資通安全維護計畫

機密等級：公開使用

版　次：1.5

最新版本發行日期：112 年 12 月 7 日

本文件由國立臺北大學「資通安全委員會」簽准頒行，使用者對本文件之各項內容存有疑義者，可逕洽政策規劃暨推廣小組詮釋。對本文件之內容有任何建議，可填寫「文件修訂建議表」並經相關人員審核後，擲送「政策規劃暨推廣小組」做為修正依據。

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：

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
校園網路維運系統	學術網路維運系統	□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。	1 天
行政/教師/學生校務資訊系統	校園校務資訊系統	□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。 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。	2 天

電子郵件系統	教職員工生電子郵件系統	□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，足認為重要者	影響機關業務運作（相依性）：影響本校業務推動的資訊提供與服務。	2 天

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：

本校之非核心業務及說明，請詳「非核心業務及說明表」。

。

肆、資通安全政策及目標

一、資通安全政策

為遵循相關法令並保護國立臺北大學（以下簡稱本校）資訊資產(包括資料、軟體、硬體設備等)，免於因外在之威脅，或內部人員不當之管理與使用，致遭受竄改、揭露、破壞或遺失等風險，特制訂資訊安全政策以做為遵循依據。

本資訊安全政策係依據本校之任務目標與「教育體系資通安全暨個人資料管理規範」等相關法令與規定而訂定。

為達成本校之任務目標及最高管理階層對資訊安全之期許與要求，確保本校資訊資產之安全，本校之資訊安全政策訂為：確保本校相關業務資訊之機密性、完整性、可用性與適法性，以正確執行本校作業與各項業務。

其中資訊安全之本質的可用性、完整性、機密性與適法性，說明如下：

1. 可用性：

確保經授權的人員在需要時，均能在可接受的時間內取得相關資訊及設備。。

2. 完整性：
維持資訊或系統之正確與完整。
3. 機密性：
確保只有經授權的人員才能存取相關資訊。
4. 適法性：
確保資訊與處理方式過程，須遵守法律、規定、合約義務或組織內部政策、章程之規範要求。

二、資通安全目標

為達成上述目的，將相關目標分為定量與定性二類，說明如下：

(一)、定量化目標

(1) 確保相關資訊安全措施或規範符合政策與現行法令之要求，每1年至少進行一次查核。

(2) 核心資通系統每2年至少進行一次業務持續運作演練作業。

(二)、定性化目標

(1) 確保資訊資產受適當之保護，防止未經授權或因作業疏忽對資產所造成之損害。

(2) 確保所有資訊安全事件或可疑之安全弱點，皆依適當通報程序反映，並予以適當調查及處理。

(3) 符合政府資訊安全相關政策、規定以及相關法令要求。

(4) 定期實施資訊安全教育。

(三)、本校於完成目標時考量下列項目：

(1) 所需配置之人員、預算、設備技術與程序表單等資源。

(2) 活動或事項負責人員。

(3) 活動或事項預計完成時間。

(4) 管理目標是否達成之評估方式。

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通安全委員會審核並由資通安全長核定。

四、資通安全政策及目標之宣導

1. 本校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. 本校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

一、資通安全長

依本法第 11 條之規定，本校訂定主任秘書為資通安全長，負責督導本校資通安全相關事項，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，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. 資通安全保護執行小組：

(1)ISMS 文件建立、維護、管理與版本控制。

(2)每年或不定期修訂各項作業辦法與維護檢討本校的資安政策，並教導修訂的新規範。

(3)訂定年度資安宣導與訓練計畫。

(4)每年或不定期指導資訊安全活動，及辦理安全認知與教育訓練，宣導資訊安全觀念與控管機制，以確認符合資訊安全政策與程序。

(5)規劃危機處理程序。

(6)查明安全事件原因，確定資安事件影響範圍並作損失評估。

(7)辦理資訊安全事件通報與紀錄管理。

(8)執行緊急應變措施及解決辦法。

(9)蒐集陳報資訊安全政策中所訂定安全指標。

(10)負責與推動資訊資產風險評鑑與風險管理，並提出風險評鑑報告。

(11)發展資訊安全架構、標準及解決方案，包括伺服器、工作站、網路、資料庫、應用程式等。

(12)發展與維護系統、資料庫、網路與應用程式的存取控制規則。

(13)研發、協調、教導與協助安控機制與措施之執行。

(14)建立與維護業務持續運作之計畫。

(15)訂定系統安全等級及建置資訊安全措施，並執行資訊安全監控。

2. 資通安全保護稽核小組：

(1)討論及規劃年度內部稽核作業，決定稽核重點與方式，必要時舉辦稽核員講習。

(2)於每年進行稽核作業前完成稽核計畫並提交予資通安全保護執行秘書審核。

(3)每年執行資安稽核活動並提出稽核報告及相關建議事項予資通安全保護執行秘書。

(4)報告稽核結果與改善情況追蹤。

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，其分工如下，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。其相關人力規範要求，遵循本校資訊安全管理制度(ISMS)之資安相關人事作業辦法(NTPU-ISMS-C-002)辦理。
   (1) 資通安全管理面業務與資通安全管理法法遵事項業務，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，以及本校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) 資通系統安全管理業務與資通安全防護業務，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，以及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。
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) 資安專職人員總計應持有１張以上資通安全職能評量證書。
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。
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，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)之資通安全風險管理程序(NTPU-ISMS-B-002)與資訊資產風險評鑑作業辦法(NTPU-ISMS-C-005)辦理。

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(NTPU-ISMS-C-004)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(NTPU-ISMS-C-001)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(NTPU-ISMS-C-011)與實體與環境安全管理作業辦法(NTPU-ISMS-C-006)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(NTPU-ISMS-C-009)與應用系統資料處理暨程式存取控制作業辦法(NTPU-ISMS-C-010)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(NTPU-ISMS-B-005)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(NTPU-ISMS-C-011)與檔案及設備之安全控制作業辦法(NTPU-ISMS-C-012)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(NTPU-ISMS-B-004)。

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。

(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(NTPU-ISMS-C-007)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)之資安相關人事作業辦法(NTPU-ISMS-C-002)之要求辦理。

壹拾參、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、國立臺北大學職員獎懲要點，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。

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(NTPU-ISMS-B-006)之要求辦理。

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)之資通安全管理階層審查程序(NTPU-ISMS-B-003)之要求辦理。
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. 公務機關所屬人員資通安全事項獎懲辦法
7. 資訊安全政策(NTPU-ISMS-A-001)

8. 資通安全風險管理程序(NTPU-ISMS-B-002)
9. 業務持續運作管理程序(NTPU-ISMS-B-005)
10. 資通安全事件管理程序(NTPU-ISMS-B-004)
11. 存取控制作業辦法(NTPU-ISMS-C-001)
12. 資安相關人事作業辦法(NTPU-ISMS-C-002)
13. 資訊處理作業辦法(NTPU-ISMS-C-004)
14. 資訊資產風險評鑑作業辦法(NTPU-ISMS-C-005)
15. 實體與環境安全管理作業辦法(NTPU-ISMS-C-006)
16. 委外管理作業辦法(NTPU-ISMS-C-007)
17. 應用系統開發及維護作業辦法(NTPU-ISMS-C-009)
18. 應用系統資料處理暨程式存取控制作業辦法(NTPU-ISMS-C-010)
19. 網路通訊管理作業辦法(NTPU-ISMS-C-011)
20. 檔案及設備之安全控制作業辦法(NTPU-ISMS-C-012)

二、附件表單

1. 資通安全推動小組成員及分工表
2. 保密切結書(NTPU-ISMS-D-039)
3. 資通安全各資訊服務申請單
4. 資產清冊-NTPU 風險評鑑工具組(NTPU-ISMS-D-024)
5. 電腦機房進出申請表(NTPU-ISMS-D-029)
6. 資訊設備與應用系統進出管制單(NTPU-ISMS-D-030)
7. 委外考核表(NTPU-ISMS-D-032)
8. 年度資通安全教育訓練計畫
9. 資通安全認知宣導及教育訓練簽到表
10. 資通安全維護計畫實施情形
11. 稽核日程計畫表(NTPU-ISMS-D-011)
12. 內部稽核查核表(NTPU-ISMS-D-010)
13. 內部稽核報告(NTPU-ISMS-D-023)
14. 矯正預防措施紀錄單(NTPU-ISMS-D-006)
15. 矯正預防措施未結案件紀錄表(NTPU-ISMS-D-012)
16. 非核心業務及說明表