



國立臺灣大學
National Taiwan University

資通系統盤點說明

2025/01





本校資安政策與法規說明

本校資安政策

國立臺灣大學				
文件編號	NTU-IS1-01	文件名稱	版本	2.0
制定單位	資通安全管理委員會	資訊安全政策	頁數	/2

資訊安全政策

壹、目的

為確保國立臺灣大學（以下簡稱本校）之資訊資產的機密性、完整性、可用性與法律遵循性，並保障使用者資料隱私，以符合相關法規之要求，免於遭受內、外部蓄意或意外之威脅，並衡酌之業務需求，特訂定本政策。

貳、範圍

本校。

參、目標

- 一、保護本校業務安全，避免未經授權的存取，以確保資訊資產的機密性，並保障使用者資料隱私。
- 二、保護本校業務安全，避免未經授權的修改，以確保資訊資產的正確性與完整性。
- 三、依照 ISO 27001 要求，進行風險管理，落實品質管理循環（PDCA）精神，以持續改善資訊安全管理系統（ISMS）之有效性。
- 四、建立本校之業務持續運作計畫，以確保本單位業務服務之持續運作。
- 五、確保本校之各項業務服務之執行須符合相關法規之要求。

本校資安政策

肆、 責任

- 一、本校應成立資訊安全組織統籌資訊安全事項推動。
- 二、管理階層應積極參與及支持資訊安全管理制度，提供相關資源，並分配適當權責。
- 三、本校人員皆應遵守本政策、資通安全管理法、智慧財產權及個人資料保護法。
- 四、本校人員均有責任透過適當機制，通報資通安全事件或弱點。

伍、 審查

- 一、本政策應定期審查，檢視落實狀況，以確保有效性，並符合相關法規、主管機關及本校資訊安全要求。
- 二、當組織或業務發生重大改變時應主動進行審查。

陸、 發佈

本政策應定期公告週知，確保本校人員及利害關係團體瞭解相關規定。

柒、 實施

本政策經「資通安全管理委員會」核定後實施。

法規說明

因應教育部針對全校要求執行資通系統與IOT設備及大陸廠牌資通訊產品盤點盤點。

- 相關法令與施行細則
 - 一 資通安全管理法
 - 二 資通安全管理法施行細則



2

資通系統盤點說明

新增盤點項目—1



🏠 / 資通系統盤點

資通系統盤點

*防護需求等級出現【高】有紅點警示的話，送出彙整前建議先找我們諮詢，專業團隊協助你診斷系統藥到病除。

+ 新增 **+** 新增中英文網站平台填報範本 **全部送彙整**

序號	單位名稱	資通系統名稱	系統屬性	核心系統	防護需求等級	填報時間
1131	計算機及資訊網路中心程式設計組	test	行政	是	普	2025-01-07

如為使用「中英文網站」平台製作之網站，點選此選項新增。

如非使用「中英文網站」平台製作之網站，點選此選項新增。

新增盤點項目—2



國立臺灣大學
National Taiwan University

資通盤點系統

盤點專區 ▾

其他服務 ▾

登出 →



個人區



送彙整

🏠 / 資通系統盤點

資通系統盤點

※防護需求等級出現【高】有紅點警示的話，送出彙整前建議先找我們諮詢，專業團隊協助你診斷系統藥到病除。

➕ 新增

➕ 新增中英文網站平台填報範本

☁️ 全部送彙整

編輯	序號	單位名稱	資通系統名稱	系統屬性	核心系統	防護需求等級	填報時間
     	1131	計算機及資訊網路中心程式設計組	test	行政	是	普	2025-01-07

如為使用「中英文網站」平台製作之網站，
新增好後，點此進入編輯頁面。

※點選「新增」者，則會直接進入編輯頁面。

資通系統盤點平台欄位說明—1

新增



資通系統盤點

存檔

離開

第一階段 - 基本資料

填報單位 

程式設計組

系統名稱 

系統屬性 

行政

建置方式 

本機關委外開發

建置方式補充說明 

建置類型為【其他】時，必須填寫補充說明

建置廠商 

填寫建置廠商名稱or國立臺灣大學or主管/上級/其他機關名稱

建置廠商之統一編號 

維運廠商 

填寫維運廠商or國立臺灣大學or主管/上級/其他機關名稱

維運廠商之統一編號 

資通系統盤點平台欄位說明—2

欄位名稱	欄位說明
填報單位	請選擇資通系統所屬的單位
系統名稱	<ol style="list-style-type: none">1. 機關運用計畫經費所籌獲之資通系統亦應納入盤點2. 若為委外雲端服務，請填寫該雲端系統之名稱3. 有關係統盤點如係不同廠商所建置、維運，應盤出不同系統；另如機關係將各系統以群組命名，則一律納為高防護等級之系統，群組內各系統一律適用。
系統屬性	限填「行政」、「業務」、「兼具行政/業務」
建置方式	限填「本機關委外開發」、「本機關租用服務」、「本機關購置套裝軟體」、「本機關自行開發」、或「其他」
建置方式補充說明	「系統建置方式」為「其他」者必填

資通系統盤點平台欄位說明—3

欄位名稱	欄位說明
建置廠商	<ol style="list-style-type: none">1. 系統建置方式為「套裝軟體」者請填「套裝軟體」2. 若為機關自行開發者，請填寫該機關名
建置廠商之統一編號	<ol style="list-style-type: none">1. 若廠商無統一編號請填寫「0」2. 系統建置方式為「套裝軟體」者請填「2」3. 若為機關建置，請填寫該機關之OID
維運廠商	<ol style="list-style-type: none">1. 系統建置方式為「套裝軟體」者請填「套裝軟體」2. 若為機關自行維運者，請填寫該機關名
維運廠商之統一編號	<ol style="list-style-type: none">1. 若廠商無統一編號請填寫「0」2. 系統建置方式為「套裝軟體」者請填「2」3. 若為機關建置，請填寫該機關之OID

資通系統盤點平台欄位說明—4

系統IP	系統網址
<input type="text" value="IP寫法是140.112.1.1"/>	<input type="text"/>
主機實體位置	主機實體位置補充說明
<input type="text" value="計中虛擬主機租賃"/>	<input type="text" value="主機實體位置為其他的時候為必填"/>
主機設置於校內	核心系統
<input type="text" value="是"/>	<input type="text" value="是"/>
系統管理者	系統使用者
<input type="text"/>	<input type="text" value="全機關"/>
機敏資訊	加密機敏資訊
<input type="text" value="是"/>	<input type="text" value="是"/>
機敏資訊類別	民生權益相關
<input type="text"/>	<input type="text" value="是"/>
個資筆數	系統建置年月
<input type="text" value="無"/>	<input type="text" value="----年--月"/>

資通系統盤點平台欄位說明—5

欄位名稱	欄位說明
系統IP	系統IP (Internet Protocol) 指的是在互聯網或局域網中，用於識別和定位計算機或網絡設備的唯一標識符。IP地址由一串數字組成，通常表現為四組由句點分隔的數字 (例如：192.168.0.1) 。
系統網址	系統網址是指一個網站、應用程式或服務的網絡地址，也稱為網站URL (Uniform Resource Locator) 。系統網址通常由幾個部分組成。 例如，一個標準的URL可能包含協議 (例如http://或https://) 、域名 (例如www.example.com) 和路徑 (例如/path/to/page) 等元素。這些部分組合在一起提供了一個完整的網址。
主機實體位置	主機實體位置是指計算機系統中主機 (通常是伺服器) 的物理位置或放置位置。這是指主機所在的地理位置或具體的建築物、機房或機櫃等實體位置。
主機實體位置補充說明	主機非放置校內請填寫補充說明。
主機設置於校內	限填「是」或「否」
核心系統	<ol style="list-style-type: none">1. 限填「是」或「否」2. 核心資通系統指支持核心業務持續運作必要之系統，或依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之規定，判定其防護需求等級為高者 註：機關之核心系統以應用系統為主

資通系統盤點平台欄位說明—6

欄位名稱	欄位說明
系統管理者	請填寫擁有系統管理權限功能者之所在部門/單位
系統使用者	<ol style="list-style-type: none">1. 請填寫主要使用該系統的單位(可為多個單位)，如為機關全單位都有使用，則填寫全機關2. 若系統為跨機關使用，亦請填寫使用該系統之機關，例如：直轄市、縣市政府3. 若該系統亦提供民眾使用，請加註「...處，且供民眾使用」
機敏資訊	限填「是」、「否」
加密機敏資訊	限填「是」、「否」、「無機敏資訊」
民生權益相關	限填「是」、「否」
機敏資訊類別	<ol style="list-style-type: none">1. 「無機敏資訊」者免填2. 機敏資訊：例如身分證字號、特種個資、稅務資料等
個資筆數	單位擁有個資的數量。
系統建置年月	請填系統上線日期，並以數字表示，例如於2023年3月上線之系統，本項應填「2023/3」

資通系統盤點平台欄位說明—7

第二階段 - 防護等級評估

系統是否對外[?]

是



開放遠端連線維護[?]

否



包含於ISMS導入範圍[?]

是



有流量清洗機制[?]

是



備妥靜態網頁[?]

是



每天尖峰使用人數[?]

1000人以下



系統日誌保存超過6個月[?]

是



禁用弱密碼[?]

是



系統有備份[?]

是



有CDN啟用作業程序[?]

是



可10分鐘內切換至靜態網頁[?]

是



使用頻率[?]

隨時



資通系統盤點平台欄位說明—8

欄位名稱	欄位說明
系統是否對外	1. 限填「是」、「否」 2. 「系統對外」係指以網際網路即可連線檢視或使用之系統
系統日誌保存時間超過6個月	限填「是」、「否」
開放遠端連線維護	限填「有」、「無」 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」
禁用弱密碼	限填「是」、「否」、「不適用」
包含於ISMS導入範圍	限填「是」、「否」
系統有備份	系統備份是指將計算機系統中的數據、應用程式、配置和設定等重要資訊複製並保存到另一個儲存媒介或位置的過程。

資通系統盤點平台欄位說明—9

欄位名稱	欄位說明
有流量清洗機制	非為對外之系統，本項請填「非對外系統」
有CDN啟用作業程序	非為對外之系統，本項請填「非對外系統」
備妥靜態網頁	非為對外之系統，本項請填「非對外系統」
可10分鐘內切換至靜態網頁	非為對外之系統，本項請填「非對外系統」
每天尖峰使用人數	系統每日於熱門使用時段的使用人數。
使用頻率	系統的使用頻率。

資通系統盤點平台欄位說明—10

機密性 (連動防護需求等級) ⓘ	完整性 (連動防護需求等級) ⓘ
普 ▼	普 ▼
可用性 (連動防護需求等級) ⓘ	法律遵循性 (連動防護需求等級) ⓘ
普 ▼	普 ▼
資通系統防護需求等級 ⓘ	系統回復時間目標(RTO) ⓘ
普 ▼	3天以內 ▼
資料回復目標點(RPO) ⓘ	最大可容忍中斷時間(MTPD) ⓘ
30天 ▼	4天 ▼
備註 ⓘ	
<input type="text"/>	

 存檔  離開

資通系統盤點平台欄位說明—11

欄位名稱	欄位說明
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面產生影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面產生影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面產生影響。
法律遵循性	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。
資通系統防護需求等級	限填「普」、「中」、「高」、「套裝軟體」

資通系統之防護需求等級之四大構面



資通系統防護需求分級原則—機密性

分級原則說明	分級
發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生「 非常嚴重 」或「 災難性 」之影響。	高
發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生「 嚴重 」之影響。	中
<ol style="list-style-type: none">發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生「有限」之影響。儲存特種個資或大量個資者，不得評為普。	普

資通系統防護需求分級原則—完整性

分級原則說明	分級
發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生「 非常嚴重 」或「 災難性 」之影響。	高
發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生「 嚴重 」之影響。	中
發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生「 有限 」之影響。	普

資通系統防護需求分級原則—可用性

分級原則說明	分級
<ol style="list-style-type: none">發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生「非常嚴重」或「災難性」之影響。最大可容忍中斷時間 (MTPD) 低於8小時者，應評為高。	高
發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生「 嚴重 」之影響。	中
發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生「 有限 」之影響。	普

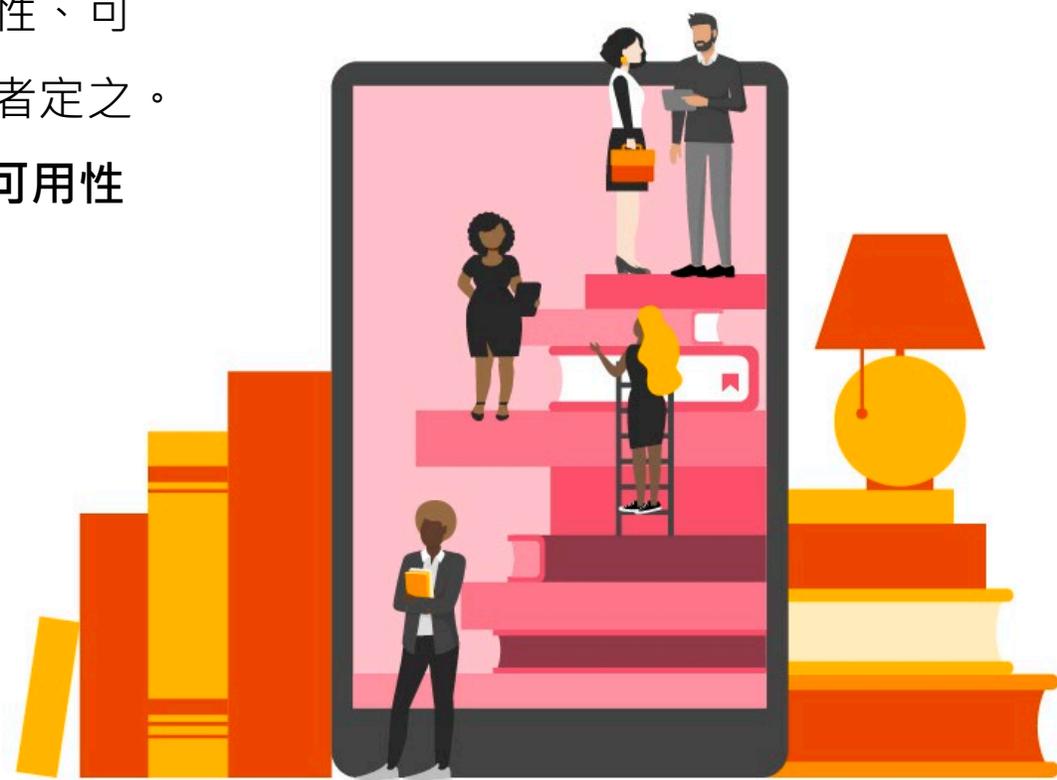
資通系統防護需求分級原則—法律遵循性

分級原則說明	分級
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，並使機關所屬人員負 刑事責任 。	高
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，並使機關或其所屬人員受 行政罰、懲戒或懲處 。	中
其他資通系統設置或運作於法令有相關規範之情形。	普

資通系統之防護需求等級之判斷

- 資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性 & 法律遵循性構面中，任一構面之防護需求等級之最高者定之。
資通系統之防護需求等級=Max(機密性分級，完整性分級，可用性分級，法律遵循性分級)
- 判斷是否為核心系統

防護需求等級	高	中	低
	核心系統	核心系統/非核心系統	非核心系統



資通系統盤點平台欄位說明—12

欄位名稱	欄位說明
最大可容忍中斷時間 (MTPD)	最大可容忍中斷時間 (Maximum Tolerable Period of Disruption, MTPD) 關鍵業務發生中斷後，恢復至最低運作水準，所能容許的中斷時間。
系統回復時間目標(RTO)	系統回復時間目標 (Recovery Time Objective，簡稱RTO) 即業務中斷可容忍回復時間，於基礎設施正常供應下，核心業務從資通安全事件或災難發生到業務復原的目標時間。
資料回復目標點(RPO)	資料回復目標點 (Recovery Point Objective，簡稱RPO) 是指於基礎設施正常供應下，核心業務從資通安全事件或災難發生到復原期間資料所能回復的時間點。



Thank you

簽到連結



© 2024 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.