國立臺北大學內部稽核查核表(ISMS)

文件編號:**NTPU-ISMS-D-010** **版本**:**4.0** **發行日期**:**114**年**12**月**31**日
機密等級:內部使用 **紀錄編號**:

稽核項目	符合	不符合	不適用	稽核紀錄
本文 資訊安全管理系統				
本文4.1 組織是否決定與其目的有關且影響達成其資訊安全管理系統預期成果能力之外部及內部議題？				
本文4.2 組織是否瞭解與資訊安全管理系統相關關注方，並了解其要求事項(包括法律及法規要求事項，及契約義務)將透過資訊安全管理系統因應？				
本文4.3 組織是否考量內外部關注方及要求事項，並識別組織執行的活動與其他組織執行活動間的界面與相依性，決定符合組織需要之資訊安全管理系統適用範圍？				
本文4.4 組織包括所需過程及其互動是否符合PDCA循環方式維運資訊安全管理系統？				
本文5.1 是否有文件或紀錄顯示高階管理階層對資訊安全管理系統的領導力與承諾?				
本文5.2 組織制訂的資訊安全政策內容是否包含資訊安全目標、滿足資訊安全相關要求的承諾，和持續改善資訊安全管理系統的承諾？				
本文5.2 組織是否將資訊安全政策公布給全組織同仁和提供給利害相關團體？				
本文5.3 為使組織ISMS符合標準要求，組織高階管理者如何分配資訊安全相關角色的責任與授權，並適時向上(高階主管)報告ISMS績效？				
本文6.1.1 組織是否已規劃風險與機會的處理措施，並將措施整合入ISMS流程中執行，以及組織如何評估處理措施的有效性？				
本文6.1.2 組織建立之資訊安全風險評鑑流程是否包含:資訊安全風險準則、確保重複執行後其結果的可比較性、識別資訊安全風險、分析資訊安全風險、評估資訊安全風險？				
本文6.1.2 組織於識別資訊安全風險階段，是否已識別ISMS範圍中與資訊機密性、完整性與可用性喪失相關的風險，並識別風險擁有者？				
本文6.1.2 組織如何分析已識別風險可能發生的潛在結果和發生的可能性，以以如何決定風險的等級？				

稽核項目	符合	不符合	不適用	稽核紀錄
本文6.1.2 組織執行風險評鑑後, 是否產出風險處理計畫, 並對處理的順序進行排列？				
本文6.1.3 組織是否依據風險評鑑結果擬訂適用性聲明書, 並說明選擇與不選擇的理由？				
本文6.1.3 資訊安全風險處理計畫和殘餘風險是否已由風險擁有者核准？				
本文6.2 組織是否已擬訂資訊安全目標？資訊安全目標是否可量測？是否與資訊安全政策一致？ 組織是否已規劃達成資安目標所應執行的事項、所需資源和負責人員、完成時間和成果評估方式？				
本文6.3 組織決定需要對資訊安全管理系統變更時, 是否以規劃之方式執行變更？				
本文7.1 組織是否提供建立、實行、維護與持續改善資訊管安全管理系統所需的資源？				
本文7.2 組織是否對員工進行適切的資訊安全教育訓練, 並留存相關教育訓練記錄, 以確保員工具備執行資安控制措施的能力？				
本文7.3 組織員工是否了解資訊安全政策內容, 並且知道該如何執行與遵守資訊安全政策的要求？				
本文7.4 組織是否已制訂對內與對外應溝通的事項、溝通的時機點、由誰來執行溝通, 以及影響溝通的流程, 以確保溝通有效性？				
本文7.5.1 組織已制訂哪些資訊安全相關制度文件, 如:資訊安全政策、存取控制政策、機密或保密協議、資訊轉移政策與程序、供應商關係的資訊安全政策、風險評鑑準則等？				
本文7.5.2 資訊安全制度文件是否制訂文件格式規範(包含標題、日期、作者和編號)和文件審核流程？				
本文7.5.3 組織如何確保內部員工與外部團體能於需要時, 能取得正確版本之ISMS相關文件規範?				
本文7.5.3 組織如何控管ISMS文件內容之變更管制、保存與銷毀程序?				

稽核項目	符合	不符合	不適用	稽核紀錄
本文7.5.3 組織對於要求外部團體遵守的文件化程序是否管制其適切性？				
本文8.1 組織是否留存執行資訊安全要求事項所需之各項執行計畫與行動方案之紀錄文件?				
本文8.1 組織如何管理各項計劃的變更與審查未預期變更, 以降低對組織的不良影響？				
本文8.2 組織如遇動大變更時是否執行風險評鑑作業, 並留存風險評鑑結果？				
本文8.2 組織是否追蹤風險處理計畫的執行情形？				
本文9.1 組織如何量測資訊安全績效與ISMS控制措施有效性, 其評估方法為何?				
本文9.1 組織何時進行資訊安全績效與ISMS控制措施有效性量與分析?				
本文9.1 組織是否指派適當人員執行覽視、量測、分析與評估各項資安績效與控制措施有效性評估, 並留存量測紀錄備查?				
本文9.2 組織擬訂之內部稽核計畫是否包含稽核準則、稽核範圍、稽核執行方法?				
本文9.2 組織如何選擇稽核員, 是否有其資格限制, 以確保稽核過程的客觀性與公平性?				
本文9.2 組織是否保存稽核結果的相關證據文件, 並將稽核結果向相關管理單位報告?				
本文9.3 組織高階管理階層是否定期召開管理審查會議, 用以討論前次管理措施狀態、ISMS內外部議題的變更、訊安全續效回饋、利害相關團體回饋、風險評鑑結果和風險處理計劃狀態, 以及持續改善的機會, 並留存管理審查會議記錄供審查?				
本文10.1 對於不符合事項組織是否評估其原因和影響, 並擬訂控制與矯正措施？				
本文10.1 組織是否進一步評估相似的不符合事項是否存在, 並予以改善？				

稽核項目	符合	不符合	不適用	稽核紀錄
本文10.1 組織是否履行矯正措施, 並留存相對應之文件化證據, 以供審查其有效性?				
本文10.2 組織、業務程序、資訊和資訊設施有變更時, 是否同步評估與調整ISMS, 確保ISMS適切性？				
5 組織控制措施				
A.5.1 資訊安全政策 資訊安全政策及主題特定政策是否予以定義、由管理階層核可、發布、傳達予相關人員及相關關注方, 且其係知悉, 並依規劃期間及發生重大變更時審查?				
A.5.2 資訊安全之角色及責任 組織是否依需要, 定義並配置資訊安全之角色及責任？				
A.5.3 職務區隔 衝突之職務及責任範圍是否予以區隔？				
A.5.4 管理階層責任 管理階層是否要求所有人員, 依組織所建立資訊安全政策、主題特定政策及程序, 實施資訊安全?				
A.5.5 與權責機關之聯繫 組織是否建立並維持與相關權責機關之聯繫？				
A.5.6 與特殊關注群組之聯繫 組織是否建立並維持與各特殊關注群組或其他各專家安全論壇及專業協會之聯繫？				
A.5.7 威脅情資控 是否蒐集並分析與資訊安全威脅相關之資訊, 以產生威脅情資？				
A.5.8 專案管理之資訊安全 是否將資訊安全整合入專案管理中？				
A.5.9 資訊及其他相關聯資產之清冊 是否製作並維護資訊及其他相關聯資產(包括擁有者)之清冊？				
A.5.10 可接受使用資訊及其他相關聯資產 是否識別、書面記錄及實作對處置資訊及其他相關聯資產之可接受使用的規則及程序？				
A.5.11 資產之歸還 人員及其他關注方於其聘用、契約或協議變更或終止時, 是否歸還其持有之所有組織資產？				
A.5.12 資訊之分類分級 資訊是否依組織之資訊安全需要, 依機密性、完整性、可用性及相關關注方要求事項分類分級？				
A.5.13 資訊之標示 組織是否依所採用之資訊分類分級方案, 發展及實作一套適切的資訊標示程序？				

稽核項目	符合	不符合	不適用	稽核紀錄
A.5.14 資訊傳送 是否備妥資訊傳送規則、程序或協議, 用於組織內及組織與其他各方間之所有型式的傳送設施？				
A.5.15 存取控制 是否依營運及資訊安全要求事項, 建立並實作對資訊及其他相關聯資產之實體及邏輯存取控制的規則？				
A.5.16 身分管理 是否管理身分之整個生命週期？				
A.5.17 鑑別資訊 鑑別資訊之配置及管理是否由管理過程控制, 包括告知人員關於鑑別資訊的適切處理？				
A.5.18 存取權限 是否依組織存取控制的主題特定政策及規則, 提供、審查、修改及刪除對資訊及其他相關聯資產之存取權限？				
A.5.19 供應者關係中之資訊安全 是否定義並實作過程及程序, 管理與供應者產品或服務之使用相關聯的資訊安全風險？				
A.5.20 於供應者協議中闡明資訊安全 是否依供應者關係之型式, 建立相關的資訊安全要求事項, 並與各供應者議定？				
A.5.21 管理ICT供應鏈中之資訊安全 是否定義並實作過程及程序, 管理與ICT產品及服務供應鏈相關聯之資訊安全風險？				
A.5.22 供應者服務之監視、審查及變更管理 組織是否定期監視、審查、評估及管理供應者資訊安全實務作法及服務交付之變更？				
A.5.23 使用雲端服務之資訊安全 組織是否依資訊安全要求事項, 建立獲取、使用、管理及退出雲端服務的過程？				
A.5.24 資訊安全事故管理規劃及準備 組織是否藉由定義、建立並溝通或傳達資訊安全事故管理過程、角色及責任, 規劃並準備管理資訊安全事故？				
A.5.25 資訊之評鑑及決策 組織是否評鑑資訊安全事件, 並判定是否將其歸類為資訊安全事故？				
A.5.26 對資訊安全事故之回應 是否依書面記錄程序, 回應資訊安全事故？				
A.5.27 由資訊安全事故中學習 是否使用由資訊安全事故中所獲得之知識, 強化及改善資訊安全控制措施？				
A.5.28 證據之蒐集 組織是否建立並實作程序, 用以識別、蒐集、獲取及保存與資訊安全事件相關之證據？				

稽核項目	符合	不符合	不適用	稽核紀錄
A.5.29 中斷期間之資訊安全 組織是否規劃如何於中斷期間維持資訊安全於適切等級？				
A.5.30 營運持續之ICT備妥性 是否依營運持續目標及ICT持續之要求事項, 規劃、實作、維護及測試ICT備妥性？				
A.5.31 法律、法令、法規及契約要求事項 是否識別、書面記錄及保持更新資訊安全相關法律、法令、法規及契約之要求事項, 以及組織為符合此等要求事項的作法？				
A.5.32 智慧財產權 組織是否實作適切程序, 以保護智慧財產權？				
A.5.33 紀錄之保護 是否保護紀錄, 免於遺失、毀損、偽造、未經授權存取及未經授權發布？				
A.5.34 隱私及PII保護 組織是否依適用之法律、法規及契約的要求事項, 識別並符合關於隱私保護及PII保護之要求事項？				
A.5.35 資訊安全之獨立審查 是否依規劃之期間或當發生重大變更時, 獨立審查組織對管理資訊安全的作法及其實作(包括人員、過程及技術)？				
A.5.36 資訊安全政策、規則及標準之遵循性 是否定期審查組織資訊安全政策、主題特定政策、規則及標準之遵循性？				
A.5.37 書面記錄之運作程序 是否書面記錄資訊處理設施之運作程序, 並使所有需要的人員均可取得？				
6 人員控制措施				
A.6.1 篩選 是否對所有成為員工之候選者, 於其加入組織前, 進行背景查證調查, 且持續進行, 同時將適用的法律、法規及倫理納入考量, 並宜相稱於營運要求事項, 其將存取之資訊的分類分級及所察覺之風險？				
A.6.2 聘用條款及條件 聘用契約協議是否敘明人員及組織對資訊安全之責任？				
A.6.3 資訊安全認知及教育訓練 組織及相關關注方之人員, 是否均接受與其工作職能相關的組織資訊安全政策、主題特定政策及程序之適切資訊安全認知及教育訓練, 並定期更新？				
A.6.4 獎懲過程 是否明確訂定並傳達獎懲過程, 以對違反資訊安全政策之人員及其他相關關注方採取行動？				

稽核項目	符合	不符合	不適用	稽核紀錄
A.6.5 聘用終止或變更後之責任 是否對相關人員及其他關注方定義、施行並傳達於聘用終止或變更後, 仍保持有效之資訊安全責任及義務？				
A.6.6 機密性或保密協議 反映組織對資訊保護之需要的機密性或保密協議, 是否由人員及其他相關關注方, 識別、書面記錄、定期審查及簽署？				
A.6.7 遠端工作 是否實作安全措施, 當人員於遠端工作時, 保護於組織場所外存取、處理或儲存之資訊？				
A.6.8 資訊安全事件通報 組織是否提供機制, 供人員透過適切之管道, 及時通報所觀察到或可疑的資訊安全事件？				
7 實體控制措施				
A.7.1 實體安全周界 是否定義及使用安全周界, 以保護收容資訊及其他相關聯資產之區域？				
A.7.2 實體進入 保全區域是否藉由適切之進入控制措施及進出點加以保護？				
A.7.3 保全辦公室、房間及設施 是否設計辦公室、房間及設施之實體安全並實作之？				
A.7.4 實體安全監視 是否持續監視場所, 防止未經授權之實體進出？				
A.7.5 防範實體及環境威脅 是否設計並實作防範實體及環境威脅(諸如天然災害及其他對基礎設施之蓄意或非蓄意的實體威脅)之措施？				
A.7.6 於安全區域內工作 是否設計並實作於安全區域內工作之安全措施？				
A.7.7 桌面淨空及螢幕淨空 是否定義對紙本及可移除式儲存媒體之桌面淨空規則, 以及對資訊處理設施的螢幕淨空規則, 並適切實施之？				
A.7.8 設備安置及保護 設備是否安全安置並受保護？				
A.7.9 場所外資產之安全 是否保護場域外資產?				
A.7.10 儲存媒體 儲存媒體是否依組織之分類分級方案及處置要求事項, 於其獲取、使用、運送及汰除的整個生命週期內進行管理？				
A.7.11 支援之公用服務事業 是否保護資訊處理設施免於電源失效, 以及因支援之公用服務事業失效, 所導致的其他中斷？				

稽核項目	符合	不符合	不適用	稽核紀錄
A.7.12 佈纜安全 是否保護傳送電源、資料或支援資訊服務之纜線，以防範竊聽、干擾或破壞？				
A.7.13 設備維護 是否正確維護設備，以確保資訊之可用性、完整性及機密性？				
A.7.14 設備汰除或重新使用之保全 是否查證包含儲存媒體之設備項目，以確保於汰除或重新使用前，所有敏感性資料及具使用授權的軟體已移除或安全覆寫？				
8 技術控制措施				
A.8.1 使用者端點裝置 是否保護儲存於使用者端點裝置、由使用者端點裝置處理或經由使用者端點裝置可存取之資訊?				
A.8.2 特殊存取權限 是否限制並管理特殊存取權限之配置及使用?				
A.8.3 資訊存取限制 是否依已建立之關於存取控制的主題特定政策，限制對資訊及其他相關聯資產之存取?				
A.8.4 對原始碼之存取 是否適切管理對原始碼、開發工具及軟體函式庫之讀寫存取?				
A.8.5 安全鑑別 安全鑑別技術及程序是否依資訊存取限制及關於存取控制之主題特定政策實作?				
A.8.6 容量管理 資源之使用是否受監視及調整，以符合目前容量要求及預期容量要求?				
A.8.7 防範惡意軟體 是否實作防範惡意軟體之措施，並由適切的使用者認知支援之?				
A.8.8 技術脆弱性管理 是否取得關於使用中之資訊系統的技術脆弱性資訊，並評估組織對此等脆弱性之暴露，且採取適切措施?				
A.8.9 組態管理 是否建立、書面記錄、實作、監視並審查硬體、軟體、服務及網路之組態(包括安全組態)?				
A.8.10 資訊刪除 當於資訊系統、裝置或所有其他儲存媒體中之資訊不再屬必要時，是否刪除之?				
A.8.11 資料遮蔽 是否依組織存取控制及其他相關之主題特定政策、營運要求事項及適用法令，使用資料遮蔽？				
A.8.12 資料洩露預防 是否將資料洩露預防措施，套用至處理、儲存或傳輸敏感性資訊之系統、網路及所有其他裝置？				

稽核項目	符合	不符合	不適用	稽核紀錄
A.8.13 資訊備份 是否依議定之關於備份的主題特定政策, 維護資訊、軟體及系統之備份複本, 並定期測試之？				
A.8.14 資訊處理設施之多備 資訊處理設施之實作是否具充分多備(redundancy), 以符合可用性之要求事項？				
A.8.15 存錄 是否記錄活動、異常、錯誤及其他相關事件之日誌, 產生、儲存、保護及分析之?				
A.8.16 監視活動 是否監視網路、系統及應用之異常行為, 並採取適切措施, 以評估潛在資訊安全事故?				
A.8.17 鐘訊同步 組織所使用資訊處理系統之鐘訊, 是否與經認可的時間源同步？				
A.8.18 具特殊權限公用程式之使用 是否限制並嚴密控制可能篡越系統及應用程式之控制措施的公用程式之使用?				
A.8.19 運作中系統之軟體安裝 是否實作各項程序及措施, 以安全管理對運作中系統安裝軟體？				
A.8.20 網路安全 網路與網路裝置是否受保全、管理及控制, 以保護系統及應用程式中之資訊？				
A.8.21 網路服務之安全 是否識別、實作及監視網路服務之安全機制、服務等級及服務要求事項?				
A.8.22 網路區隔 是否區隔組織網路中各群組之資訊服務、使用者及資訊系統?				
A.8.23 網頁過濾 是否管理對外部網站之存取, 以降低暴露於惡意內容？				
A.8.24 密碼技術之使用 是否定義並實作有效使用密碼技術之規則(包括密碼金鑰管理)？				
A.8.25 安全開發生命週期 是否建立並施行安全開發軟體及系統之規則？				
A.8.26 應用系統安全要求事項 開發或獲取應用系統時, 是否識別、規定並核可資訊安全要求事項？				
A.8.27 安全系統架構及工程原則 是否建立、書面記錄及維護工程化安全系統之原則, 並套用於所有資訊系統開發活動？				
A.8.28 安全程式設計 軟體開發是否施行安全程式設計原則？				

國立臺北大學內部稽核查核表(ISMS)

稽核項目	符合	不符合	不適用	稽核紀錄
A.8.29 開發及驗收中之安全測試 是否於開發生命週期中定義並實作安全測試過程?				
A.8.30 委外開發 組織是否指引、監視及審查與委外系統開發相關之活動？				
A.8.31 開發、測試與運作環境之區隔 是否區隔開發環境、測試環境與生產環境, 並保全之？				
A.8.32 變更管理 資訊處理設施及資訊系統之變更, 是否遵循變更管理程序?				
A.8.33 測試資訊 是否適切選擇、保護及管理測試資訊？				
A.8.34 稽核測試期間資訊系統之保護 涉及運作中系統之評鑑的稽核測試及其他保證活動, 是否於測試者與適切管理階層間規劃並議定？				