國立陽明交通大學校園網站健檢

為有效確保本校網站服務品質，提升資訊安全，並提供各單位於規劃、建置及維護管理本校網站服務時有所遵循，擬於 110 年 9 月 1 日至 10 月 15 日進行校園網站健檢。

一、 適用範圍：本校行政單位、學院及系所網頁。

二、 網頁健檢指標內容說明：

（一）網站介面（10 分）

1、 版面規劃

（1） 網站名稱及標誌(Logo)

（2） 網站資訊開放宣告

（3） 個人資料保護及資訊安全宣告

（4） 網站頁籤圖示(Favicon)

2、 語言版本

網站具備多語言版本供使用者選擇。

3、 網站導覽功能

提供描述網站之網站地圖(Sitemap)連結架構，讓使用者在網站瀏覽上的資訊需求能快速獲得，並提高 SEO 搜尋引擎優化效果。

（二）網站內容（12 分）

1、 公告資訊

單位經營之業務、活動、展覽、徵才等對外公開的訊息，如：最新消息、業務公告訊息、活動訊息等。

2、 單位介紹或業務資訊

單位基本資料，如：組織架構、業務執掌（主管業務範圍內的服務項目或核心資訊）、歷史沿革、所屬單位介紹、資料統計或出版品（研究成果發表、刊物）等。

3、 單位聯絡資訊

單位基本聯絡資訊，如單位電話（含區域號碼）、傳真、完整通訊地址（含郵遞區號）、交通資訊、位置圖、Email 及單位服務時間等。

4、 人員/師資負責業務及聯絡資訊

單位內各業務承辦人的姓名、業務內容、聯絡電話及 Email。

5、 相關連結

提供上級單位網站連結及相關專業性質網站連結，依屬性分類呈現。

6、 便民服務

提供申辦項目之表單下載服務。

（三）維運管理與資訊安全（46 分）

1、 內容更新

（1） 網站最新消息、新聞稿或公告資訊等，應標示更新日期，並依日期由新至舊排列。

（2） 從本校首頁能正確連結。

（3） 版權宣告標示年份及更新日期者，應更新至最新年度。

2、 有效連結

網站提供之連結，應確保其連結有效性。

（本項檢測工具為：Dr. Link Check，網址：https://www.drlinkcheck.com/）

3、 更新頻率

健檢期間「前 2 個月」內網站內容更新數量，例如：最新消息、活動資訊、新聞稿或公告等，且包含更新日期及有效期限。

4、 加密連線

網站使用 HTTPS 加密連線，除安裝 SSL 憑證，尚需完成強制導入 HTTPS，並排除混合內容問題。

5、 網頁防護

網頁應設置防火牆防護機制，如：網頁防火牆（WAF）。

若為開源程式碼之 WAF 或自行建置，請提出相關證明（如：設定畫面、軟/硬體廠牌）。

6、 弱點掃描

依資訊中心提供之弱掃結果進行改善，並回覆資訊中心弱點處理報告，經複掃確認已排除高、中弱點。

（詳細「網站健檢弱點檢測計畫」請參考附件一）

（四）網站服務（12 分）

1、 站內搜尋服務

提供站內搜尋服務，搜尋輸入框應置於版面明顯之處，且可搜尋近期發布之內容。

2、 意見回饋

提供管道供使用者申訴或提出意見、反應問題；如：意見信箱（或首長信箱）、留言版、問卷調查等。

3、 文件格式

提供下載之文件應全數提供通用格式。可編輯者提供 ODF、不可編輯者提供 PDF，並標示檔案格式。

4、 符合無障礙網頁規範

通過無障礙 2A 等級以上檢測。檢測工具：Freego 2.0，安裝說明網址：

https://accessibility.ncc.gov.tw/News/Detail/4376?Category=43。

（五）行動友善：網站支援行動裝置，可自動偵測裝置導向至行動版。（10

分）

1、 響應式網頁設計（RWD）或自適應式網頁設計（AWD）

網站設計應採用響應式網頁設計（RWD）或自適應式網頁設計（AWD）設計，以提升行動裝置瀏覽便利性。

2、 網頁載入速度

網站應確保網頁載入所需的時間維持適當的水準，以免影響使用體驗。（本項檢測工具為：PageSpeed Insights，網址：https://developers.google.com/speed/pagespeed/insights/；平均分數＝(行動版得分+電腦版得分)/2）

（六）外語網站維運（10 分）

1、 網站外語版

考量外語人士之使用需求，提供業務網站外語版。

2、 外語版更新

提供外語版最新消息、新聞稿或公告資訊等並定期更新，於健檢期間前 2 個月至少有 1 項更新，另應標示更新日期，並依日期由新至舊排列。

3、 外語版業務說明

提供外語版單位重要政策或重點業務說明。

4、 外語版單位聯絡資訊

除了基本聯絡資訊（電話、傳真、地址、交通資訊、位置圖、Email、時間等）外，也可提供業務承辦人的服務專線及 Email。

5、 外語版民意回饋

提供管道給使用者提供意見及反應問題，如：意見信箱（或首長信箱）、留言版、問卷調查等。

（七）創新應用及其他：本項採加減分制

1、 提供線上申辦

業務網站提供線上申辦服務。

2、 系統防護

「資通系統防護基準表」落實及達成率。

（詳細「資通防護基準作業程序」請參考附件二）

表 1 網站健檢指標及配分表

指標	次指標	摘要說明	配分	給分條件
網站介面(10%)	版面規劃	網站名稱及標誌(Logo)	4	符合 1 項：給 1 分（最高給 4 分）； 無：給 0 分。
		網站資訊開放宣告		
		個人資料保護及資訊安全宣告		
		網站頁籤圖示(Favicon)		
	語言版本	網站具備多語言版本供使用者選擇	2	有：給 2 分； 無：給 0 分。
	網站導覽功能	提供描述網站之網站地圖(Sitemap)連結架構，讓使用者在網站瀏覽上的資訊需求能快速獲得，並提高 SEO 搜尋引擎優化效果。	4	有：給 4 分； 無：給 0 分。
★網站內容(12%)	公告資訊	單位經營之業務、活動、展覽、徵才等對外公開的訊息，如：最新消息、業務公告訊息、活動訊息等。	2	有：給 2 分； 無：給 0 分。
	單位介紹或業務資訊	單位基本資料，如：組織架構、業務執掌（主管業務範圍內的服務項目或核心資訊）、歷史沿革、所屬單位介紹、資料統計或出版品（研究成本發表、刊物）等。	2	有：給 2 分； 無：給 0 分。
	單位聯絡資訊	單位基本聯絡資訊，如單位電話（含區域號碼）、傳真、完整通訊地址（含郵遞區號）、交通資訊、位置圖、Email 及單位服務時間等。	2	有：給 2 分(至少三項)； 無：給 0 分。
	人員/師資負責業務及聯絡資訊	單位內各業務承辦人的姓名、業務內容、聯絡電話及 Email。	2	有：給 2 分； 無：給 0 分。
	相關連結	提供上級單位網站連結及相關專業性質網站連結，依屬性分類呈現。	2	有：給 2 分； 無：給 0 分。

	便民服務	提供申辦項目之表單下載服務	2	有：給 2 分； 無：給 0 分。
★ 維運管理與資訊安全 (46%)	內容更新	網站最新消息、新聞稿或公告資訊等，應標示更新日期，並依日期由新至舊排列。	2	有：給 2 分； 無：給 0 分。
		從本校首頁能正確連結	2	有：給 2 分； 無：給 0 分。
		版權宣告標示年份及更新日期者，應更新至最新年度。	2	有：給 2 分； 無：給 0 分。
	有效連結	網站提供之連結，應確保其連結有效性。 （本項檢測工具為：Dr. Link Check）	4	皆為有效：給 4 分； 1 筆無效：給 2 分； 2 筆以上無效：給 0 分。
	更新頻率	健檢期間「前 2 個月」內網站內容更新數量，例如：最新消息、活動資訊、新聞稿或公告等，且包含更新日期及有效期限。	2	3 筆以上：給 2 分。 1~2 筆：給 1 分。 無：給 0 分。
	加密連線	網站使用 HTTPS 加密連線，除安裝 SSL 憑證，尚需完成強制導入 HTTPS，並排除混合內容問題。	8	全網站使用 HTTPS 並完成強制導入及排除混合內容問題：給 8 分。 全網站使用 HTTPS，完成強制導入，但未排除混合內容問題：給 6 分。 全網站使用 HTTPS，未完成強制導入：給 2 分。 無：給 0 分。
	網頁防護	網頁應設置防火牆防護機制，如：網頁防火牆（WAF）。若為開源程式碼之 WAF 或自行建置，請提出相關證明（如：設定畫面、軟/硬體廠牌）。	9	使用學校 WAF，其餘使用開源程式碼之 WAF 及自行建置者須提出管理證明(設定畫面、軟/硬體廠牌)：給 9 分； 無：給 0 分。
	弱點掃描	依資訊中心提供之弱掃結果進行改善，並回覆資訊中心弱點處理報告，經複掃確認已排除高、中弱點。 （詳細檢測計畫請參考附件	17	有：給 17 分； 無：給 0 分。

		一）		
網站服務(12%)	站內搜尋服務	提供站內搜尋服務，搜尋輸入框應置於版面明顯之處，且可搜尋近期發布之內容。	4	有：給 4 分； 無：給 0 分。
	意見回饋	提供管道供使用者申訴或提出意見、反應問題；如：意見信箱（或首長信箱）、留言版、問卷調查等。	2	有：給 2 分； 無：給 0 分。
	★ 文件格式	提供下載之文件應全數提供通用格式。可編輯者提供 ODF、不可編輯者提供 PDF，並標示檔案格式。	3	有：給 3 分； 無：給 0 分。
	符合無障礙網頁規範	通過無障礙 2A 等級以上檢測。（檢測工具：Freego 2.0）	3	有：給 3 分； 無：給 0 分。
行動友善(10%)	響應式網頁設計（RWD）或自適應式網頁設計（AWD）	網站設計應採用響應式網頁設計（RWD）或自適應式網頁設計（AWD）設計，以提升行動裝置瀏覽便利性。	5	具備 RWD/AWD：給 5 分； 無：給 0 分。
	網頁載入速度	網站應確保網頁載入所需的時間維持適當的水準，以免影響使用體驗。	5	70 分以上：給 5 分； 50~69 分以上：給 3 分； 30~49 分以上：給 1 分； 未滿 30 分：給 0 分。
外語網站維運(10%)	網站外語版	考量外語人士之使用需求，提供業務網站外語版。	2	有：給 2 分； 無：給 0 分；
	外語版更新	提供外語版最新消息、新聞稿或公告資訊等並定期更新，於健檢期間前 2 個月至少有 1 項更新，另應標示更新日期，並依日期由新至舊排列。	2	有：給 2 分； 無：給 0 分；
	外語版業務說明	提供外語版單位重要政策或重點業務說明。	2	有：給 2 分； 無：給 0 分；

	外語版單位聯絡資訊	除了基本聯絡資訊（電話、傳真、地址、交通資訊、位置圖、Email、時間等）外，也可提供業務承辦人的服務專線及 Email。	2	有：給 2 分； 無：給 0 分；
	外語版民意回饋	提供管道給使用者提供意見及反應問題，如：意見信箱（或首長信箱）、留言版、問卷調查等。	2	有：給 2 分； 無：給 0 分；
創新應用及其他(加減分)	提供線上申辦	業務網站提供線上申辦服務。	+2	本項採加分制，若有符合：總分加 2 分。
	系統防護	「資通系統防護基準表」落實及達成率。	+6	本項採加分制； 達成率達 100%，總分加 6 分； 達成率達 80%以上，總分加 4 分； 達成率達 60%以上，總分加 2 分；

註： 標記「★」項者，若其英文網頁為不同網站名稱，須另行檢測該項一同併入計分。

附件一

110 年國立陽明交通大學網站健檢弱點檢測計畫

一、計畫說明

鑑於網際網路環境蓬勃發展，學校公開資訊多數皆已數位化，為確保本校網站主機系統資訊安全，避免因具備弱點而遭有心人士利用、進行不當連線，資訊技術服務中心將針對校園網站主機系統進行弱點檢測，以維護校園資訊安全。

二、計畫目標

為提升維護本校網路安全性，及加強校園之資訊安全，並配合資通安全管理法、資通安全責任等級分級辦法、本校資通系統資訊安全管理規範之規定，進行資通網站主機系統弱點掃描檢測。

三、業務負責人

國立陽明交通大學 資訊技術服務中心 網路系統組 何馨晴、汪祐弘、張鈺欣
E-MAIL：heather.sc@nycu.edu.tw、youhong@nycu.edu.tw、yuhsin1021@nycu.edu.tw
連絡電話：03-5712121#52885、#31483、#52886

四、檢測範圍

針對網站健檢之網站進行弱點掃描，並涵蓋中英文版本網站。

五、檢測工具與方式

使用業界公認網站主機系統安全掃描軟體進行健檢網站之安全性測試。
※請勿自行進行網站主機系統相關測試，避免觸及本校資安防禦機制。

六、檢測項目

(一) 主機弱點檢測內容為主要探測主機狀態、網路埠狀態、作業系統類型、系統服務及應用程式類型等。

(二) 網站弱點掃描依據 OWASP TOP 10 項目進行檢測，檢測項目如下：

A1 Injection
A2 Broken Authentication
A3 Sensitive Data Exposure
A4 XML External Entities (XXE)
A5 Broken Access Control
A6 Security Misconfiguration
A7 Cross-Site Scripting (XSS)
A8 Insecure Deserialization

A9 Using Components with Known Vulnerabilities
A10 Insufficient Logging & Monitoring

七、影響範圍

執行弱點掃描時，並不會影響網站業務正常運作。

八、辦理方式

由網路系統組統一辦理執行弱點掃描檢測，初掃完成後將檢測結果通知網站管理單位，請網站負責人員於期限內進行弱點修補，修補完成後由網路系統組統一進行複掃作業。

九、檢測期程

(一)【網站資料備份】：為避免網站進行檢測作業時，造成網站資料變更，請網站負責人務必於 110 年 6 月 30 日(三)前完成網站資料備份作業。

(二)【第一次弱點掃描間】：110 年 7 月 1 日(四) 至 7 月 23 日(五)進行弱點掃描作業。

(三)【通知檢測結果】：於 110 年 7 月 30 日(五)前，以 E-Mail 方式通知各單位網站負責人員初步弱掃結果。

(四)【限期完成修補作業】：網站管理單位限期於 110 年 8 月 27 日(五)前將弱點處理報告單回覆網路系統組業務負責人。

(五)【第 2 次檢測掃描(複掃)】：為確認已排除風險或接受風險，進行複掃作業。

月/日 作業		6 月	7 月				8 月				9 月			
		~30	1~2	5~9	19~23	26~30	2~6	9~13	16~20	23~27	30~3	6~10	13~17	20~24
1	網站資料備份													
2	第一次弱點掃描													
3	通知檢測結果													
4	限期完成修補作業													
5	第 2 次檢測掃描													

十、修補作業

(一)高風險弱點修補，除有技術面合理說明或其他因應策略，並經單位主管確認者外，均應進行修補；中低風險若未完成修補，需自行評估風險後提報主辦單位。

(二)高風險弱點未完成修補期間，應每日自行檢查及確認網站運作狀況，並留存檢查及修補記錄。

(三)針對高風險弱點，各業務負責人應確實填寫弱點處理報告單，並由各單位

主管進行確認後，回覆至網路組弱點掃描業務負責人。

(四)本次檢測之各項網站弱點，將於下次進行弱點掃描時再次進行追蹤與確認。

附件二

國立陽明交通大學 資通防護基準作業程序

依據資通安全管理法之資通安全責任等級分級辦法訂定國立陽明交通大學資通系統防護基準作業程序，並依據系統普中高分級訂定等級之防護作業程序。

普級系統

	構面	措施	檢查內容
1.	存取控制	帳號管理	所有帳號之申請、開通、停用及刪除需透過電子郵件或書面向管理者提出申請，申請資料須至少留存 1 年。
		遠端存取	須依據使用者之連線需求給相應之權限，使用者權限檢查作業應於伺服器端完成。
2.	稽核與可歸責性	稽核事件	一、系統須建立稽核紀錄，並至少留存 3 個月。 二、稽核紀錄須包含以下項目： 1. 管理員帳號登入紀錄 2. 管理員帳號操作紀錄 3. 使用者身分驗證失敗紀錄
		稽核紀錄內容	稽核紀錄格式須具備一致性，並應包含下列資訊： 1. 事件類型 2. 事件發生時間 3. 事件相關之使用者身分識別等資訊(Ex：使用者帳號)
		稽核儲存容量	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。
		稽核處理失效之回應	資通系統於稽核處理失效時(Ex：儲存空間不足)，應採取適當之行動(Ex：覆寫較舊之稽核紀錄)。
		時戳及校時	系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。
		稽核資訊之保護	稽核紀錄僅允許系統管理員進行存取。
3.	營運持續計畫	系統備份	一、系統可容忍資料損失時間為 1 個月。 二、系統應每 1 個月執行系統與資料備份。
4.	鑑別與識別	內部使用者之識別與鑑別	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。

		身分驗證管理	一、使用預設密碼登入系統時，應於登入後要求立即變更。 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三次後，至少十五分鐘內不允許該帳號繼續嘗試登入。 四、使用者更換密碼時，至少不可以與前三次使用過之密碼相同，且每日僅允許變更密碼 1 次。 五、強制密碼最短為 8 碼且每 1 年需進行密碼變更。 六、若使用者非本校之教職員生，可不必強制密碼變更，但仍需建議使用者定期更換密碼。
		鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊(EX：以「登入失敗」取代「帳號不存在」、「密碼錯誤」)。
		非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。
5.	系統與服務獲得	系統發展生命週期需求階段	系統發展生命週期需求階段須執行下列需求： 針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。
		系統發展生命週期開發階段	系統發展生命週期開發階段須執行下列需求： 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、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	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、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二、資通系統相關軟體，不使用預設密碼。
		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。

		系統文件	應儲存與管理系統發展生命週期之相關文件。
6.	系統與資訊完整性	漏洞修復	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	發現資通系統有被入侵跡象時，應通報本校資訊技術服務中心。

中級系統

	構面	措施	檢查內容
1.	存取控制	帳號管理	一、所有帳號之申請、開通、停用及刪除需透過電子郵件或書面向管理者提出申請，申請資料須至少留存 1 年。 二、應每個月檢視刪除資通系統閒置帳號、已逾期之臨時或緊急帳號。
		最小權限	採最小權限原則，須依據使用者之連線需求給相應之權限，使用者權限檢查作業應於伺服器端完成。
		遠端存取	應監控資通系統遠端連線，所有遠端連線應採用加密機制，並需限制遠端連線之來源 IP。
2.	稽核與可歸責性	稽核事件	一、系統管理員需每個月檢視稽核紀錄。 二、系統須建立稽核紀錄，並至少留存 3 個月。 三、稽核紀錄須包含以下項目： 1. 管理員帳號登入紀錄 2. 管理員帳號操作紀錄 3. 使用者身分驗證失敗紀錄
		稽核紀錄內容	稽核紀錄格式須具備一致性，並應包含下列資訊： 1. 事件類型 2. 事件發生時間 3. 事件相關之使用者身分識別等資訊(Ex：使用者帳號)
		稽核儲存容量	依據稽核紀錄儲存需求，配置所需之儲存容量。
		稽核處理失效之回應	資通系統於稽核處理失效時(Ex：儲存空間不足)，應採取適當之行動(Ex：覆寫較舊之稽核紀錄)。
		時戳及校時	一、系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。 二、系統內部時鐘應每週與 ntp.nctu.edu.tw 進行同步。
		稽核資訊之保護	一、稽核紀錄僅允許系統管理員進行存取。 二、稽核紀錄應運用雜湊或其他適當方式之完整性確保機制。
4.	營運持續計畫	系統備份	一、系統可容忍資料損失時間為 1 個月。 二、系統應每 1 個月執行系統與資料備份，並測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。
		系統備援	系統從中斷後至重新恢復服務之可容忍時間為 1 天，原服務中斷時，於可容忍時間內，由備援設備取代提供服務。
5.	鑑別與識別	內部使用者之識別與鑑別	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。

		身分驗證管理	一、使用預設密碼登入系統時，應於登入後要求立即變更。 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 身分驗證失敗達三次後，至少十五分鐘內不允許該帳號 繼續嘗試登入。 四、強制密碼最短為 8 碼且每 1 年需進行密碼變更。 五、若使用者非本校之教職員生，可不必強制密碼變更，但仍需建議使用者定期更換密碼。 六、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 七、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。 八、使用者更換密碼時，至少不可以與前三次使用過之密碼相同，且每日僅允許變更密碼 1 次。
		鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊(EX：帳號不存在、密碼錯誤)。
		加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。
		非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。
6.	系統與服務獲得	系統發展生命週期需求階段	系統發展生命週期需求階段須執行下列需求： 針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。
		系統發展生命週期設計階段	系統發展生命週期設計階段須執行下列需求： 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。
		系統發展生命週期開發階段	系統發展生命週期開發階段須執行下列需求： 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、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	系統發展生命週期測試階段須執行下列需求： 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	系統發展生命週期部署與維運階段須執行下列需求： 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，並關閉不必要服務及埠口。 二、資通系統相關軟體，不使用預設密碼。

			三、於系統發展生命週期之維運階段，須注意版本控制與變更管理。
		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	開發、測試及正式作業環境應為區隔。
		系統文件	應儲存與管理系統發展生命週期之相關文件。
7.	系統與資訊完整性	漏洞修復	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、發現資通系統有被入侵跡象時，應通報本校資訊技術服務中心。 二、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。
		軟體及資訊完整性	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、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、發現違反完整性時，資通系統應實施適當之安全保護措施。(Ex：還原至符合完整性之備份、執行弱點掃描等)

高級系統

	構面	措施	檢查內容
1.	存取控制	帳號管理	一、所有帳號之申請、開通、停用及刪除需透過電子郵件或書面向管理者提出申請，申請資料須至少留存 1 年。 二、應每個月檢視刪除資通系統閒置帳號、已逾期之臨時或緊急帳號。 三、使用者閒置逾 1 小時後，系統應自動將使用者登出。 四、監控資通系統帳號，如發現帳號違常使用時回報管理者。
		最小權限	採最小權限原則，須依據使用者之連線需求給相應之權限，使用者權限檢查作業應於伺服器端完成。
		遠端存取	應監控資通系統遠端連線，所有遠端連線應採用加密機制，並需限制遠端連線之來源 IP。
2.	稽核與可歸責性	稽核事件	一、系統管理員需每個月檢視稽核紀錄。 二、系統須建立稽核紀錄，並至少留存 3 個月。 三、稽核紀錄須包含以下項目： 1. 管理員帳號登入紀錄 2. 管理員帳號操作紀錄 3. 使用者身分驗證失敗紀錄
		稽核紀錄內容	稽核紀錄格式須具備一致性，並應包含下列資訊： 1. 事件類型 2. 事件發生時間 3. 事件相關之使用者身分識別等資訊(Ex：使用者帳號)
		稽核儲存容量	依據稽核紀錄儲存需求，配置所需之儲存容量。
		稽核處理失效之回應	資通系統於稽核處理失效時(Ex：儲存空間不足)，應採取適當之行動(Ex：覆寫較舊之稽核紀錄)。
		時戳及校時	一、系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。 二、系統內部時鐘應每週與 ntp.nctu.edu.tw 進行同步。
		稽核資訊之保護	一、稽核紀錄僅允許系統管理員進行存取。 二、系統管理員需每個月檢視稽核紀錄。 三、稽核紀錄應運用雜湊或其他適當方式之完整性確保機制。 四、每個月備份稽核紀錄至與原稽核系統不同之實體系統。
4.	營運持續計畫	系統備份	一、系統可容忍資料損失時間為 1 個月。 二、系統應每 1 個月執行系統與資料備份，並測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 三、應將備份還原，作為營運持續計畫測試之一部分。

			四、應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。
		系統備援	系統從中斷後至重新恢復服務之可容忍時間為 1 天，原服務中斷時，於可容忍時間內，由備援設備取代提供服務。
5.	鑑別與識別	內部使用者之識別與鑑別	一、資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。 二、對帳號之網路或本機存取採取多重認證技術。
		身分驗證管理	一、使用預設密碼登入系統時，應於登入後要求立即變更。 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 身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入。 四、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 五、強制密碼最短為 8 碼且每半年需進行密碼變更。 六、若使用者非本校之教職員生，可不必強制密碼變更，但仍需建議使用者定期更換密碼。 七、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。 八、使用者更換密碼時，至少不可以與前三次使用過之密碼相同，且每日僅允許變更密碼 1 次。
		鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊(EX：以「登入失敗」取代「帳號不存在」、「密碼錯誤」)。
		加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。
		非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。
6.	系統與服務獲得	系統發展生命週期需求階段	系統發展生命週期需求階段須執行下列需求： 針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。
		系統發展生命週期設計階段	系統發展生命週期設計階段須執行下列需求： 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。
		系統發展生命週期開發階段	系統發展生命週期開發階段須執行下列需求： 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、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。 四、具備系統嚴重錯誤之通知機制。 五、執行「源碼掃描」安全檢測。
		系統發展生命週期測試階段	系統發展生命週期測試階段須執行下列需求： 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	系統發展生命週期部署與維運階段須執行下列需求： 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，並關閉不必要服務及埠口。 二、資通系統相關軟體，不使用預設密碼。 三、於系統發展生命週期之維運階段，須注意版本控制與變更管理。 四、執行「滲透測試」安全檢測。
		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	開發、測試及正式作業環境應為區隔。
		系統文件	應儲存與管理系統發展生命週期之相關文件。
7.	系統與通訊保護	傳輸之機密性與完整性	一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二、使用公開、國際機構驗證且未遭破解之演算法。 三、支援演算法最大長度金鑰。 四、加密金鑰或憑證週期性更換。 五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。
		資料儲存之安全	靜置資訊及相關具保護需求之機密資訊應加密儲存。
8.	系統與資訊完整性	漏洞修復	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、發現資通系統有被入侵跡象時，應通報本校資訊技術服務中心。 二、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。 三、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。
		軟體及資訊完整性	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、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、發現違反完整性時，資通系統應實施適當之安全保護措施。 (Ex：還原至符合完整性之備份、執行弱點掃描等)

			四、應定期執行軟體與資訊完整性檢查。