國立臺北大學
National Taipei University

從防禦起點到採購終點：建構校園數位韌性的資安檢核攻略

法規 X 採購 X 稽核

國立臺北大學
National Taipei University

簡報、評量與相關資訊

- 資訊安全保護專區
  https://isms.gm.ntpu.edu.tw/
- 本次教育訓練簡報與評量
  https://isms.gm.ntpu.edu.tw/
- 外部法規要求
  https://isms.gm.ntpu.edu.tw/法規規章
- 相關表單
  https://isms.gm.ntpu.edu.tw/下載專區

大綱

- 年度資訊安全工作事項說明
- 法規說明
- 資安稽核事項說明
- 資訊安全日常作業說明
- 總結
- Q&A

年度資訊安全工作事項說明(主因)

外部檢測

- 實地查核(二年內或不定期)
- 技術檢測(二年內或不定期)
- 資訊安全攻防演練(每年 7-12月)
- 電子郵件社交工程(每年4-12月)
- 資安通報演練(每年9-10月)
- 端點防護回報(每月)

內部檢測

- 內部稽核(二年內完成全機關稽核)
- 網頁弱點掃瞄(不定期或核銷時進行)
- 滲透測試(二年內或不定期)
- 資安健檢(二年內或不定期)
- 業務永續演練(二年內或不定期)

國立臺北大學
National Taipei University

法規說明

- 所屬公務機關及所管特定 非公務機關資通安全稽核計畫說明(委外)
- 115年度對國私立大專院校資安攻防演練計畫
- 『資通安全責任等級分級辦法』附表五 C級之公務機關應辦事項
- 『資通安全責任等級分級辦法』附表十資通系統防護基準所定各控制措施辦理
- 資通安全管理法施行細則第四條
- 資通安全事件通報及應變辦法
- 禁止使用及採購「大陸廠牌資通訊產品」相關規定(依據 行政院秘書長109年12月18日院臺護長字第1090201804A號函 規定，禁止使用及採購大陸廠牌資通訊產品（含軟體、硬體及服務）。
- **「大陸廠牌資通訊產品及委外經營公眾場域盤點原則**
- 本校之「資訊安全管理系統(ISMS)」管理制度
- 行政院及所屬各機關行動化服務發展作業原則

法規說明–所屬公務機關及所管特定 非公務機關資通安全稽核計畫說明

所屬公務機關及所管特定 非公務機關資通安全稽核計畫說明

第1階段：技術檢測、技術檢測分為8大檢測項目，各檢測項目之執行內容及配分說明如表

第2階段：實地查核 、實地稽核分策略面、管理面及技術面3個構面

表 3、技術檢測項目及配分

項次	檢測項目	檢測子項	配分
1	使用者電腦安全檢測	使用者電腦弱點掃描	5
		使用者電腦安全防護檢測	10
2	網路惡意活動檢測	中繼站連線阻擋檢測	5
3	核心資通系統安全檢測	核心資通系統內網滲透測試	15
		核心資通系統防護基準檢測	10
4	網路架構檢測	網路架構檢測	10
5	目錄伺服器安全檢測	目錄伺服器安全防護檢測	10
6	物聯網設備安全檢測	物聯網設備安全檢測	15
7	組態設定安全檢測	組態設定安全檢測	10
8	資料庫安全檢測	資料庫安全檢測	10
9	準備作業配合度	應備文件及相關紀錄完整性	採倒扣，至多扣減 10 分
		合計	100

表 4、實地稽核項目及配分

構面	稽核項目	配分
策略面	一、核心業務及其重要性	10
	二、資通安全政策及推動組織	10
	三、專責人力及經費配置	10
管理面	四、資訊及資通系統盤點及風險評估	10
	五、資通系統或服務委外辦理之管理措施	10
	六、資通安全維護計畫與實施情形之持續精進及績效管理機制	10
技術面	七、資通安全防護及控制措施	20
	八、資通系統發展及維護安全	10
	九、資通安全事件通報應變及情資評估因應	10
其他	準備作業配合度	採倒扣，至多扣減 5 分
	合計	100

法規說明–所屬公務機關及所管特定 非公務機關資通安全稽核計畫說明

所屬公務機關及所管特定 非公務機關資通安全稽核計畫

實地查核：資通系統或服務委外辦理之管理措施要求

5.1	採購前，是否識別資通系統分級？另依資通系統分級，於採購文件明確規範防護基準需求？
5.2	委外辦理之資通系統或服務如涉及國家機密，是否記載於招標公告、招標文件及契約？並針對受託人員辦理適任性查核（辦理前是否有取得當事人書面同意，並依規定限制人員出境）？
5.3	委外廠商執行委外作業時，是否確保其具備完善之資通安全管理措施或通過第三方驗證？開發維運環境之資通安全管理進行評估？
5.3.1	是否依行政院111年5月26日函送之「資通系統籌獲各階段資安強化措施」，將所要求之相關措施納入委外安全管理程序?

普中高分級

弱點掃瞄或源碼檢測

目　次

RFP文件資安服務需求建議書範本 - 國家資通安全研究院

法規說明–所屬公務機關及所管特定 非公務機關資通安全稽核計畫說明

所屬公務機關及所管特定 非公務機關資通安全稽核計畫

資通系統或服務委外辦理之管理措施要求

5.4	委外業務如允許複委託，則對複委託之受託者應具備資通安全維護措施要求為何？如何確認其落實辦理？
5.5	是否要求委外廠商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？其要求標準為？機關及委外廠商是否皆已指定專案管理人員，負責推動、協調及督導委外作業之資通安全管理事項？其負責督導的委外作業資通安全管理事項有哪些？
5.6	委外客製化資通系統開發者，若屬核心資通系統或委託金額達新臺幣一千萬元以上者，委託機關是否自行或另行委託第三方進行安全性檢測？
5.7	委外客製化資通系統開發者，是否要求委外廠商提供資通系統之安全性檢測證明，並請其針對非自行開發之系統或資源，標示內容與其來源及提供授權證明？

可請廠商提供證明

第三方安全性檢測建議包含弱點掃描、滲透測試與源碼掃描等

資通系統籌獲各階段資安強化措施

一、依據資通安全管理法(以下簡稱本法)第九條規定，公務機關或特定非公務機關於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，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。為協助公務機關及特定非公務機關於本法適用範圍內委外辦理相關作業，補充說明委託機關依本法施行細則第四條規定選任或監督受託者之相關行政流程及應注意事項，特訂定本措施。

二、本措施所稱資通系統籌獲，指委託機關辦理本法第九條所定委外辦理資通系統之建置、維運或資通服務提供，其執行方式[1]包含但不限於：

(一)採購[2]：包含工程之定作、財物之買受、定製、承租及勞務之委任或僱傭等，不論是否依據政府採購法辦理，只要經由工程、財物或勞務性質採購取得或其執行時使用資通系統者皆屬之。

(二)委任：依行政程序法第十五條第一項規定委任所屬下級機關執行業務，取得或其執行時使用資通系統者皆屬之。

(三)委託：依行政程序法第十五條第二項或第十六條規定，委託不相隸屬之行政機關執行業務，或委託民間團體或個人辦理業務，取得或其執行時使用資通系統者皆屬之。

法規說明–所屬公務機關及所管特定 非公務機關資通安全稽核計畫說明

所屬公務機關及所管特定 非公務機關資通安全稽核計畫

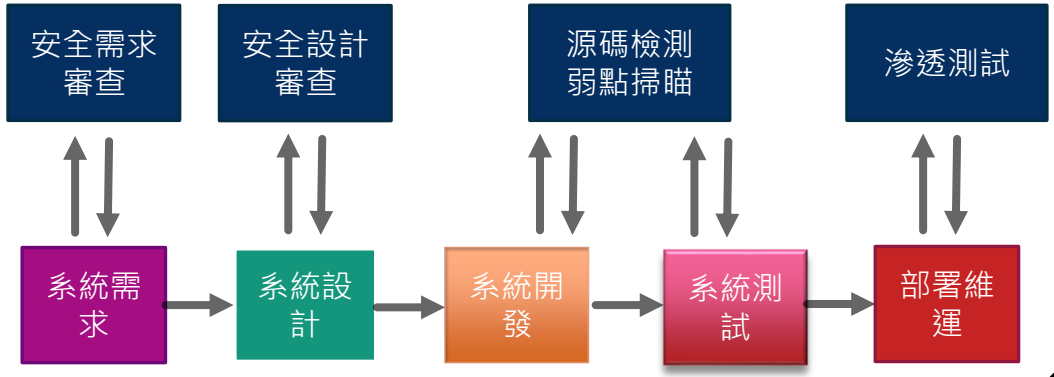
資通系統或服務委外辦理之管理措施要求

5.8	是否訂定委外廠商對於機關委外業務之資安事件通報及相關處理規範？委外廠商執行委外業務，違反資通安全相關法令或知悉資通安全事件時，是否立即通知機關並採行補救措施？
5.9	委外關係終止或解除時，是否確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料？
5.10	是否對委外廠商執行受託業務之資安作為進行檢視？其時機及做法為何？針對查核發現，是否建立後續追蹤及管理機制？

實地稽核、書面稽核

需求分析：收集並明確功能和安全需求。
設計：根據需求進行系統和架構設計，考慮安全機制。
實作：編寫程式碼，遵循安全編碼標準。
測試：執行功能和安全測試，確保系統符合要求。
部署：將系統部署到生產環境，確保配置安全。
維護：持續監控和更新系統，修補新出現的安全漏洞。

SSDLC架構示意圖



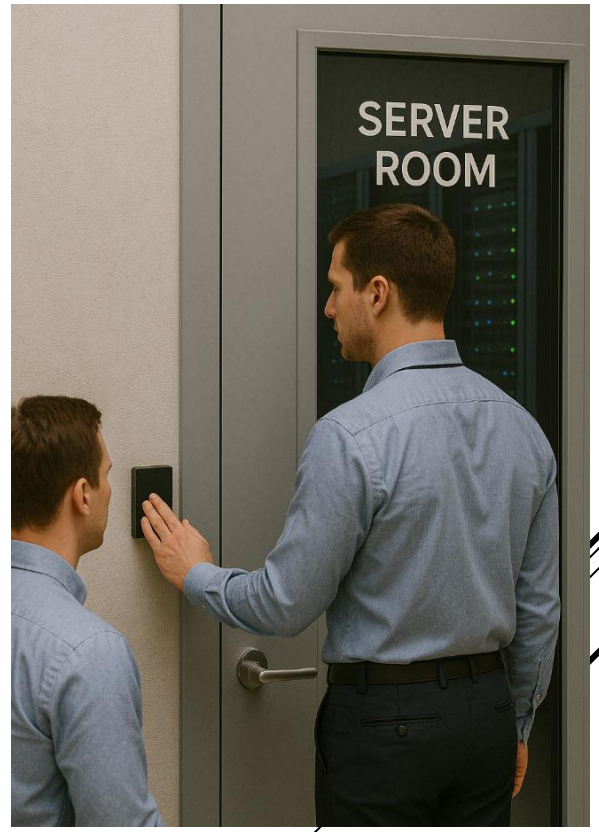
國立臺北大學 National Taipei University

法規說明–所屬公務機關及所管特定 非公務機關資通安全稽核計畫說明

所屬公務機關及所管特定 非公務機關資通安全稽核計畫

資通系統或服務委外辦理之管理措施要求

5.11	委外廠商專案成員進出機關範圍是否被限制？對於委外廠商駐點人員使用之資訊設備（如個人、筆記型、平板電腦、行動電話及智慧卡等）是否建立相關安全管控措施？是否定期檢視並分析資訊作業委外之人員安全、媒體保護管控、使用者識別及鑑別、組態管控等相關紀錄？
5.12	是否訂定委外廠商系統存取程序及授權規定（如限制其可接觸之系統、檔案及資料範圍等）？委外廠商專案人員調整及異動，是否依系統存取授權規定，調整其權限？



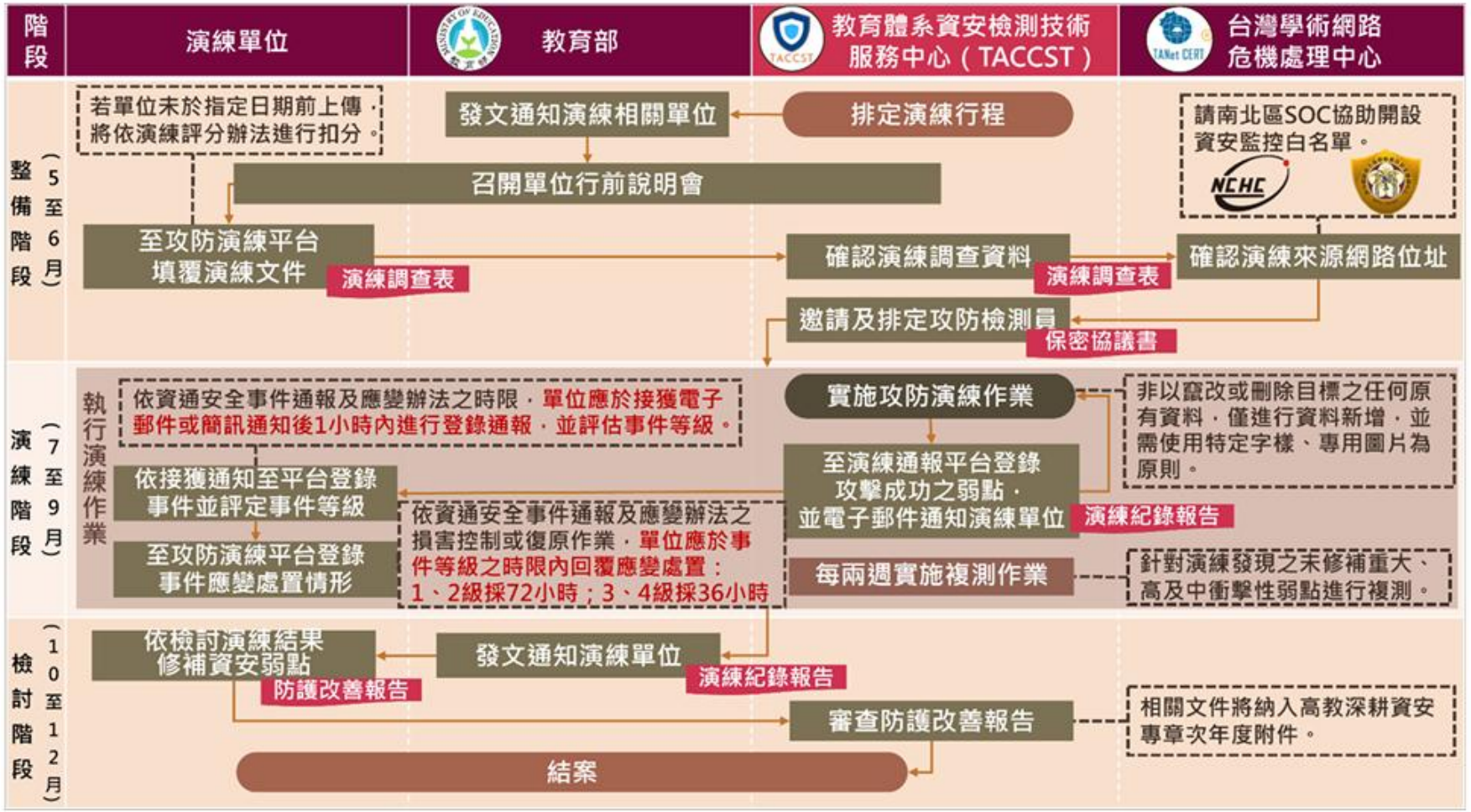
法規說明–所屬公務機關及所管特定 非公務機關資通安全稽核計畫說明

資通系統或服務委外辦理之管理措施要求

5.13	針對涉及資通訊軟體、硬體或服務相關之採購案、具委外營運公眾場域之委外案，契約範圍內是否使用大陸廠牌資通訊產品? 針對委外營運公眾場域之委外案，是否於數位發展部資通安全署管考系統填報並經機關資安長確認? 委外廠商或所涉及之人員是否為大陸廠商有陸籍身分？是否於契約內明訂禁止委外廠商使用大陸廠牌之資通訊產品，包含軟體、硬體及服務等？ 【114年資安法修正，新增公務機關自行或委外營運場所提供公眾視聽或使用之傳播設備及網際網路接取服務，於維護資通安全之必要時，不得下載、安裝或使用危害國家資通安全產品】

法規說明–對國私立大專院校 資安攻防演練計畫

由教育部發起，並委由教育體系資安檢測技術服務中心辦理(以下簡稱檢測中心)，以統籌編成資安攻防演練團隊(以下簡稱演練團隊)，負責規劃與執行資安攻防演練各項事宜。 (115年6月17日完成系統資訊通報) (115年5月-12月進行攻防演練)



目標為帶學校域名或使用學校IP之系統、網站與主機

資料來源教育部

資安稽核事項說明-資安攻防演

教育部 114 年度對國私立大專院校 資安攻防演練計畫

演練總期程

114 年 5 月至 114 年 12 月

TACCST

教育體系資安檢測技術服務中心

Taiwan Academic Network Center for Cyber Security Technology

漏洞清單

您可以在這裡查您所屬單位的漏洞資訊。

Show 200 entries Search:

序號	標題	衝擊性等級	須通報期限	須應變期限	狀態
CD-20240903-0000590	國立臺北大學資	4.高衝擊性	2024-09-03 10:41:55	2024-09-06 09:41:55	已複測
CD-20240731-0000329	國立臺北大學校	4.高衝擊性	2024-07-31 15:46:16	2024-08-03 14:46:16	已複測
CD-20240731-0000320	國立臺北大學資	5.重大衝擊性	2024-07-31 10:36:29	2024-08-03 09:36:29	已複測
CD-20240730-0000314	國立臺北大學資	4.高衝擊性	2024-07-30 17:20:42	2024-08-02 16:20:42	已複測
CD-20240730-0000310	國立臺北大學推	4.高衝擊性	2024-07-30 17:38:02	2024-08-02 16:38:02	已複測
CD-20240730-0000308	國立臺北大學GP	4.高衝擊性	2024-07-30 17:20:57	2024-08-02 16:20:57	已複測
CD-20240730-0000306	國立臺北大學歷	2.低衝擊性	2024-07-30 16:13:59	2024-08-02 15:13:59	已回報
CD-20240730-0000267	國立臺北大學回	1.資訊類	2024-07-30 11:04:07	2024-08-02 10:04:07	已回報

Showing 1 to 8 of 8 entries Previous 1 Next

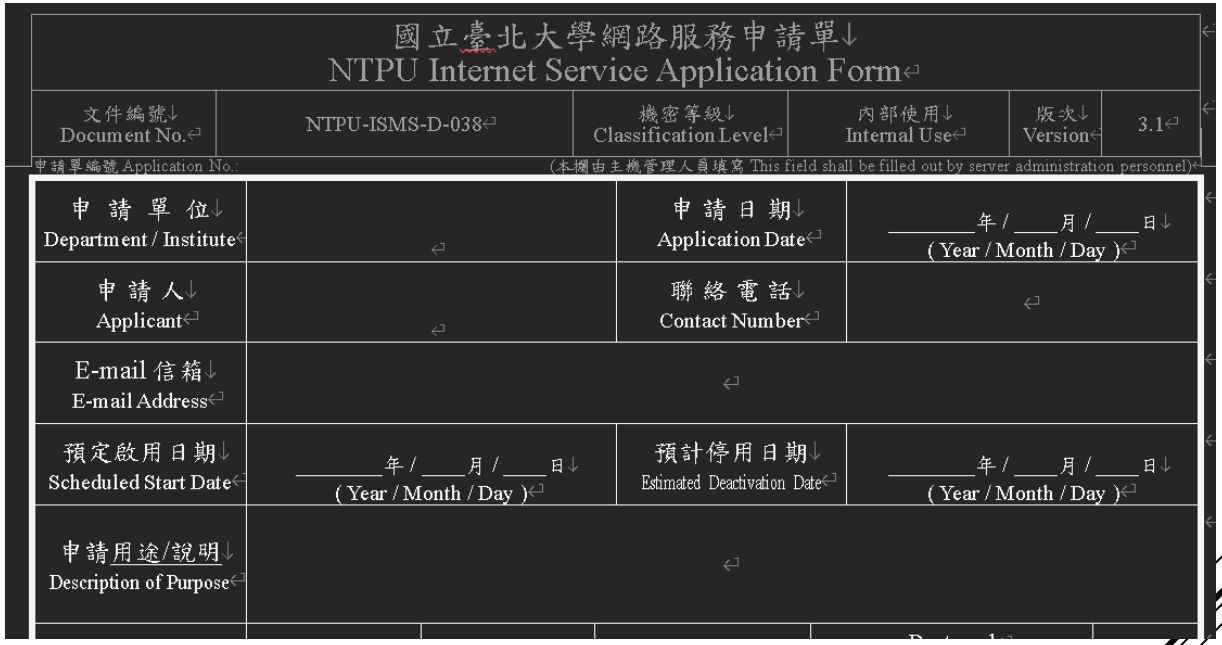
依演練計畫要求，自接獲通知起 8 小時內需修復，如超過三天未修補將封鎖網站

國立臺北大學 National Taipei University

資安稽核事項說明-委外廠商VPN帳號使用說明

廠商VPN申請流程

文件	• NTPU-ISMS-D-038 網路服務申請單 NTPU-PIIS-D-004 委外廠商保密切結書
會辦單位	• 資訊中心(網路組)
審核	•資訊中心主任審核



國立臺北大學網路服務申請單
NTPU Internet Service Application Form

文件編號 Document No.	NTPU-ISMS-D-038	機密等級 Classification Level	內部使用 Internal Use	版次 Version	3.1

申請單編號 Application No.: (本欄由主機管理人員填寫 This field shall be filled out by server administration personnel)

申請單位 Department / Institute		申請日期 Application Date	____年 / ____月 / ____日 (Year / Month / Day)
申請人 Applicant		聯絡電話 Contact Number	
E-mail 信箱 E-mail Address			
預定啟用日期 Scheduled Start Date	____年 / ____月 / ____日 (Year / Month / Day)	預計停用日期 Estimated Deactivation Date	____年 / ____月 / ____日 (Year / Month / Day)
申請用途/說明 Description of Purpose			

VPN服務提供校外連線校內網路服務
登入校園VPN後，即無法瀏覽校外網站

https://ntpu.twaren.net

國立臺北大學
National Taipei University

資安稽核事項說明-教育部電子郵件社交工程說明

演練對象：全校教職員 (包含學校之正副首長、各級主管、一般行政人員、教職員工等)
演練時間：自115年4月起至12月止，期間辦理2次演練
演練目標：各演練對象社交工程郵件開啟率應低於10%（含），社交工程郵件點閱率應低於6%（含）
演練期間，請勿開啟並立即刪除任何不明寄件人、主旨聳動或欲誘使點擊之可疑郵件。請勿點選可疑郵件之任何連結及附加檔案，並請關閉郵件預覽功能，轉寄郵件與設定為垃圾郵件視同開啟行為，因此，也請勿將可疑郵件轉寄至私人信箱或他人信箱。
提醒各位同仁**4月**開始留意社交工程演練釣魚信件，**郵件主旨分為八卦、休閒、保健、財經、新奇、時事、模擬實際社交工程樣本等類型，郵件內容包含連結網址或附檔**。請各位同仁切勿點選不明之電子郵件。
請確實完成設定將"郵件預覽"功能關閉"（若沒關閉將直接觸發開啟率）

歷史社交工程演練信件範例主旨	附件檔名
內部講座活動通知	數位轉型下的職場挑戰與機會簡報.doc
超兇畫面晃爆！鏡子出賣「林襄傲人車頭燈」	中職啦啦隊.doc
黃金大反彈！專家：「這時」將上看5000美元	把握良機.doc
便宜機票要來了！長榮航總經理：「這航線」降價會很有感	出國旅遊.doc
偵測到0utlook連續登入失敗　請重設密碼	密碼重設驗證碼.doc
2026年行事曆搶先看！假日多5天「9連假請假攻略必看」	9連假請假攻略.doc

資安稽核事項說明-教育部電子郵件社交工程說明

【教育部測試信】北北基桃「1200元月票」通路一次看 External 收件匣 ×

月票購買處 <newsweb@newsweb.forum>
寄給 我

「教育部社交工程演練測試/確認信，請協助開啟郵件及點閱附件，謝謝!」

【教育部測試信】冷氣團40年來最早！今冬備戰3寒流　反聖嬰年讓西半部雨量偏少

郵件預覽如有開啟，就會導致發生開啟率

交通部長王國材說，「初步公共運輸的月票的部分是，3年200億北北基桃.中彰投.南高屏，各地方不是一個月1200喔，要看地方的特性。」

交通部長王國材，出席台灣燈會記者會時透露，月票補助不侷限北台灣，為力拚觀光，將向中央爭取285億特別預算，200億推動月票、25億發展觀光公車、60億吸引光觀客來台。

交通部長王國材說，「國外的組團社跟國內的接地社的補助，自由行的部分就是談到送高鐵票，如果你是機加酒的話可能會送住宿，轉機客送半日遊，有的也送台灣觀巴的一日遊，悠遊卡一卡通的儲值500塊大概這樣。」

北北基桃「1200元月票」通路一次看

敬祝 平安 順心

1 個附件 • 已通過 Gmail 掃描檢查 ⓘ　新增到雲端硬碟

W
1200元月票通路.doc

點擊附件，就會導致發生點閱率

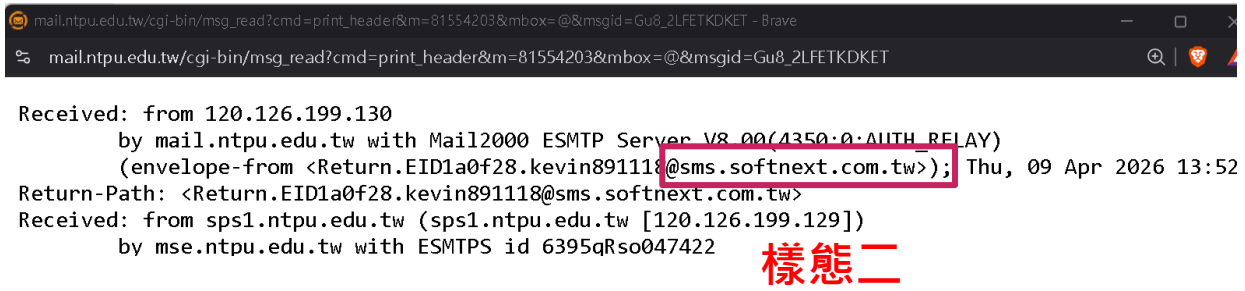
國立臺北大學
National Taipei University

資安稽核事項說明-近期社交釣魚信件說明

樣態一：寄件者網域與宣稱單位不符
樣態二：異常的發信主機與關聯網域活動
樣態三：利用短網址技術進行防護規避
樣態四：錯字網域（Typosquatting）與偽造政府層級

樣態四

例如 ntpu@ntpuedu.com.tw 模仿臺北大學網址



樣態二

樣態一

樣態三

國立臺北大學
National Taipei University

法規說明-附表五C級之公務機關應辦事項

全國法規資料庫
Laws & Regulations Database of The Republic of China (Taiwan)

整合查詢 | 請輸入關鍵字 | 查詢 | 輔助說明

熱門詞彙：刑法、職業安全衛生、憲法、勞基法、採購法

最新訊息 | 中央法規 | 司法解釋 | 條約協定 | 兩岸協議 | 綜合查詢 | 跨機關檢索

現在位置：首頁 > 中央法規 > 所有條文

下載 | 友善列印

所有條文

法規名稱：資通安全責任等級分級辦法 EN

修正日期：民國 115 年 01 月 07 日

法規類別：行政 > 數位發展部 > 資通安全目

附檔：
- 附表一 資通安全責任等級A級之公務機關應辦事項.PDF
- 附表二 資通安全責任等級A級之特定非公務機關應辦事項.PDF
- 附表三 資通安全責任等級B級之公務機關應辦事項.PDF
- 附表四 資通安全責任等級B級之特定非公務機關應辦事項.PDF
- 附表五 資通安全責任等級C級之公務機關應辦事項.PDF
- 附表六 資通安全責任等級C級之特定非公務機關應辦事項.PDF
- 附表七 資通安全責任等級D級之各機關應辦事項.PDF
- 附表八 資通安全責任等級E級之各機關應辦事項.PDF
- 附表九 資通系統防護需求分級原則.PDF
- 附表十 資通系統防護基準.PDF

所有條文 | 條號查詢 | 條文檢索 | 沿革

※歷史法規係提供九十年四月以後法規修正之歷次完整舊條文。
※如已配合行政院組織改造，公告變更管轄或停止辦理業務之法規條文，請詳見沿革

法規說明-附表五C級之公務機關應辦事項

第十一條附表五修正規定

附表五 資通安全責任等級C級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級及其防護基準之妥適性。
	資訊安全管理系統之導入		全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專職人員		配置一人以上。
	內部資通安全稽核		每二年辦理一次。
	營運持續計畫演練		全部核心資通系統每二年辦理一次。

- NTPU-ISMS-D-056 安全等級評估表
- NTPU-ISMS-D-057 資通系統盤點表

- NTPU-ISMS-D-052 資訊資產清單
- NTPU-ISMS-D-D53 威脅及弱點評估表

法規說明-附表五C級之公務機關應辦事項

技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄服務系統設定及防火牆連線設定檢視	
	資通安全弱點管理		一、知悉資通安全弱點時，應適時修補或採行緩解措施。 二、依主管機關指定方式導入弱點管理作業，並持續維運。
	資通安全防護	防毒軟體	完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	

- NTPU-PIIS-D-002　帳號清查紀錄表
- NTPU-ISMS-D-054　個人電腦安全檢查表

認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年接受十二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	每人每二年接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		資通安全專職人員分別持有證照及證書各一張以上，並持續維持證照及證書之有效性。

2.校園Vans(端點防護)軟體

一、依據資通安全責任等級分級辦法附表五，資通安全責任等級 C 級之公務機關應辦事項規定辦理。

二、為落實政府法規之要求，資訊中心已建置政府機關資安弱點通報平台，處理本校資安弱點通報作業，請各單位協助配合

Vans(端點防護軟體) 下載連結

法規說明-附表十資通系統防護基準

全國法規資料庫
Laws & Regulations Database of The Republic of China (Taiwan)

整合查詢 | 請輸入關鍵字 | 查詢 | 輔助說明

熱門詞彙：刑法、職業安全衛生、憲法、勞基法、採購法

最新訊息 | 中央法規 | 司法解釋 | 條約協定 | 兩岸協議 | 綜合查詢 | 跨機關檢索

現在位置：首頁 > 中央法規 > 所有條文

下載 | 友善列印

所有條文

法規名稱：資通安全責任等級分級辦法 EN

修正日期：民國 115 年 01 月 07 日

法規類別：行政 > 數位發展部 > 資通安全目

附檔：
- 附表一 資通安全責任等級A級之公務機關應辦事項.PDF
- 附表二 資通安全責任等級A級之特定非公務機關應辦事項.PDF
- 附表三 資通安全責任等級B級之公務機關應辦事項.PDF
- 附表四 資通安全責任等級B級之特定非公務機關應辦事項.PDF
- 附表五 資通安全責任等級C級之公務機關應辦事項.PDF
- 附表六 資通安全責任等級C級之特定非公務機關應辦事項.PDF
- 附表七 資通安全責任等級D級之各機關應辦事項.PDF
- 附表八 資通安全責任等級E級之各機關應辦事項.PDF
- 附表九 資通系統防護需求分級原則.PDF
- 附表十 資通系統防護基準.PDF

所有條文 | 條號查詢 | 條文檢索 | 沿革

※歷史法規係提供九十年四月以後法規修正之歷次完整舊條文。
※如已配合行政院組織改造，公告變更管轄或停止辦理業務之法規條文，請詳見沿革

法規說明-附表十資通系統防護基準

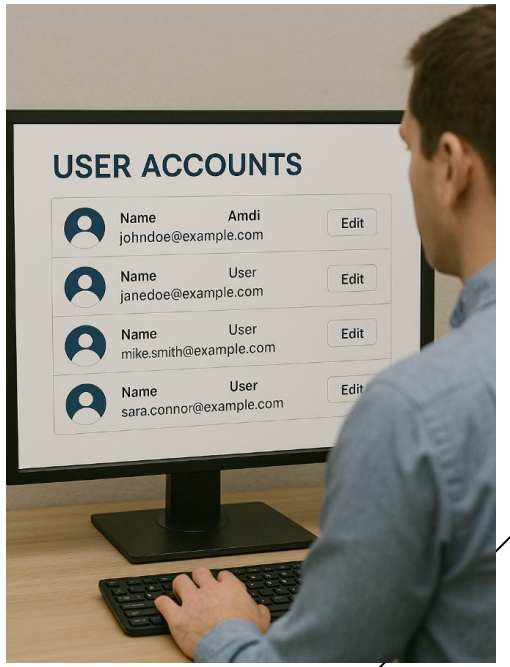
- 存取控制
  - 帳號管理
  - 最小權限
  - 遠端存取
- 事件日誌與可歸責性
  - 記錄事件
  - 日誌紀錄內容
  - 日誌儲存容量
  - 日誌處理失效之回應
  - 時戳及校時
  - 日誌資訊之保護
- 營運持續計畫
  - 系統備份
  - 系統備援
- 識別與鑑別
  - 內部使用者之識別與鑑別
  - 身分驗證管理
  - 鑑別資訊回饋
  - 加密模組鑑別
  - 非內部使用者之識別與鑑別
- 系統與服務獲得
  - 系統發展生命週期需求階段
  - 系統發展生命週期設計階段
  - 系統發展生命週期開發階段
  - 系統發展生命週期測試階段
  - 系統發展生命週期部署與維運階段
  - 系統發展生命週期委外階段
  - 獲得程序
  - 系統文件
- 系統與通訊保護
  - 傳輸之機密性與完整性
  - 資料儲存之安全
- 系統與資訊完整性
  - 漏洞修復
  - 資通系統監控
  - 軟體及資訊完整性

法規說明-附表十資通系統防護基準

第十一條附表十修正規定

附表十　資通系統防護基準

系統防護需求分級 / 控制措施		高	中	普
構面	控制措施			
存取控制	帳號管理	一、應依機關規定之情況及條件，使用資通系統。 二、監控資通系統帳號，如發現帳號違常使用時，回報管理者。 三、等級「中」之所有控制措施。	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。 二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 三、等級「普」之所有控制措施。	一、建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。 二、已逾期之臨時或緊急帳號應刪除或禁用。 三、資通系統閒置帳號應禁用。 四、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		
	遠端存取	一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。 二、使用者之權限檢查作業應於伺服器端完成。 三、應監控遠端存取機關內部網段或資通系統後臺之連線。 四、應採用加密機制。 五、遠端存取之來源應為機關已預先定義及管理之存取控制點。		



法規說明-附表十資通系統防護基準

系統防護需求分級 / 控制措施		高	中	普
構面	控制措施			
事件日誌與可歸責性	記錄事件	一、應定期審查機關所保留資通系統產生之日誌。 二、等級「普」之所有控制措施。	一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。 三、應記錄資通系統管理者帳號所執行之各項功能。	

	日誌紀錄內容	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。		
	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。		
	日誌處理失效之回應	一、機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。	資通系統於日誌處理失效時，應採取適當之行動。	
	時戳及校時	一、資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間（UTC）或格林威治標準時間（GMT）。 二、系統內部時鐘應定期與基準時間源進行同步。		
	日誌資訊之保護	一、定期備份日誌至原系統外之其他實體系統。 二、等級「中」之所有控制措施。	一、應運用雜湊或其他適當方式之完整性確保機制。 二、等級「普」之所有控制措施。	對日誌之存取管理，僅限於有權限之使用者。

法規說明-附表十資通系統防護基準

控制措施 \ 系統防護需求分級		高	中	普
構面	控制措施			
營運持續計畫	資料備份	一、應將備份還原，作為營運持續計畫演練之一部分。 二、應建立資料異地備份機制。 三、等級「中」之所有控制措施。	一、應定期測試備份資料，以驗證備份媒體之可靠性及資訊之完整性。 二、等級「普」之所有控制措施。	一、訂定資料可容忍損失之時間要求。 二、執行資料備份。
	系統備援	一、應將備援啟動作為營運持續計畫演練之一部分。 二、等級「中」之所有控制措施。	一、應定期測試原服務中斷時，於最大可容忍中斷時間內，由備援設備或其他方式取代並提供服務。 二、等級「普」之所有控制措施。	訂定資通系統從中斷後至重新恢復服務之最大可容忍中斷時間要求。

法規說明-附表十資通系統防護基準

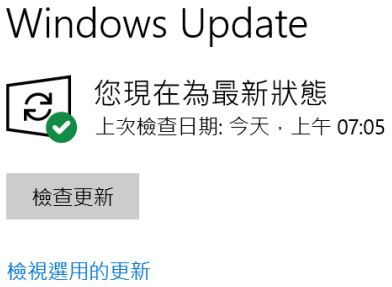
構面	控制措施	高	中	普
識別與鑑別	使用者之識別與鑑別	一、對資通系統之存取採取多因子鑑別技術。 二、等級「中」及「普」之所有控制措施。	資通系統應識別及鑑別使用者，並禁止使用者使用共用帳號。	
	身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。		一、使用預設密碼初次登入系統時，應於登入後立即變更。
		三、等級「普」之所有控制措施。		二、身分驗證相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 四、使用密碼進行驗證時，應強制最低密碼複雜度；依機關密碼效期規定變更密碼。 五、密碼變更時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對外部使用者，機關得自行規範辦理。
	鑑別資訊保護	一、資通系統如以密碼進行鑑別時，該密碼應經雜湊或其他適當方式處理後儲存。 二、等級「普」之所有控制措施。		資通系統應遮蔽鑑別過程中之資訊。

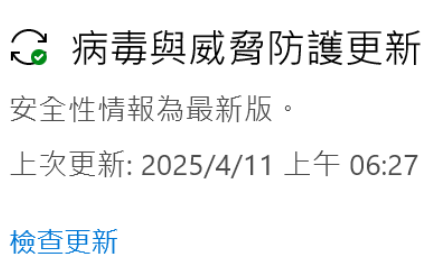
法規說明-附表十資通系統防護基準

構面	控制措施	系統防護需求分級 高	中	普
系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性）進行確認。		
	系統發展生命週期設計階段	一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	無要求。	
	系統發展生命週期開發階段	一、執行「源碼掃描」安全檢測。 二、系統應具備發生嚴重錯誤時之通知機制。	一、應針對安全需求實作必要控制措施。 二、應注意避免軟體常見漏洞及實作必要控制措施。	
		三、等級「中」及「普」之所有控制措施。	三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	
	系統發展生命週期測試階段	一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。	執行「弱點掃描」安全檢測。	
	系統發展生命週期部署與維運階段	一、於系統發展生命週期之維運階段，應執行版本控制與變更管理。 二、等級「普」之所有控制措施。	一、於部署環境中應針對相關資通安全威脅，進行更新與修補。 二、識別並關閉不必要服務及埠口。 三、資通系統不使用預設密碼。 四、執行系統源碼備份。	
	系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。		
	獲得程序	一、開發、測試及正式作業環境應為區隔。 二、等級「普」之所有控制措施。	識別資通系統使用之第三方軟體、服務、函式庫或其他元件。	
	系統文件	應儲存與管理系統發展生命週期之相關文件。		

法規說明-附表十資通系統防護基準

系統防護需求分級 / 控制措施		高	中	普
構面	控制措施			
系統與資訊完整性	漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
	資通系統監控	一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 二、等級「中」之所有控制措施。	一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 二、等級「普」之所有控制措施。	發現資通系統有被入侵跡象時，應通報機關特定人員。
	軟體及資訊完整性	一、應定期執行軟體與資訊完整性檢查。 二、等級「中」之所有控制措施。	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二、發現違反完整性時，資通系統應實施機關指定之安全保護措施。 三、等級「普」之所有控制措施。	使用者輸入資料合法性檢查應置放於應用系統伺服器端。





法規說明-資通安全管理法施行細則第四條

第 4 條

1 各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項：

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。

四、受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

五、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安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者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。

六、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。

七、委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。

八、受託者應採取之其他資通安全相關維護措施。

九、委託機關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。

2 委託機關辦理前項第四款之適任性查核，應考量受託業務所涉及國家機密之機密等級及內容，就執行該業務之受託者所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核有無下列事項：

一、曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。

二、曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。

三、曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

四、其他與國家機密保護相關之具體項目。

3 第一項第四款情形，應記載於招標公告、招標文件及契約；於辦理適任性查核前，並應經當事人書面同意。

法規說明-大陸廠牌資通訊產品及委外經營公眾場域盤點原則

危害國家資通安全產品限制使用原則

一、依據 行政院秘書長109年12月18日院臺護長字第1090201804A號函 規定，**禁止使用及採購大陸廠牌資通訊產品（含軟體、硬體及服務）。**

二、依據 行政院112年6月20日院授數資安字第1121000202號函 及 行政院113年12月31日院授數資安字第1131000727號函 說明，重申各公務機關使用資通訊產品原則：

（一）若因業務需求且無其他替代方案，仍需使用危害國家資通安全產品時，**應具體敘明理由，並經機關資通安全長及其上級機關資通安全長逐級核可，函報資通安全管理法主管機關（數位發展部）核定**。

（二）就各機關所盤點之危害國家資通安全產品，相關因應措施摘要如下：

•行政院於110年5月5日中央及地方政府資通安全長暨行政院國家資通安全會報第37次委員會已向各機關宣達，針對未達使用年限之財物如須報廢時，於相關文件中註明報廢原因，**可專案報廢處理。**

•於汰換前則應有適當之配套措施或相應作為：

1.停用（封存）。

2.使用但不與公務網路介接，或擬訂其他適當配套管制措施。

3.將使用情形列入年度稽核時之檢視項目。

4.產品使用屆期後不得再購買危害國家資通安全產品。

國立臺北大學
National Taipei University

法規說明-大陸廠牌資通訊產品及委外經營公眾場域盤點原則

（三）**辦理採購案時，得依個案特性及實際需要於採購文件中循以下方式辦理**：

1.參考行政院公共工程委員會（下稱工程會）採購範本投標須知範本第16點，廠商所供應標的（含工程、財物及勞務）之原產地不允許大陸地區，以及資訊服務採購契約範本第8條第24款，如採購案內涉資通訊軟體、硬體或服務等相關事務，機關可要求廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。

2.倘涉雲端服務者，可另參考工程會資訊雲端服務採購契約範本第17條，廠商履約有下列情形之一者，機關得以書面通知廠商終止契約或解除契約之部分或全部，且不補償廠商因此所生之損失：16.經查廠商提供大陸廠牌、 資通訊產品（含硬體、軟體及服務）、雲端服務之所屬 一切資料存取、備份及備援之實體所在地位於大陸地區（含香港、澳門），或跨該等境內傳輸相關資料。

3.自行或委外營運，提供公眾活動或使用之場地，不得使用危害國家資通安全產品，且應將相關限制式樣納入委外契約或場地使用規定中，以避免後續履約爭議，並將契約訂定相關文字列入年度稽核時之檢視項目。

4.依工程會113年8月13日工程企字第11300155871號函，機關辦理採購涉及物聯網設備技術規格之訂定，請各機關於採購物聯網設備時依該函說明事項辦理。

5.可參考數位發展部數位產業署之能量登錄機制資訊，揀擇適當之標的、廠商或於契約中載明須提出相關能量登錄證書等。

法規說明-大陸廠牌資通訊產品及委外經營公眾場域盤點原則

大陸品牌眾多，公務機關環境常見大陸品牌包含以下(如遇無法判斷者，可以請廠商提供證明或上網搜尋該品牌資訊)

- 海康威視(Hikvision)
- 華為(Huawei)
- 普聯(TP-Link)
- 大華(Dahua)
- 歐加(OPPO)
- 吉翁(TOTOLINK)
- 福斯康姆(FOSCAM)
- 小米(MI)
- 騰達(Tenda)
- 大疆創新(DJI)
- 維沃(VIVO)
- 中興通訊(ZTE)
- 高巨創新(EMO)
- 真我(REALME)
- 海信(Hisense)

相關資料來源為維基百科

小米集團 [編輯]

條目 討論 汉 漢 臺灣正體 閱讀 編輯 檢視歷史 工具 84 種語言

維基百科，自由的百科全書

此條目的主題是在中華人民共和國創立的科技企業。關於一種糧食，請見「小米」。

小米集團（英語：Xiaomi Corporation，簡稱：**小米**，港交所：1810、港交所：81810（人民幣結算））成立於2010年4月6日，[4]2018年7月9日於香港交易所主機板掛牌上市，是一家以智慧型手機、智慧型硬體和IoT平台為核心的消費電子及智慧型製造公司[5]。

小米集團
Xiaomi Corporation

小米位於中國北京市海淀區的總部園區

簡介 [編輯]

2010年4月，小米成立於中華人民共和國北京市[6]，並於2011年8月發表小米手機進軍手機市場[7]。據全球市場調研機構Canalys的統計，在2021年第二季度，小米智慧型手機市場占有率位居全球第二，占比17%[8]。小米還是繼蘋果、三星、華為之後第四家擁有手機晶片自研能力的手機廠商[9]。

小米旗下擁有多個子品牌，面向不同產品品類、地區市場及消費人群。通過與其生態鏈企業的研發與合作，其旗下產品涵蓋了智慧型手機、可穿戴裝置、智慧型電視、空氣清淨機等多種智慧化的消費電子產品[10]。小米擁有其直接控股或間接控制的生態鏈

相關資料來源為公司基本資料

我們是誰

AnyViewer 是Aomei科技開發的一款免費、安全的遠端控制軟體。它提供對遠端電腦的快速穩定的存取，並提供高品質的圖像，讓您感覺像是在使用本機電腦一樣。 AnyViewer 支援從任何裝置以及任何地點安全地遠端存取您的企業或個人電腦，並透過強大的 256 位元橢圓曲線加密 (ECC) 算法進行端對端加密。

未來，AnyViewer將專注於為使用者提供全面有效的遠端存取和支援指南，幫助提高工作效率，創造最大價值。

Aomei科技是一家擁有十年軟體開發經驗的網路公司。該公司成立於2010年，現已成為香港發展最快的公司之一，僱用了超過170名行業精英。公司致力於全球資料保護，以「始終讓全球資料更安全」為使命。為此，Aomei提供了一系列卓越的軟體來幫助個人和企業防止資料遺失。

真我（**realme**）是一家中國智慧型手機和IoT產品製造商，總部位於廣東深圳，由李炳忠於2018年5月4日創立，初時主要面向印度市場。2018年7月，realme脫離OPPO，由6月成立的**深圳市銳爾覓移動通訊有限公司**運營[1][2]。2018年11月15日，Realme推出了新標識。

2019年4月，realme進入中國市場[3]，後進行國際擴張，目前，realme已經覆蓋中國大陸、印度、印度尼西亞、西班牙、法國、義大利、英國、俄羅斯、越南、泰國、台灣、馬來西亞、巴基斯坦、埃及等全球23個國家與地區[4]。

2019年，realme全球手機出貨量達到了2500萬台[5]。據市場分析機構Counterpoint 2019年第三季度全球智慧型手機出貨量統計資料，新興智慧型手機品牌realme在全球智慧型手機出貨量排行榜中位列第七，正式躋身主流智慧型手機品牌行列。與2018年同期相比，realme的增長率高達808%，增長速度位居全球第一，成為全球成長最快的智慧型手機品牌[6]。

深圳市銳爾覓移動通訊有限公司
RealMe重慶移動通訊有限公司

realme

realme

公司類型	子公司
成立	2018年5月4日，6年前
創辦人	李炳忠
代表人物	李炳忠（CEO） 徐起（副總裁、行銷總裁） 姚坤（副總裁、研發總裁） 王偉（副總裁、產品總裁）
總部	中國廣東省深圳市後海街道卓越後海中心8樓

National Taipei University

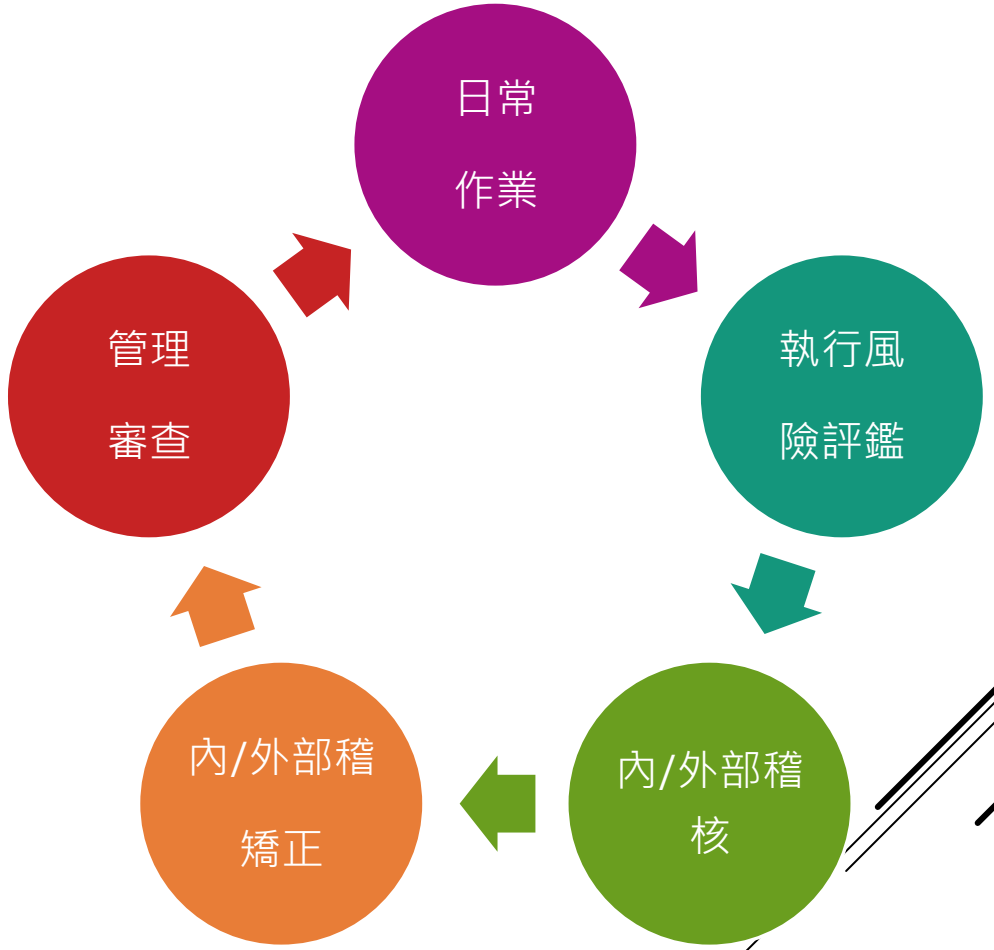
資訊安全日常作業說明

資安日常作業內容（每年）

單位文件
- NTPU-ISMS-D-052　資訊資產清單
- NTPU-ISMS-D-D53　威脅及弱點評估表
- NTPU-ISMS-D-056　安全等級評估表
- NTPU-ISMS-D-057　資通系統盤點表

個人文件
- NTPU-PIIS-D-002　帳號清查紀錄表
- NTPU-ISMS-D-054　個人電腦安全檢查表

系統文件
- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表



相關文件可在資訊中心與資訊安全保護專區中下載

國立臺北大學
National Taipei University

資訊安全日常作業說明-資訊系統上線前文件

如以資訊系統方式分類，資安日常作業內容（每年）

單位文件

系統上線前需準備的文件
- NTPU-ISMS-D-052　資訊資產清單
- NTPU-ISMS-D-D53　威脅及弱點評估表
- NTPU-ISMS-D-056　安全等級評估表
- NTPU-ISMS-D-057　資通系統盤點表

- NTPU-PIIS-D-004　委外廠商保密切結書
- 資訊系統弱點掃瞄報告(無中等以上風險)
- 資訊系統弱點掃瞄處理記錄（資訊系統適用)
- NTPU-ISMS-D-049 主機網域名稱-4-V3.1

請購時文件
- 國立臺北大學系統採購檢核表-採購前(請購時)
- 國立臺北大學委外廠商資通安全檢核表(核銷時)

相關文件可在資訊中心與資訊安全保護專區中下載

國立臺北大學
National Taipei University

資訊安全日常作業說明（單位文件）

- NTPU-ISMS-D-052　資訊資產清單
- NTPU-ISMS-D-D53　威脅及弱點評估表
- NTPU-ISMS-D-056　安全等級評估表
- NTPU-ISMS-D-057　資通系統盤點表

文件名稱：資訊資產清單　　機密等級：□公開使用 ■內部使用 □限制使用 □授權使用

文件編號：NTPU-ISMS-D-052　　版次：V1.0

紀錄編號：　　填表日期：　　年　　月　　日

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資訊資產價值
SYS-PE-001	PE	管理階層人員	主任(1)、組長(4)	資訊中心	資訊中心	資訊中心	4	1	4	4
SYS-PE-006	PE	廠商維護人員	維護工程師				3	1	3	3
SYS-PE-008	PE	臨時人員	工讀生				1	1	1	1
SYS-CM-007	CM	一般網路設備	網路及資源組L2線網路開道與無				1	1	2	2
SYS-DA-002	DA	次要系統資料	DNS資料、Log資料				3	3	3	3
SYS-DA-003	DA	個人電腦資料	辦公室個人電腦				3	2	3	3
SYS-HW-001	HW	重要系統主機	DNS(2)、LDAP(				1	1	4	4
SYS-HW-004	HW	個人電腦	辦公室電腦				1	1	1	1

- 資產類別
  - 資料（DA）
  - 軟體/應用程式（SW）
  - 硬體（HW）
  - 人員（PE）
  - 環境（EV）
  - 通訊（CM）

國立臺北大學 National Taipei University

資訊安全日常作業說明（單位文件）

- NTPU-ISMS-D-052　資訊資產清單
- NTPU-ISMS-D-D53　威脅及弱點評估表
- NTPU-ISMS-D-056　安全等級評估表
- NTPU-ISMS-D-057　資通系統盤點表

文件名稱：資訊資產清單　　機密等級：□公開使用 ■內部使用 □限制使用 □授權使用

文件編號：NTPU-ISMS-D-052　　版次：V1.0

紀錄編號：　　填表日期：　　年　　月　　日

資產編號	使用單位	機密性	完整性	可用性	資訊資產價值
SYS-PE-001	資訊中心	4	1	4	4
SYS-PE-006	系統組	3	1	3	3
SYS-PE-008	資訊中心	1	1	1	1
SYS-CM-007	系統組	1	1	2	2
SYS-DA-002	全校	3	3	3	3
SYS-DA-003	資訊中心	3	2	3	3
SYS-HW-001	資訊中心	1	1	4	4
SYS-HW-004	資訊中心	1	1	1	1

- 機密性(confidentiality):• 資料不得被未經授權之個人、實體或程序所取得或揭露的特性。
- 完整性(Integrity)：• 確保資料無論是在傳輸或儲存的生命週期中，保有其正確性與一致性。
- 可用性(Availability)：• 當使用者需透過資訊系統進行操作時，資料與服務須保持可用狀況(能用)，並能滿足使用需求(夠用)。
- 資訊資產價值比較：「機密性、完整性和可用性」的值，選擇**最大值**

資訊安全日常作業說明（單位文件）

- NTPU-ISMS-D-052　資訊資產清單
- NTPU-ISMS-D-D53　威脅及弱點評估表
- NTPU-ISMS-D-056　安全等級評估表
- NTPU-ISMS-D-057　資通系統盤點表

構面 \ 分數	4	3	2	1
機密性	此資訊資產所包含資訊為組織或法律所規範的機密資訊	此資訊資產僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用	此資訊資產僅供組織內部人員或被授權之單位及人員使用	此資訊資產無特殊之機密性要求
完整性	該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害甚至造成業務終止	該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，但不至於太嚴重	該資訊資產本身具有完整性要求，當完整性遭受破壞時，不會對組織造成傷害	該資訊資產本身完整性要求極低
可用性	該資訊資產僅容許失效8小時以下	該資訊資產僅容許失效8小時以上，1天以下	該資訊資產可容許失效1天以上，3天以下	該資訊資產可容許失效3天以上

資訊安全日常作業說明（單位文件）

- NTPU-ISMS-D-052　資訊資產清單
- NTPU-ISMS-D-D53　威脅及弱點評估表
- NTPU-ISMS-D-056　安全等級評估表
- NTPU-ISMS-D-057　資通系統盤點表

分數 / 構面	3	2	1
威脅	平均每月都可能發生一次以上	平均每季都可能發生一次以上	平均每年發生次數2次以內或沒發生過但可能發生
弱點	弱點很容易被利用	弱點被利用的難度適中	弱點很難被利用

威脅及弱點評估表

等級：☐公開使用 ■內部使用 ☐限制使用 ☐授權使用

文件編號：OOOISMS-D-053　　版　次：1.0

紀錄編號：112-002　　填表日期：112 年 07 月 18 日

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級(發生之可能性) 低(1)	中(2)	高(3)	弱點等級(受到威脅利用之容易) 低(1)	中(2)	高(3)	風險值
SYS-HW-001	HW	重要系統主機	4	硬體失效	不夠充分的維護措施		1			2		8
				硬體或儲存媒體損害	缺乏硬體耗損控管		2			1		8
				操作失誤	缺乏有效組態變更控制		2			1		8
				操作失誤	專業訓練不足		2			1		8
				電源供應中斷	不穩定的電壓		1			1		4
					缺乏保護措施		1			1		4
				取或使用	缺乏監督與稽核機制		1			1		4
					易受濕度、灰塵、溫度影響		1			1		4

- 資產-識別範圍內各項資產
- 威脅-指威脅發生的機率或可能性
- 弱點-是指資訊資產之弱點被利用的難易度

風險值的計算

風險值=（資訊資產價值x威脅等級x弱點等級）

可接受風險：**16含以下**

資訊安全日常作業說明（單位文件）

- NTPU-ISMS-D-052　資訊資產清單
- NTPU-ISMS-D-D53　威脅及弱點評估表
- NTPU-ISMS-D-056　安全等級評估表
- NTPU-ISMS-D-057　資通系統盤點表

安全等級評估表

- 「資通安全責任等級分級辦法」附表九_資通系統防護需求分級原則

構面 \ 防護需求	高	中	普	備註
機密性	產生非常嚴重或災難性之影響	產生嚴重之影響	產生有限之影響	可能造成未經授權之資訊揭露（資料外洩），對機關之營運、資產或信譽等方面
完整性	產生非常嚴重或災難性之影響	產生嚴重之影響	產生有限之影響	可能造成資訊錯誤或遭竄改(資料刪除)等情事，對機關之營運、資產或信譽等
可用性	產生非常嚴重或災難性之影響	產生嚴重之影響	產生有限之影響	可能造成對資訊、資通系統之存取或使用之中斷(服務無法使用)，對機關之營運、資產或信譽等
法律遵循性	使機關所屬人員負刑事責任	使機關或其所屬人員受行政罰、懲戒或懲處	其他資通系統設置或運作於法令有相關規範之情形	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性(適法性)

- 全球資訊網 安全等級評估表

■ 功能說明：提供本校首頁之網頁訊息與公告服務

■ 網址：https://new.ntpu.edu.tw

■ 業務屬性：□行政類 ∨業務類　　日期：115年 03 月 03 日

影響構面				資訊系統安全等級
1.機密性	2.完整性	3.可用性	4.法律遵循姓	
普	普	普	普	普
			資訊系統安全等級：	普

步驟1：設定影響構面等級

影響構面		安全等級	原因說明
1.機密性	初估	普	網站資訊均為可公開之一般性資料
	異動		
2.完整性	初估	普	本網站主要提供資訊公告及各系統入口連結
	異動		
3.可用性	初估	普	本網站提供一般性資料瀏覽
	異動		
4.法律遵循姓	初估	普	僅提供入口及一般性資料，無違反法律之可能性
	異動		

步驟2：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	業務類	提供學校簡介、政策措施介紹、對外資訊服務
	異動		

備註	

業務單位：　　業務單位主管：

資訊安全日常作業說明（單位文件）

- NTPU-ISMS-D-052　資訊資產清單
- NTPU-ISMS-D-D53　威脅及弱點評估表
- NTPU-ISMS-D-056　安全等級評估表
- NTPU-ISMS-D-057　資通系統盤點表

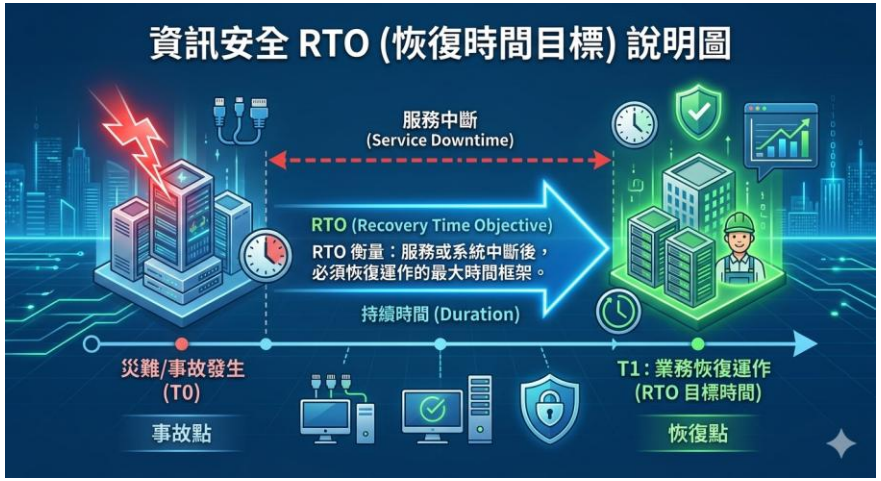
資通系統盤點表

- 依上表NTPU-ISMS-D-056　安全等級評估表中內容填寫

資通系統盤點表

日期：2025.9.4

NO.	單位	組別	保管人	資產名稱	廠商	資產類別	資訊系統安全等級（等級填寫詳見 總體評估	機密性	完整性	可用性	法律遵循性	是否為大陸廠商或工程師建置	備註說明	對外是否連通	網址	IP位址	中斷後至重新恢復服務之可容忍時間（RTO/小時）	可容忍資料損失時間（RPO/小時）
1	資訊中心	研發組		學生校務資訊系統 教師校務資訊系統 行政校務資訊系統	無	軟體	中	中	普	普	中	否	自行開發建置	是	https://cof.ntpu.edu.tw https://sea.cc.ntpu.edu.tw/teacher https://sea.cc.ntpu.edu.tw/admin_n	120.126.197.81 120.126.197.7	24 48 48	24 24 24
2	資訊中心	研發組		學校官方網頁系統(新\舊)	無	軟體	普	普	普	普	普	否	自行開發建置	是	新：https://new.ntpu.edu.tw/ 舊：	120.126.192.181 120.126.192.182	48	48
3	資訊中心	系統組		電子郵件系統	昇恆陽	軟體	中	普	普	中	普	否	委外維護	是	https://webmail.ntpu.edu.tw/cgi-bin/login?index=1	120.126.199.162	48	48
4	資訊中心	系統組		網路服務	昇恆陽	軟體	中	普	普	中	普	否	委外維護	否			24	24



- 請依現況機制填寫可容忍中斷時間與可損失資料時間

國立臺北大學
National Taipei University

資訊安全日常作業說明（個人文件）

- NTPU-PIIS-D-002　帳號清查紀錄表
- NTPU-ISMS-D-054　個人電腦安全檢查表

帳號清查紀錄表					
文件編號	NTPU-PIIS-D-002	機密等級	限制使用	版次	1.0

填表日期：　　年　　月　　日

系統名稱	系統型態	帳號	使用者	權限說明	備註
系網頁	Ap	admin	XXX	ALL	php 8.4
系網資料庫	DB	root			mysql8.0
作業系統	OS	administrator			Windows 2022 21H2
個人電腦	OS	administrator			Windows 11 25H2
個人電腦	OS	user			Windows 11 25H2

【注意事項】
系統型態：作業系統(OS)、應用系統(AP)、資料庫(DB)
權限說明：全部權限(All)、使用者權限(User)、其他(Other，請敘明權限資訊)

承辦人：　　單位主管審查：

- 填寫所管或所屬的資訊系統或電腦的作業系統及資訊系統的帳號與權限
- 備註欄位填寫軟體版本及注意是否已無法更新

- 型態類型可以參考註意事項

國立臺北大學
National Taipei University

資訊安全日常作業說明（個人文件）

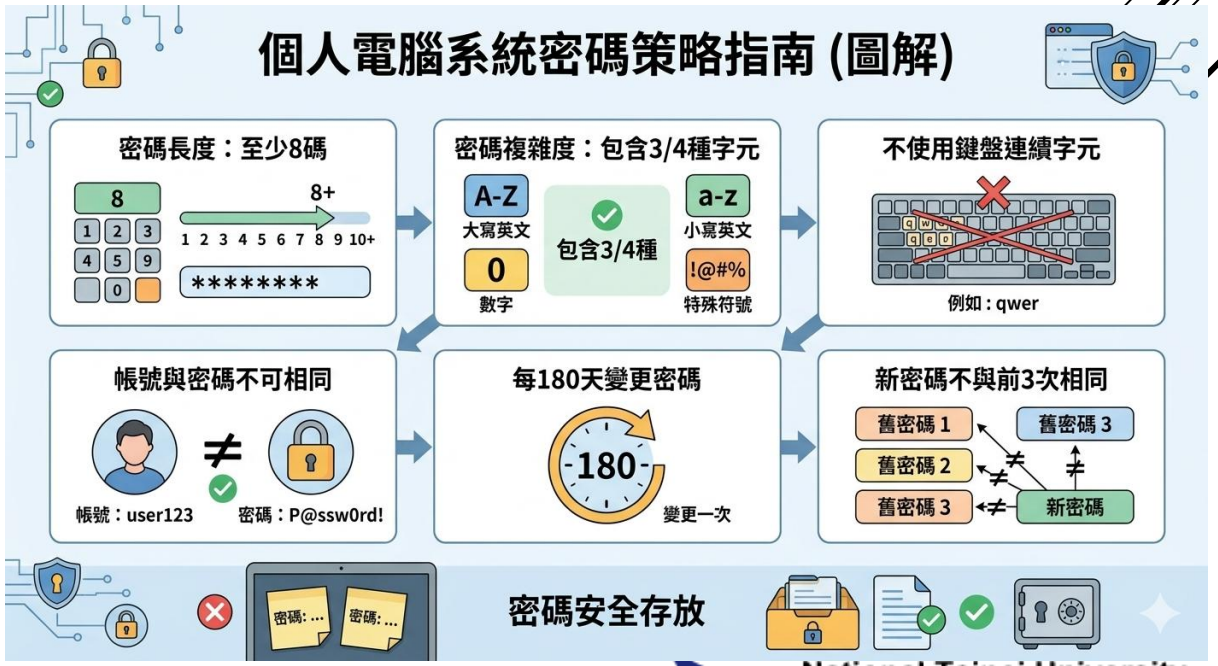
- NTPU-PIIS-D-002　帳號清查紀錄表
- NTPU-ISMS-D-054　個人電腦安全檢查表

機密等級：□公開使用☑內部使用□限制使用□授權使用 紀錄編號:

NTPU-ISMS-D-054(版本1.1)	個人電腦安全檢查表	檢查日期：			
單位		姓名		IP位址		作業系統版本	
檢查項目		檢查說明		檢查狀況	備註
1	a.個人電腦系統密碼長度至少**8碼**， b.**密碼複雜度**需包含英文大、小寫、數字、特殊符號以上4種字元之其中**3種**，不得使用鍵盤連續字元組成（如：qwer）且帳號密碼不可相同） c.通行密碼至少**每180天**變更一次， d.修改密碼不得與前**3**次（以上）密碼相同。 e.密碼未置放於顯而易見之處。	檢查設定：搜尋列執行" gpedit.msc"->出現本群組原則編輯器->電腦設定->windows 設定->安全性設定->帳戶原則->密碼原則->**檢視密碼長度、密碼複雜度、強制執行密碼歷程記錄、密碼最長使用期限**是否符合檢查項目要求。		□符合 □不符合	
2.	取消密碼永久有效設定	檢查設定：對本機圖示右鍵->選擇管理->點選本機使用者和群組->使用者->選擇使用者帳號並右鍵內容->取消密碼永久有效選項->點確定完成		□符合 □不符合	
3	電腦已啟動螢幕保護程式且設定密碼保護（閒置超過15分鐘即啟動螢幕保護程式或鎖定）。	檢查設定：桌面右鍵->個人化->鎖定畫面->螢幕保護設置->設定等候15分鐘->勾選「繼續執行後，顯示登入畫面」。		□符合 □不符合	
4	電腦作業系統已啟動系統自動更新程式（Windows Update），同仁已配合進行軟體更新及修補漏洞，且保持更新至最新狀態。	檢查設定：開始->設定(齒輪圖示)->點選更新與安全性或Windows update，確認是否為「最新狀態」->進階選項需開啟。		□符合 □不符合	
5	電腦已安裝及啟用防火牆安全防護功能。	檢查設定：控制台(類別選取大圖示)-> Windows Defender 防火牆，確認防火牆是否已啟用。(或啟用防毒軟體之防火牆)		□符合 □不符合	
6	電腦已安裝防毒軟體，且病毒碼已更新至最新版本，嚴禁任意移除或關閉防毒軟體。	1.檢查電腦右下角是否有防毒軟體圖示。 2.使用外來檔案，應先掃毒，請勿任意移除或關閉防毒軟體。		□符合 □不符合	
檢查人員		單位主管			
※檢查人員若發現不符合事項時，應於「備註」欄，詳細填寫查核之具體事證。 ※若發現不符合項目時，須將電腦進行調整至符合上述需求，再請單位主管進行複查，以確認完全符合檢查項目。					

- 檢查人員填寫完成後，務必請主管蓋章

- 可依照檢查說明執行檢查
- 如有不符合的地方請立即改正，以避晚日後教育部資訊安全稽核時被發現



資訊系統採購與核銷流程說明

新採購與維護申請（請購流程）

文件
- 請購單
- 國立臺北大學系統採購檢核表-採購前
- 合約書或系統需求文件

會辦單位
- 資訊中心(研發組、網路組)
- 其他單位(事務組、主計室等)

審核
- 校長審核

新採購與維護申請（核銷流程）

文件
- 核銷文件(定期維護報告等)
- 國立臺北大學系統採購檢核表-採購前
- 合約書或系統需求文件
- 無中等風險以上系統弱點掃瞄報告或矯正預防單(風險無法處理時)
- 國立臺北大學委外廠商資通安全檢核表

會辦單位
- 資訊中心(研發組、網路組)
- 其他單位(事務組、主計室等)

審核
- 校長審核

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

委外廠商保密切結書

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（承包廠商名稱）茲向國立臺北大學（以下簡稱貴校）保證：本公司承攬　貴校「＿＿＿＿＿＿＿＿」業務，自 貴校取得之資訊（不論技術、商業資訊或個人資訊），除已經公開流通之資訊外，應嚴格保密；且除因遵循法令或相關主管機關規定外，非經　貴校同意，不得向第三人披露。如因本公司故意或過失，違反上開情事而為洩漏、竄改、交付或使用，致損及貴校權益時，本公司願負法律責任。

此致
國立臺北大學

立同意書寶號：＿＿＿＿＿＿＿＿＿＿＿＿
代　表　人：＿＿＿＿＿＿＿＿＿＿＿＿
統 一 編 號：＿＿＿＿＿＿＿＿＿＿＿＿
地　　址：＿＿＿＿＿＿＿＿＿＿＿＿

中　華　民　國　　年　　月　　日

- 此項為廠商(公司)的保密切結

委外廠商人員保密切結書

具保密切結廠商(人員)　　於民國　年　月　日起於國立臺北大學（以下簡稱　貴校）執行「＿＿＿＿＿＿＿＿」專案業務，因而知悉　貴校機密或任何不公開之文書、圖畫、消息、物品或其他資訊，將恪遵保密規定，未經　貴校書面授權，不得以任何形式利用或洩漏、告知、交付、移轉予任何第三人，如有違誤，願負法律上之責任。本切結書自簽訂日期起，十年內有效。

此致
國立臺北大學

具切結書委外廠商(人員)：
所屬單位：
單位電話：
單位地址：

中　華　民　國　　年　　月　　日

- 如要申請廠商VPN登入帳號，需檢附此文件影本與申請書共同提供

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

演練方式
.模擬演練（腳本演練、書面演練)
.實地演練

- BCP演練簽核 ⟫ BCP演練計畫 ⟫ BCP演練記錄 ⟫ BCP演練通報與矯正

普級系統BCP演練一般以備份演練為主

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

檢測記錄

排程日期	檢測狀態	弱掃狀態	嚴重風險	高風險	中風險	低風險	信　息	威脅等級	更新日期	檢測結果	弱掃報告
2026-02-24 17:00	執行完成	completed	0	0	0	1	10	低	2026-02-24 18:02	瀏覽	報告下載
2025-03-06 00:00	執行完成	completed	0	0	0	0	8	安全	2025-03-06 02:55	瀏覽	報告下載

.ntpu.edu.tw

Scan details

Scan information	
Start time	2026-03-12T00:11:29.168554+08:00
Start url	
Host	
Scan time	64 minutes, 59 seconds
Profile	Full Scan
Server information	Apache
Responsive	True
Server OS	Unknown
Server technologies	PHP
Application build	25.11.251107123

Threat level

Acunetix Threat Level 4

One or more critical-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	287
Critical	16
High	128
Medium	124
Low	13
Informational	6

- 此系統風險很高，會資料外洩或被作為跳板的風險

- 教育部每年至少會進行一次以上的弱點掃瞄作業。
- 各項網頁系統均需完成中等以上風險修正，方可避免發生資安事件

WordPress Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') Vulnerability

Severity	Critical
Reported by module	/Scripts/WebApps/wordpress_7.script

Description

Before version 4.8.2, WordPress mishandled % characters and additional placeholder values in $wpdb->prepare, and thus did not properly address the possibility of plugins and themes enabling SQL injection attacks.

Impact

- 資料庫竄改風險

Recommendation

References

CVE-2017-14723 (https://nvd.nist.gov/vuln/detail/CVE-2017-14723)
CVE-2017-14723 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14723)

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

排程日期	檢測狀態	弱掃狀態	嚴重風險	高風險	中風險	低風險	信　息	威脅等級	更新日期	檢測結果	弱掃報告
2026-03-12 00:00	執行完成	completed	16	128	124	13	6	嚴重	2026-03-12 01:22	瀏覽	報告下載
2025-02-10 00:00	執行完成	completed	16	118	124	13	5	嚴重	2025-02-10 01:00	瀏覽	報告下載

WordPress Improper Neutralization of Special Elements used in a Command ('Command Injection') Vulnerability

Severity	Critical
Reported by module	/Scripts/WebApps/wordpress_7.script

Description

The isMail transport in PHPMailer before 5.2.20 might allow remote attackers to pass extra parameters to the mail command and consequently execute arbitrary code by leveraging improper interaction between the escapeshellarg function and internal escaping performed in the mail function in PHP. NOTE: this vulnerability exists because of an incorrect fix for CVE-2016-10033.

Impact

Recommendation

166

References

CVE-2016-10045 (https://nvd.nist.gov/vuln/detail/CVE-2016-10045)
CVE-2016-10045 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10045)

Affected items

Web Server
Details
wordpress v4.0-4.0
Request headers

- 命令注入攻擊（Command Injection）也是一種 Injection Attack 不過它注入的通常是惡意的系統命令，命令注入攻擊通常發生在接受使用者輸入並將其視為系統命令的應用程式中，例如Shell命令、作業系統命令或其他可執行的命令

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

排程日期	檢測狀態	弱掃狀態	嚴重風險	高風險	中風險	低風險	信　息	威脅等級	更新日期	檢測結果	弱掃報告
2026-03-12 00:00	執行完成	completed	16	128	124	13	6	嚴重	2026-03-12 01:22	瀏覽	報告下載
2025-02-10 00:00	執行完成	completed	16	118	124	13	5	嚴重	2025-02-10 01:00	瀏覽	報告下載

WordPress Server-Side Request Forgery (SSRF) Vulnerability

Severity	**Critical**
Reported by module	/Scripts/WebApps/wordpress_7.script

Description

WordPress before 5.2.4 has a Server Side Request Forgery (SSRF) vulnerability because Windows paths are mishandled during certain validation of relative URLs.

Impact

Recommendation

References

CVE-2019-17670 (https://nvd.nist.gov/vuln/detail/CVE-2019-17670)
CVE-2019-17670 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17670)

Affected items

Web Server
Details
wordpress v4.0-4.0
Request headers

- 由於缺乏對 url 參數的適當驗證，伺服器會盲目地執行請求。
- 最終造成內部資源回傳給 Web 伺服器，Web 伺服器再將原本不應公開的內部敏感資料回傳給攻擊者。

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

排程日期	檢測狀態	弱掃狀態	嚴重風險	高風險	中風險	低風險	信　息	威脅等級	更新日期	檢測結果	弱掃報告
2026-03-12 00:00	執行完成	completed	16	128	124	13	6	嚴重	2026-03-12 01:22	瀏覽	報告下載
2025-02-10 00:00	執行完成	completed	16	118	124	13	5	嚴重	2025-02-10 01:00	瀏覽	報告下載

Press Improper Privilege Management Vulnerability

Severity	**Critical**
Reported by module	/Scripts/WebApps/wordpress_7.script

Description

wp-includes/class-wp-xmlrpc-server.php in WordPress before 5.5.2 allows attackers to gain privileges by using XML-RPC to comment on a post.

Impact

Recommendation

References

CVE-2020-28036 (https://nvd.nist.gov/vuln/detail/CVE-2020-28036)
CVE-2020-28036 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28036)

Affected items

Web Server
Details
wordpress v4.0-4.0
Request headers

- XML-RPC 是一種基於 HTTP 傳輸和 XML 封裝的遠端程序呼叫（RPC）協議，允許軟體跨平台在遠端伺服器執行函數並取得結構化數據。它具備輕量級與跨語言特性，廣泛用於 API 接口，例如 WordPress 預設啟用 xmlrpc.php 進行遠端發文，但也容易成為暴力破解的資安風險

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

採購檢核表檢核項目

- 系統功能需求
- 合約期間
- 違約及服務績效罰則
- 資訊系統防護等級判斷
- 雲端服務
- 使用者操作
- 版本更新
- 資訊安全管理
- 教育訓練及輔導上線
- 權利及責任
- 行動化應用程式(APP)
- 物聯網設備
- 涉及國安或具敏感性或含資安
- 系統環境建置/維護
- 資料備援及移置
- 資訊安全
- 維護服務範圍
- 維護內容
- 維護方式
- 交付文件
- 資訊安全相關

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用

國立臺北大學

委外資訊系統建置/開發/維護需求標準作業流程

2

網頁/系統/服務 ☐建置或開發 ■維護 採購檢核表

作業目的:

(一)為提升行政效率優化服務品質，特訂定本作業流程協助行政單位委外資訊系統自我管理能力，並能督促廠商建置穩定安全的系統。

(二) 請依本作業流程各項目先行檢核，並且敘明於**招標需求書、規格文件或採購合約內**，註記敘明於文件頁數後，隨本校採購流程至資訊中心審核。

(三)請於本案完成並於驗收前，依本檢核表各項目依序檢核無誤後，始得辦理驗收作業。

3

申請日期	年　月　日	申請單位	校友中心
委外系統名稱		是否為核心資通系統	☐是　■否
預算金額　(a+b=c)			
資訊經費數額(a)		1.此兩項經費由總務處事務組審核 2.超過15萬元案件請務必填寫	
資安經費數額(b)	資安經費為資訊經費數額5%以上		

1

更新日期：114.10.13

國立臺北大學 National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

- 符合：請填寫需求書或合約"頁數"與"編號"
- 不符合：需填寫原因(或改善作為)
- 不適用：通常為無此需求、未購置或法規可允許

一、　契約檢核要項

	項目	檢核重點	規格內容	單位填寫	
				自我檢核是否符合	敘明招標需求書(含規格文件)頁數編號或未符合原因
1.	系統功能需求	功能規格需求說明	經與廠商訪談及報價分析，制定需求建議書，並彙整功能規格需求。	☑符合 ☐未符合 ☐不適用	合約 1&6（p.2&3）
2.	合約期間	合約或維護有效期間	自　年　月　日至　年　月　日止。	☑符合 ☐未符合 ☐不適用	合約 3-1（p.2）
3.	違約及服務績效罰則	未達所定服務水準及績效時，計算違約點數	履約期間內廠商未達機關所訂服務水準及績效，依評估項目、評斷方式要求基準訂定處罰規則。	☑符合 ☐未符合 ☐不適用	合約 11（p.5）
4.	資訊系統防護等級判斷	資通系統防護基準	依資通系統防護需求分級原則完成資通系統分級，本案資通系統安全等級為普級，須依『資通安全責任等級分級辦法』附表十資通系統防護基準所定各控制措施辦理。	☑符合 ☐未符合 ☐不適用	合約 6-4（p.3）
5.	雲端服務(無校外雲端服務免填)	須具備完善資通安全管理措施	須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	☑符合 ☐未符合 ☐不適用	合約 6-5（p.4）
6.			廠商不得為大陸地區廠商第三地區含陸資成分廠商	☑符合 ☐未符合 ☐不適用	合約 5-4（p.3）

網頁放置於校外需填寫

報價單與規格需求

罰則與扣款項目

安全等級評估表

通過資安認證

主要資料與備份都不可存放於有害地區

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

7.		弱點管理	雲端應用系統平台具備定期檢視PaaS之應用、組件或Web服務是否存在漏洞並進行更新修補	☑符合 ☐未符合 ☐不適用	合約 6-8（p.4）
8.			雲端應用系統平台提供帳號安全認證、權限管理、網路安全傳輸及遠端存取控管佐證	☑符合 ☐未符合 ☐不適用	合約 6-5（p.4）
9.		存取控制	須針對維運管道建立基於零信任(ZTA)控管基礎之防護機制，並導入同等(AAL2)或更高等級的多因子身份鑑別機制	☑符合 ☐未符合 ☐不適用	合約 6-8（p.4）
10.		事件日誌保存與可歸責性	應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求	☑符合 ☐未符合 ☐不適用	合約 6-4（p.3）
11.		供應商及產品安全要求	針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險 1.供應商安全：符合以下任一條件。 (1)廠商有公開漏洞回報應變機制 (2)廠商有第三方檢測團隊執行檢測 2.產品安全：符合以下任一條件。 (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告 (2)提供經商用弱點檢測軟體未含___等級風險之掃描報告 (3)取得第三方認可實驗室認證,如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證	☑符合 ☐未符合 ☐不適用	合約 6-4（p.3）

漏洞修正與帳號管控

需提供二種登入方式，
例如帳密再加上手機驗證

附表十資通系統防護基準
法規要求

網頁放置於校外需填寫

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

12.		資料安全	未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區	☑符合 ☐未符合 ☐不適用	合約 9-2（p.4）
13.			資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。	☑符合 ☐未符合 ☐不適用	合約 9-2（p.4）
14.			廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證	☑符合 ☐未符合 ☐不適用	合約 6-5（p.4）
15.		資安檢測	主機弱點掃描	☑符合 ☐未符合 ☐不適用	合約 6-8（p.4）
16.			網站弱點掃描	☑符合 ☐未符合 ☐不適用	合約 6-8（p.4）
17.			滲透測試掃描(由檢測人員測試雲端服務是否具備 TLS v1.2以上安全通訊協定)(核心系統適用)	☐符合 ☐未符合 ☑不適用	非核心系統
18.		資安教育訓練	廠商需參加機關資安規範教育訓練(廠商需參加政府機關或本校資安規範教育訓練)	☑符合 ☐未符合 ☐不適用	合約 5-5（p.3）

系統與備份資料均不依於大陸地區

提供弱點掃描報告

廠商參與校內教育訓練或提供相關證明

網頁放置於校外需填寫

國立臺北大學 National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

19.	使用者操作	支援穩定主流瀏覽器(網頁系統適用)	需完整支援 Edge、Chrome、Firefox、Safari 等主流瀏覽器最新穩定版本。	☑符合 ☐未符合 ☐不適用	合約1-4（p. 2）
20.		支援多(雙)語系 (多語系系統適用)	支援正體中文、英文語系。	☑符合 ☐未符合 ☐不適用	合約1-4（p. 2）
21.		響應式網頁設計 (網頁系統適用)	應符合不同主流裝置瀏覽需求。	☑符合 ☐未符合 ☐不適用	合約1-4（p. 2）
22.		符合無障礙網頁規範 (網頁系統適用)	應配合國發會網站無障礙規範最新版本。	☑符合 ☐未符合 ☐不適用	合約 6-3（p. 3）
23.	版本更新	修正系統錯誤	廠商應修正系統錯誤，進行本系統版本更新。	☑符合 ☐未符合 ☐不適用	合約 6-3（p. 3）
24.		因應法規更新	廠商應協助更新因法規或作業方式修改，進行本系統版本更新。	☑符合 ☐未符合 ☐不適用	合約 6-3（p. 3）
25.		上(更)版機制	系統重大更新前應於測試機測試驗收，再於正式機進行版本更新	☑符合 ☐未符合 ☐不適用	合約 6-3（p. 3）
26.		版本更新錯誤復原	當版本更新出錯，導致系統中斷無法運行，應復原至前一版，待錯誤修正後再進行版本更新。	☑符合 ☐未符合 ☐不適用	合約 6-3（p. 3）
27.		作業系統更新	系統應於作業系統進行版本更新後，仍可正常運行作業。	☑符合 ☐未符合 ☐不適用	合約 6-3（p. 3）
28.		雙方討論同意後執行	應於甲乙雙方討論同意後，再執行版本更新作業。	☑符合 ☐未符合 ☐不適用	合約 6-3（p. 3）

如為校內或非供大眾使用之系統可不適用，如監視器等

供大眾使用網頁依規定需逐年完成

國立臺北大學 National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

29.	資訊安全管理	配合本校之「資訊安全管理系統(ISMS)」制度	廠商需落實本校資訊帳號管理原則，且必需配合本校之「資訊安全管理系統(ISMS)」制度以及資通安全管理法等最新相關資訊安全管理及保密規定。	☑符合 ☐未符合 ☐不適用	合約 9-2（p.4）
30.		簽署保密同意書	廠商及相關人員應據實簽署「國立臺北大學保密切結書」。	☑符合 ☐未符合 ☐不適用	合約 9-3（p.4）
31.		屬本校之資產於雙方無合作關係時應予銷毀	本校提供一切機敏性資料、文件等均屬本校之資產，約定期間或雙方無法合作、或技術移轉時，廠商應依本校要求，無條件將所持有之原本交還，複製之機敏文件、資料、媒體應予銷毀。	☑符合 ☐未符合 ☐不適用	合約 9-3（p.4）
32.		違反個資法之損害賠償責任	廠商因執行本契約業務而違反個資法，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。	☑符合 ☐未符合 ☐不適用	合約 5-8（p.3）
33.		配合本校資安相關措施發現需改善之系統漏洞，應配合於合約有效期內無償進行修補改正	本校可定期進行資訊安全演練、入侵偵測、弱點掃瞄、應用程式防火牆WAF、SSL 等資安相關措施，如發現需改善之系統漏洞，廠商應配合於合約有效期內無償進行修補改正。	☑符合 ☐未符合 ☐不適用	合約 6-3（p.3）

資通安全管理法施行細則第四條法規要求

學校可定期執行資安措施，廠商需配合修正相關措施所發生之風險

國立臺北大學 National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

34.	1.演練計畫 2.演練記錄	業務持續運作演練 (中、高級系統適用)	廠商應配合本校指定流程，協助進行業務持續運作演練，確保系統緊急中斷、災害發生時之應對處理。	☐符合 ☐未符合 ☑不適用	本案非中、高級系統。
35.		災難還原機制 (中、高級系統適用)	當系統發生重大事故、中斷、錯誤無法運行，或系統無法復原之情境，廠商應協助將備援資料還原至設備並再度啟用系統，令本校業務持續進行。	☐符合 ☐未符合 ☑不適用	本案非中、高級系統。
36.		提供資料庫最高存取權限	廠商需提供資料庫的存取權限、資料綱要的文件說明，本校需擁有系統及資料庫存取之最高權限。	☑符合 ☐未符合 ☐不適用	合約 6-6（p.4）
37.		不得輸入或採取任何資料	廠商維修人員不得輸入任何干擾程式或探取、損壞、消除、竊閱、洩漏本校輸入電腦資料，如有上列情形，願負一切法律上之責任。	☑符合 ☐未符合 ☐不適用	合約 5-6（p.3）
38.		引(使)用開源程式碼(Open Source)	開發設計之原始碼若引(使)用開源程式碼(Open Source)或模組須符合 GNU 與 GPL 規範。	☐符合 ☐未符合 ☑不適用	本網站未引用開源程式碼。
39.		符合資通安全管理法施行細則第四條	必須完整符合資通安全管理法施行細則第四條之委外系統所需事項。	☑符合 ☐未符合 ☐不適用	合約 5-4（p.3）
40.		SSL 憑證安裝及費用歸屬 （有憑證要求者適用）	敘明安裝權責及費用歸屬並載明私鑰保存方式。憑證需支援 SSL 傳輸協定(不得超過13個月且費用需含於此案中)，應移除 TLS 1.1(含)以前版本並相容於 TLS1.2與1.3以上版本支援。	☑符合 ☐未符合 ☐不適用	合約 5-4（p.3）
41.	教育訓練及輔導上線	教育訓練場次時間	規劃系統管理人員及系統使用人員教育訓練___次以上，每次___小時。	☐符合 ☐未符合 ☑不適用	本案係屬維護故不再提供，但提供諮詢服務。
42.		輔導上線機制	上線時廠商是否到場支援或以其他方	☐符合	本案係屬維護故不再提供。

中高等級系統每年需請廠商提供演練與還原流程與報告

單位取得資料庫最高權限，可避免廠商惡意破壞

避免廠商人員於程式中放置惡意程式

法規面重新要求

針對使用者或管理者提供教育訓練

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

			式支援。	☐未符合 ☑不適用	
43.	權利及責任	提供合法之軟體、文件或圖片	廠商所提供或使用之軟體、文件或圖片需合法並提供使用授權，不得違反智慧財產權行為，如有違反智慧財產權者，廠商應承擔所有法律責任。	☑符合 ☐未符合 ☐不適用	合約 8 （p.4）
44.		智慧財產權歸屬	廠商履約結果涉及智慧財產權者，著作財產權歸本校所有，廠商對本校不行使著作人格權。	☑符合 ☐未符合 ☐不適用	合約 8 （p.4）
45.		派駐點或維修人員發生嚴重不當行為	廠商派駐修人員發生嚴重不當行為違反相關資安政策，須立即暫停職務、存取權限與特權，必要時立即將其護送出該場域。	☑符合 ☐未符合 ☐不適用	合約 5-7 （p.3）
46.		派駐點或維修人員違反相關政策	廠商派駐修人員違反相關資安政策，依契約相關罰則進行處置，如情節造成重大資安事件達「資通安全事件通報及應變辦法」或本校「資通安全事件管理程序」之事件等級3級以上，本校將立即終止及解除契約，並自負違反法律之責。	☑符合 ☐未符合 ☐不適用	合約 5-7 （p.3）
47.		保有契約內資訊安全相關作業稽核之權利	本校保有本校及與第三方稽核單位或人員至委外廠商進行契約內資訊安全相關作業稽核之權利，廠商不得拒絕。	☑符合 ☐未符合 ☐不適用	合約 5-2（p.3）

智慧財權歸屬與廠商使用圖片之要求

針對維護人員進行要求

保留對廠商查核的權利

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

48.	行動化應用程式(APP)	敘明 APP 上架評估及費用歸屬 (有建置 APP 者適用)	需配合教育部規範，上架逾一年下載次數未達一萬次以上需下架。 敘明上架費用歸屬。	☐符合 ☐未符合 ☑不適用	本案未提供 APP 服務。	有提供APP之系統需載明相關資安要求與費用
49.		敘明 APP 檢測規範及費用歸屬 (有建置 APP 者適用)	需配合「行政院及所屬各機關行動化服務發展作業原則」，並通過經濟部訂定行動化應用軟體之檢測項目。 敘明檢測費用歸屬	☐符合 ☐未符合 ☑不適用	本案未提供 APP 服務。	
50.	物聯網設備	行政院國家通訊傳播委員會(NCC)規範之物聯網設備	配合 NCC 之要求，公務單位必須優先採購已取得經濟部物聯網資安驗證標章之產品。	☐符合 ☐未符合 ☑不適用	本案未提供物聯網服務。	物聯網設備需取得資安標章及非陸系品牌
51.	涉及國安或具敏感性或含資安	敘明是否限制陸資	本案之資通電訊設備或系統如「涉及國家安全採購」、「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購包含複委託，禁止大陸地區廠商、第三地區含陸資成分廠商、在臺陸資廠商參與。	☑符合 ☐未符合 ☐不適用	合約 5-4（p.3）	系統與設備採購需為非陸系品牌，複委託亦同

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

52.	系統環境建置/維護	系統軟硬體建置	本案軟硬體設備放置區域與管理要求。	☑符合 ☐未符合 ☐不適用	合約1-5（p. 2）
53.		系統軟硬體規格	依系統負載使用人數評估 CPU、記憶體、空間等需求。	☑符合 ☐未符合 ☐不適用	合約1-5（p. 2）
54.		作業系統及版本	最新穩定版或為最新長期支援(Long-Term Support)版本，且具有二年以上之產品更新生命週期(請敘明版本號)。	☑符合 ☐未符合 ☐不適用	合約1-5（p. 2） ubuntu 18.04 eol
55.		應用程式伺服器及版本	最新穩定版或為最新長期支援(Long-Term Support)版本，且具有二年以上之產品更新生命週期(請敘明版本號)。	☑符合 ☐未符合 ☐不適用	合約1-5（p. 2） Apache HTTP Server 2.4.60
56.		資料庫伺服器及版本(有資料庫適用)	最新穩定版或為最新長期支援(Long-Term Support)版本，且具有二年以上之產品更新生命週期(請敘明版本號)。	☑符合 ☐未符合 ☐不適用	合約1-5（p. 2） MySQL 5.7 EOL
57.		核心開發程式及版本	最新穩定版或為最新長期支援(Long-Term Support)版本，且具有二年以上之產品更新生命週期(請敘明版本號)。	☑符合 ☐未符合 ☐不適用	合約1-5（p.2） PHP 7.4
58.		其他開發技術及版本(如無則不適用)	最新穩定版或為最新長期支援(Long-Term Support)版本，且具有二年以上之產品更新生命週期(請敘明版本號)。	☐符合 ☐未符合 ☑不適用	本案不包含其他開發技術。

軟硬體存放是否符合資安要求

說明系統所需軟硬體規格

說明系統所使用之軟體規格是否已不再支援或是無法升級，如果無法更新，需說明改善計畫

國立臺北大學 National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐[illegible]

59.	資料備援及移置	定期備份資料	廠商應協助定期備份資料庫、電子檔案、系統程式碼、系統設定、log 等資料，並明列各項機制說明及執行週期。	☑符合 ☐未符合 ☐不適用	合約 6-4（p.3）
60.		系統及資料庫移置、新舊系統資料移轉	若因資料量增加或其它因素，需更換設備或升級作業系統，廠商應無條件協助移轉新舊系統及資料庫。	☑符合 ☐未符合 ☐不適用	合約 6-8（p.4）
61.	資訊安全	主機防火牆設定	拒絕所有連線，只開放必要之通訊埠連線及管理者 IP 連線。	☑符合 ☐未符合 ☐不適用	合約1-5（p.2）
62.		主機連接埠設定	關閉不必要連接埠。	☑符合 ☐未符合 ☐不適用	合約1-5（p.2）
63.		主機校時	主機系統校時設定，需排程每日向本校時間校時主機(time.ntpu.edu.tw)進行校時。	☑符合 ☐未符合 ☐不適用	合約1-5（p.2） 設定學校校時主機（time.ntpu.edu.tw）
64.	維護服務範圍	維護保固項目	維持本案所含相關系統功能正常運作。	☑符合 ☐未符合 ☐不適用	合約 6（p.3）
65.		功能增修需求	可配合本校有功能增修需求，依雙方討論同意後執行。	☑符合 ☐未符合 ☐不適用	合約 6-8（p. 4）

需定期進行資料備份，此要求需滿足單位對可容許資料損失之要求

單位如需增加資料容量，需將針對廠商的要求列於保約中

避免不必要的系統連線，可以減少資安攻擊事件的發生

同步時間，可做為日後資安稽核的依據

說明維護的目與是否可配合單位進行功能增修的權利

國立臺北大學 National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

66.	維護內容	諮詢服務	提供單一諮詢窗口、系統的操作問題與說明、e-mail 及客服電話諮詢。	☑符合 ☐未符合 ☐不適用	合約 3-3（p.2）
67.		伺服器硬體維護 (有伺服器管理適用)	相關伺服器硬體調校與升級及漏洞修補。	☑符合 ☐未符合 ☐不適用	合約 6-3（p.3）
68.		伺服器作業系統維護 (有伺服器管理適用)	相關伺服器作業系統調校與升級及漏洞修補。	☑符合 ☐未符合 ☐不適用	合約 6-3（p.3）
69.		應用系統維護	1.平台相關維護。 2.log 檔清除整理。 3.平台效能調校(tuning)。 4.除錯、更新、漏洞修補與弱掃修正。 5.硬碟空間檢查與整理。 6.系統稽核。	☑符合 ☐未符合 ☐不適用	合約 6-4 （p.3）

廠商需提供明確的聯絡資訊與窗口

如廠商有負責管理伺服器硬體與作業系統，需進行系統更新與維護作業

維護廠商需針對平台進行檢視，並留存相關記錄

維護內容需包含

國立臺北大學 National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

70.	維護方式	系統發生問題時處理方式	當維護標的系統發生問題時，廠商在接到本校通知後，應負責與系統相關問題之診斷及排除，進行系統相關資料、程式之救援與回復。	☑符合 ☐未符合 ☐不適用	合約 6-3 （p.3）
71.		於服務時間內依以下方式處理	緊急狀況：屬系統無法運作之情況，於 4 小時內電話回覆並處理，廠商應於通報後 8 工作小時內恢復運作。 其他狀況：於 8 工作小時內回覆或透過遠端連線完成維護服務，如線上無法解決，本校得視狀況決定廠商是否需到達系統所在地進行檢修，24 工作小時內完修。	☑符合 ☐未符合 ☐不適用	合約 3-4、3-5 （p.2）
72.		服務時間	星期一至星期五 AM 8:00 ~ PM 17:00，不含國定假日。	☑符合 ☐未符合 ☐不適用	合約 3-2 （p.2）
73.		連線方式	遠端連線或到場維護，遠端連線需要維護時才開放之模式。	☑符合 ☐未符合 ☐不適用	合約 6-3（p.3）

廠商在接獲單位通知發生異常時，需在指定時間內進行回應與故障排除

廠商需明訂維護服務時間及說明維護系統的方式

國立臺北大學 National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

74.	交付文件	軟體授權證明書	註明產品授權數、授權使用期間。	☐符合 ☐未符合 ☑不適用	相關文件已於本網站建置案中提交，本維護案不再提供。
75.		保固保證書	註明保固期間，免費修復及維護方式。	☐符合 ☐未符合 ☑不適用	本案係屬維護，故相關內容清參照整份維護合約說明。
76.		系統架構圖	伺服器硬體等級與系統組成及相關運作流向說明。	☐符合 ☐未符合 ☑不適用	相關文件已於本網站建置案中提交，本維護案不再提供。
77.		系統建置及管理手冊	包含相關系統安裝、版本，系統服務啟動與停止、系統備份與還原、系統log等路徑及指令說明。	☐符合 ☐未符合 ☑不適用	相關文件已於本網站建置案中提交，本維護案不再提供。
78.		管理者操作手冊	管理者相關功能手冊。 提供系統更新後最新版本文件。	☐符合 ☐未符合 ☑不適用	相關文件已於本網站建置案中提交，本維護案不再提供。
79.		使用者操作手冊	使用者相關功能手冊。 提供系統更新後最新版本文件。	☐符合 ☐未符合 ☑不適用	相關文件已於本網站建置案中提交，本維護案不再提供。

廠商需提供軟體授權與保固證明書

系統架構圖需清楚說明軟硬體的組成與資料流向

廠商需提供完整之架構與使用手冊

國立臺北大學 National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

80.		提供程式原始碼及最新文件	廠商應提供程式原始碼及系統相關操作、說明文件，日後若系統升級或新增功能，廠商需主動提供系統變化的文件說明。	☑符合 ☐未符合 ☐不適用	合約 6-3（p.3）	廠商需提供最新原始碼與第三方套件之原始碼
81.		資料庫 Schema (有資料庫系統適用)	提供最新版本，包含資料表名稱、欄位名稱、欄位描述、欄位類型、長度、允許空值等。密碼欄位均不得採用明碼或可還原之編碼或加密演算法儲存，雜湊(Hash)函數使用必須使用SHA2以上版本並視情況加鹽(Salt)。	☑符合 ☐未符合 ☐不適用	合約 6-3（p.3）	廠商需提供最新之資料庫結構
82.		定期維護報告	定期維護報告：每 1 至少提供一次的系統維護報告，並以電子郵件或紙本方式提供相關系統現況之資訊。例如：系統是否有不正常紀錄，如使用者登入登出紀錄、使用者帳號與群組之異動、特殊權限帳號之異動與存取紀錄、系統參數之異動、重要資料存取成功與失敗紀錄、系統錯誤事件等系統稽核、硬碟空間、記憶體使用容量、備份清冊等報告。	☑符合 ☐未符合 ☐不適用	合約 6-4 （p.3）	廠商需提供定期維護報告
83.		委外廠商資通安全檢核表	廠商需於請購核銷時，提供「國立臺北大學委外廠商資通安全檢核表」。（相關表單請於資訊中心表單中下載）	☑符合 ☐未符合 ☐不適用	合約 6-8（p.4）	廠商需於請購核核時提供委外廠商資通安全檢核表

核銷時提供(影本)

國立臺北大學 National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用 ☐內部使用 ☐限制使用 ☐授權使用

84.	資訊安全	效能檢測報告 (由單位定義使用效能)	需檢附自行或第三方驗證之效能檢測報告，符合本校同時連線人數及回應秒數之正常使用需求。	☑符合 ☐未符合 ☐不適用	合約 6-8（p. 4）	單位可依需求評估是否需要對系統進行效能檢測
85.		源碼檢測報告 (高級系統適用)	需檢附自行或第三方驗證源碼檢測報告，無中等級(含)以上風險。	☐符合 ☐未符合 ☑不適用	本案非高級系統。	高等級系統需進行源碼檢測
86.		弱點掃瞄報告	需檢附自行或第三方驗證弱點掃瞄報告，無中等級(含)以上風險。必須符合行政院-政府機關弱點掃描服務委外服務案建議書徵求文件最新版。	☑符合 ☐未符合 ☐不適用	合約 6-8（p. 4）	廠商需提供無中等級以上風險之弱點掃瞄報告
87.		滲透測試報告 (高級系統適用)	需檢附自行或第三方驗證滲透測試報告，無中等級(含)以上風險。必須符合行政院-政府機關滲透測試服務委外服務案建議書徵求文件最新版。	☐符合 ☐未符合 ☑不適用	本案非高級系統。	高等級系統需進行系統滲透測試
88.		業務持續運作計畫演練報告或資料回復測試作業(中、高級系統適用)	需每年至少進行乙次業務持續運作演練或資料回復測試作業。	☐符合 ☐未符合 ☑不適用	本案非高級系統。	中、高等級系統需每年進行一次業務持續演練或資料回復測試，並留存記錄

演練資料需包括
演練計畫(開始前呈核)、腳本、演練記錄

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

機密等級：☑公開使用☐內部使用☐敏感☐機密

委外資訊系統建置/開發/維護需求標準作業流程各檢核重點遵循資通安全管理法、個人資料保護法、資通安全責任等級分級辦法及政府法規與本校資訊安全管理制度(ISMS)等規範訂定要求。請依資訊中心審核說明及建議修正於招標需求書或規格文件並併入正式合約，若有未符合法規或未改善事項由單位自行負責。	
申請單位	
承辦人	單位主管
連絡分機/email：	

二、資訊中心審核說明

資訊中心檢核說明及建議		
☐符合 ☐不符合（原因如下）		
資訊中心	承辦人	單位主管

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

國立臺北大學委外廠商資通安全檢核表

說明：

1.依據行政院「資通安全管理法」第九條及「資通安全管理法施行細則」第四條辦理。

2.執行流程，可擇一進行：

(1)本校業務單位對廠商進行實地現場訪視或調閱資料，進行稽核作業。

(2)廠商(定期)自我檢核後，由本校業務單位進行複檢。

廠商名稱		填表日	年　月　日
填表人		電話	

表單由廠商填寫並提供給單位留存備查，請購核銷時請附上影本

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

檢核項目	檢核重點	檢核結果	檢核發現
1.資安管理			
1.1是否通過資通安全相關驗證(如 ISO 27001/CNS 27001)或訂定資安相關規範？	• 檢視 ISO 27001 / CNS 27001證書與定期審查報告，廠商是否仍維持證書之有效性？ • 驗證範圍與專案作業範圍具有關聯性？ • 是否已建立資通安全管理文件與表單？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
1.2是否建立資通安全事件通報及應變處理機制，若發生資通安全事件立刻通報機關並執行相關應變措施？	• 是否已建立資通安全事件通報及應變處理相關程序規範？ • 是否知道如發生資安事件應通報本校窗口人員之聯絡方式？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
1.3人員是否接受資安相關訓練？	• 專案人員是否均曾接受過資安相關教育訓練？ • 如何確認教育訓練之有效性？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
1.4員工是否了解本校資安相關規範？	• 專案人員是否取得本校資安相關規範？ • 專案人員作業時，是否依本校資安規定執行？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
2.資安防護			
2.1是否建置防毒機制並定期更新病毒碼(主機、個人電腦、筆記型電腦、電子郵件、行動載具)?	• 專案相關人員使用之電腦設備是否已安裝防毒軟體？ • 防毒軟體之病毒碼已更新到最新版本？ • 防毒軟體是否已設定定期執行全磁碟掃描？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	

通過ISO27001或已導入相關程序與建立文件

建立廠商自身通報程序以及是否了解學校通報人員聯絡方式

廠商資訊設備是否建置防毒相關機制

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

檢核項目	檢核重點	檢核結果	檢核發現
2.2外部網路是否建置防駭機制(防火牆、入侵防禦系統)?	• 檢視網路架構圖，內外網間是否架設防火牆、入侵偵測系統等安全設備？ • 防火牆是否由專人管理？如有代理人，是否使用個別帳號？ • 防火牆是否限定能夠連線登入的網段？ • 防火牆開通出入管制規則(policy)是否須先提出申請核准？ • 防火牆是否產出紀錄，並定期檢視紀錄？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
2.3專案相關設備是否建置系統監控機制?	• 專案相關伺服器是否已建立容量(如：CPU、RAM 或硬碟)監控機制？ • 專案相關伺服器如發生異常是否已建立處理機制？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
2.4專案相關設備是否保留稽核軌跡(Log)?	• 專案相關伺服器是否已保存作業系統相關紀錄？ • 是否已訂定紀錄保存機制？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	

維護或建置廠商協助確認防火牆與相關資監控與LOG保存是否完備

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

2.5專案相關設備是否安置於受管制之區域？	• 專案相關伺服器是否放置於機房並放置於機架中？ • 機房是否設有門禁管理措施？ • 門口是否設有監視設備？監視設備影像是否至少保存六個月以上？ • 機房內是否有溫溼度管理措施？ • 機房內是否有消防設施？是否設有氣體式(CO2、新海龍等)手提滅火器？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
2.6專案相關設備是否定期進行弱點掃描並修補弱點?	• 是否定期執行弱點掃描？產出報告中是否包含專案相關設備？ • 是否已針對弱點進行評估或修補並留下紀錄？ • 是否於修補後執行複測？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	

專案若委外存放，維護或建置廠商協助確認伺服器存放安全

維護或建置廠商協助確認主機相關弱點是否完善

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

檢核項目	檢核重點	檢核結果	檢核發現
3.1是否制訂軟體開發生命週期之安全規範?	• 是否已制定程式開發相關管理程序規範？ • 是否已制定程式撰寫之安全原則規定(如：命名原則、程式撰寫格式、程式錯誤語法範例等)	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
3.2是否建置「源碼掃描」機制並執行?	• 是否已制定程式原始碼掃描機制？ • 程式原始碼掃描後，是否執行評估與程式修改並進行複測？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
3.3是否建置「弱點掃描」機制並執行?	• 是否已制定程式弱點掃描機制？ • 程式弱點掃描後，是否執行評估與程式修改並進行複測？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
3.4是否管理測試資料及環境?	• 是否設置測試環境並限制僅有本專案人員可以存取？ • 測試環境之測試資料是否為真實資料？如為真實資料是否有嚴格的存取管制措施？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
3.5是否制訂軟體變更及組態管理之作業規範？	• 是否已建立程式、安裝軟體與組態變更管理機制？ • 執行變更前是否均先測試並經申請核准後才能執行變更？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
3.6是否建立原始碼備份及版本管理機制?	• 是否已設置原始碼版本管控機制？ • 原始碼是否定期執行備份，並至少保存3代以上？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
3.7是否定期執行軟體與資訊完整性檢查?	• 是否定期檢查軟體與客戶資料內容之完整性？ • 檢查如有異常，是否建立復原機制？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	

維護或建置廠商協助確認程式開發時之各項資訊安全要求

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

4.資料保護			
4.1是否建立客戶資料保護機制(授權程序,存取管控,銷毀程序)?	• 是否建立客戶資料保護機制(如存取授權、存放位置規定等)？ • 資料銷毀是否需要先申請核准並留下銷毀方式之紀錄？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	
4.2契約終止後取得之客戶資料是否返還、確實刪除或銷毀?	• 先前契約完成驗收後客戶資料之處理方式？ • 資料返還或銷毀方式是否留有紀錄？	☐符合 ☐待改善項目 ☐缺失項目 ☐不適用	

維護或建置廠商協助確認資料保存與銷毀流程

如何確保合約結束後能完善進行資料返還或銷毀並留存記錄

國立臺北大學
National Taipei University

資訊安全日常作業說明（系統文件）

- NTPU-PIIS-D-004　委外廠商保密切結書
- 業務持續運作演練計畫（資訊系統適用)
- 資訊系統弱點掃瞄處理（資訊系統適用)
- 國立臺北大學系統採購檢核表-採購前
- 國立臺北大學委外廠商資通安全檢核表

由維護或建置廠商填寫

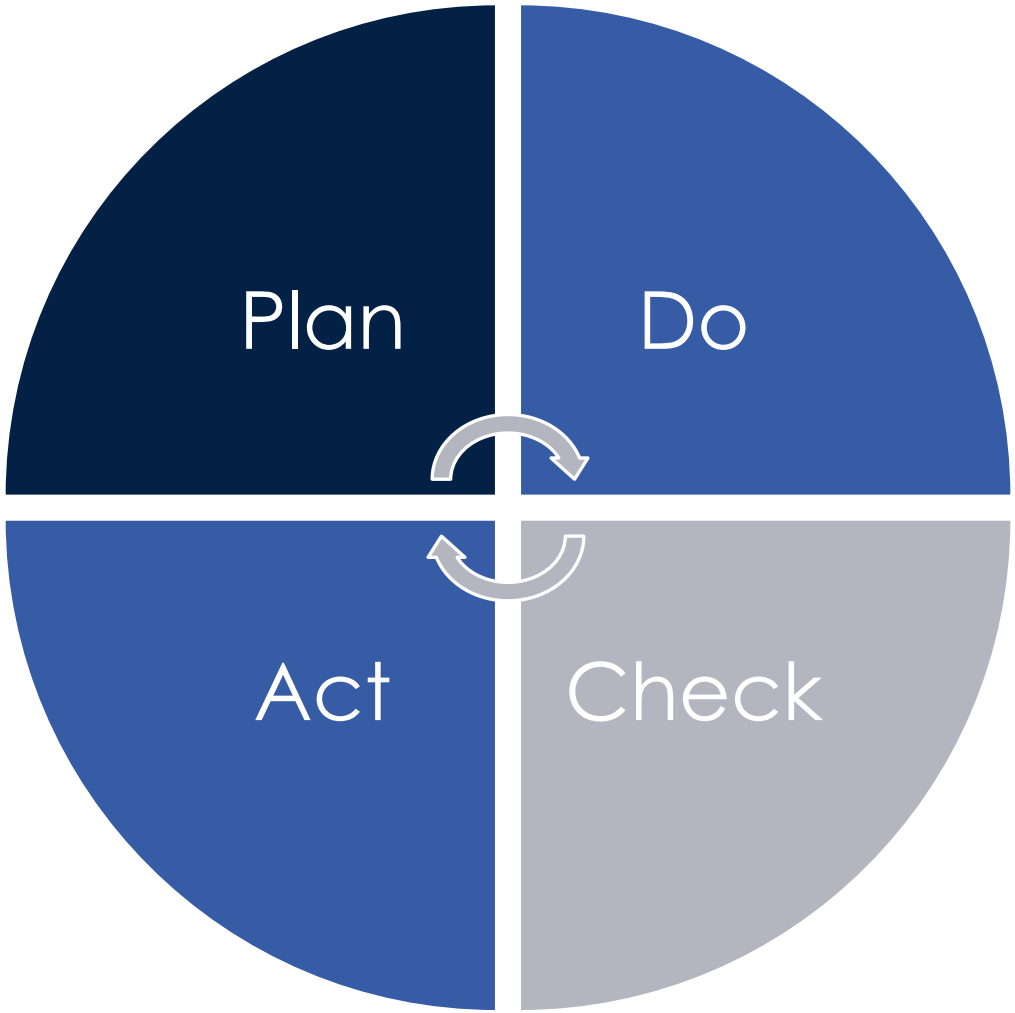
由業務單位填寫並檢核

廠商公司章		負責人簽章	

以下欄位由業務單位填寫					
檢查項目					
檢查結果	檢查結果 □符合 □部分符合 □不符合本校要求				
承辦人核章		二級主管核章		一級主管核章	
檢查日期		簽核日期		簽核日期	

總結

- 資通安全法規要求
- 校內ISMS要求
- 大陸廠牌資通訊產品及委外經營公眾場域盤點原則。
- 所屬公務機關及所管特定 非公務機關資通安全稽核計畫
- ISO27001 要求



- 資訊系統採購檢核表
- 委外廠商資通安全檢核表
- 系統需求與合約書
- 定期進行全系統備份
- 資訊系統帳號管理與清查
- 委外廠商保密切結
- 伺服器管理

- 修正資訊系統安全等級評估表
- 修正ISMS相關文件
- 修正系統需求與合約文件
- 調整資料備份規則
- 精進業務持續演練成效

- 系統與網頁弱點掃瞄
- 第三方稽核
- 滲透測試
- 源碼檢測
- 業務持續演練
- 資安事件通報
- 效能檢測

評量

https://forms.gle/i3CZLuo8TQnkBWpW7

國立臺北大學
National Taipei University

Q&A

報告完畢

如有疑義或不清楚之處，敬請使用以下方式連繫謝謝!
電洽：02-86741111分機68228
e-mail：ccsinfo@mail.ntpu.edu.tw
現場：圖資大樓二樓網路組辦公室（每日9：00-17：00）
（寒暑假期間9：00-16：00）