之應辦事項與核心資通系統之防護基準，採行相關之防護及控制措施。由於本校核心資通系統已通過（導入）ISO27001驗證，相關防護及控制措施詳如 ISMS 文件。其他應辦事項說明如下：

一、 業務持續運作演練

應針對核心資通系統制定業務持續運作計畫，並定期辦理 1 次續運作演練。

二、 執行安全性檢測

定期辦理資通安全技術性掃描（主機弱點掃描、網頁弱點掃描、滲透測試）等。

三、 執行資通安全健診

依「資通安全等級責任分類分級辦法」之規定，應每 2 年進行資安健診，並依健診結果，規劃改善措施。

四、 資通安全防護設備

(一) 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。

(二) 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，本校訂定資通安全事件通報、應變及演練相關機制，詳本校「資通安全事件管理程序書」。

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。情資分類評估及因應如下：

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。

由資通安全暨個人資料保護推動委員會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

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。

由資通安全專職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

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。

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

資通安全情資之內容如包含本校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。

資通安全暨個人資料保護推動委員會應就涉及核心業務、核心資通系統之情資評估其是否對於本校之運作產生影響，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

確保本校資訊委外作業之安全，訂定委外管理程序。請參考本校「委外管理程序書」。

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。

(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行之補救措施。

(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

為辦理全體同仁之安全管理及教育訓練，減少人員因資訊安全認知不足所引發之資訊安全事件，依據資通安全責任等級分級辦法應辦事項各類人員之教育訓練要求：

人員類別	課程類別及時數
資通安全專職人員	每人每年至少接受 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。
資通安全專職人員以外之資訊人員	每人每 2 年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練。
一般使用者及主管	每人每年須接受 3 小時以上之資通安全通識教育訓練。

二、 資通安全教育訓練辦理方式

(一) 本校應每年考量管理、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，提升本校資通安全水準，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，應使其充分瞭解本校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，對本校外部的使用者，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人事公告相關規定辦理。

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：由資通安全暨個人資料保護稽核小組於本校執行內部稽核時實施。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。

(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。

(三) 資通安全維護計畫之持續精進及績效管理

1. 資訊安全委員會應每年至少 1 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：過往管理審查議案之處理狀態、與資通安全管理系統有關之內部及外部議題的變更、資通安全績效之回饋、風險評鑑結果及風險處理計畫執行進度、重大資通安全事件之處理及改善情形、利害關係人之回饋、持續改善之機會、資安維護計畫內容修正適切性及資安維護計畫實施情況。
3. 持續改善機制之管理審查應做成會議紀錄，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

本校依據資通安全管理法第 12 條之規定，應於每年外部稽核或指定時間向上級機關，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) 資通安全情資分享辦法
(六) 公務機關所屬人員資通安全事項獎懲辦法
(七) 元智大學資通安全暨個人資料保護推動委員會組織辦法

二、 相關表單

(一) 文件清冊
(二) 資訊資產清單
(三) 矯正預防措施表
(四) 承包廠商保密同意書
(五) 承包廠商員工保密同意書
(六) 資訊安全內部稽核計畫
(七) 資訊安全內部稽核表
(八) 資訊安全內部稽核報告