

國立陽明交通大學校園網站健檢工作計畫

為有效確保本校網站服務品質、推動網站雙語化、提升資訊安全，並提供單位於規劃、建置及維護管理本校網站服務時有所遵循，擬於 115 年 5 月 4 日至 5 月 18 日進行校園網站健檢。

一、適用範圍：本校行政單位、教學單位（學院及系所）、研究中心、附設醫院、附中之中、英文網頁。

二、健檢指標說明：

（一）網站維護及服務

1、有效連結

網站提供之連結，應確保其連結有效性。（本項推薦檢測工具為：Dr. Link Check，網址：<https://www.drlinkcheck.com/>）。

2、開放文件格式

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、無障礙網站 AA 認證標章

為配合數位發展部推動無障礙網站設計，對外服務網站應取得 AA 等級以上之無障礙認證標章。

4、網站名稱及 NYCU 域名使用：該年度首次納入網站健檢及更新域名的受檢單位網站，應加檢此項。

（1）網站名稱含本校校名及單位名稱。

（2）網站應使用本校網域名稱（nycu.edu.tw）。

（3）學校首頁要能正確連結到該網站之 NYCU 網站域名。

（4）網站內所有聯絡資訊應使用 NYCU Email。

（二）資訊安全

1、網站使用 HTTPS 加密連線

（1）安裝 SSL 憑證

（2）強制導入 HTTPS

（3）排除混合內容

2、網頁防護

配合教育部網站集中化政策，各單位網站負責人請於 115 年 3 月 2 日起至 4 月 30 日止，就網頁防護項目僅接受以下兩項（擇一）：

（1）網站須建置在本中心提供之網站建置平台且使用本中心之 WAF 服務，並於指定期限內於「電子表單系統」（網址：<https://tracko.nycu.edu.tw/>，請使用校園單一入口登入）提交 WAF 服務申請單；

（2）使用 Google Cloud Platform、Microsoft Azure、Amazon Web Services、中華電信 hicloud 等公有雲平台，須購買各該雲端平台提供的 WAF 服務，並於指定期限內提交前述公有雲平台之 WAF 服務使用證明給資安 WAF 業務負責人：劉晏辰先生，分機 52822，Email：

cielo33456@nycu.edu.tw。

3、弱點掃描

- (1) 請於 115 年 1 月 13 日前完成單位網站備份及白名單設定作業。
- (2) 115 年 2 月 26 日前請各單位網站負責人確認是否收到初次弱掃報告通知信，並自行至弱點掃描平台(<https://va.nycu.edu.tw>)下載所負責網站之弱點掃描報告進行改善修補。
若未收到初次弱掃報告通知件、未能下載弱掃報告…等有關弱掃相關問題(含使用平台問題)請依序接洽以下資安弱掃業務負責人：
許世平先生，分機：52856，Email：business255work@nycu.edu.tw。
廖期鈞先生，分機：52861，Email：lio221@nycu.edu.tw。
- (3) 各單位網站負責人於收到報告時起至 115 年 4 月 30 日止進行排除單位網站弱點，並自行至「弱點掃描平台」(網址：<https://va.nycu.edu.tw/>)進行複掃，請於 115 年 4 月 30 日前至「弱點掃描平台」完成填報中、高、重風險的漏洞處理方式等弱點處理結果，由資訊中心審核是否已排除中、高、重弱點。(詳細「網站健檢弱點檢測計畫」請參考附錄)

三、 審核：

- (一) 健檢指標全數符合者為「優良」。
- (二) 資訊安全指標全數符合，但尚有它項指標未符合者為「通過」。
- (三) 資訊安全指標內有一項未符合者為「待改善」，後續將由資訊技術服務中心列管並限期追蹤改善，未於期限內改善完成者將進行關閉網站直到改善完成。
- (四) 未於 115 年 4 月 22 日起至 115 年 4 月 30 日前完成單位網站自評填報者，資訊技術服務中心仍將進行健檢及彙報，但不給予誤評更正機會，對於優良及通過等級一律評為「條件式通過(未填報)」。

四、 注意事項：

- (一) 請至「網站健檢專區」內之受檢單位清冊(網址：<https://reurl.cc/K46Qyg>)確認自己單位網站的相關資訊(如：網站名稱、中英文網址、網站負責人等)是否正確？如需異動，請將相關資訊 Email 至 janice@nycu.edu.tw 信箱辦理變更。
- (二) 本年度網站健檢將分別舉辦以下 2 場線上說明會，請各單位網站負責務必參加：
 - 1、115 年 1 月 7 日上午 9:30「弱點掃描線上說明會」(直播連結：<https://meet.google.com/mqv-tcnp-efe>)。
 - 2、115 年 2 月 12 日上午 10:00「115 年度網站健檢說明會」：請於 115 年 2 月 5 日前完成線上報名(報名網址：<https://reurl.cc/bmp4ar>)。
- (三) 請各單位網站負責人於 115 年 4 月 22 日起至 4 月 30 日止登入「網站健檢自評填報系統」(網址：<https://ismsp.it.nycu.edu.tw/>，系統將於自評期間同步開放)完成單位網站健檢自評填報作業。
各單位網站負責人進行所屬網站自評填報作業時，請確認填報網站之中、英文網址是否與健檢專區受檢單位清冊一致，如有不一致請主動提出更正，也請同時更新學校首頁中、英文網；若有未一致情形，將以受檢單位清冊上的網址進行評分，單位不得嗣後提出異議並要求誤評更正。

- (四) 115 年 6 月通知健檢評分結果，僅提供誤評部份進行校正調分。
- (五) 115 年 7 月配合中心通知待改善單位限期改善網站缺失。

(一) 表 1 網站健檢指標及配分表

指標	次指標	摘要說明	審核結果 (中英文網皆需同時符合，才視為符合！！)
網 站 維 護 及 服 務	有效連結	網站提供之連結，應確保其連結有效性。(本項推薦檢測工具為：Dr. Link Check，網址： https://www.drlinkcheck.com/)。	符合／未符合
	開放文件格式	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。	符合／未符合
	無障礙 AA 認證標章	對外服務網站應取得 AA 等級以上之無障礙認證標章。	符合／未符合
	※網站名稱及 NYCU 域名使用	網站名稱含本校校名及單位名稱	不適用／符合／未符合
		網站應使用本校網域名稱 (nycu.edu.tw)。	不適用／符合／未符合
		學校首頁要能正確連結到該網站之 NYCU 網站域名	不適用／符合／未符合
		網站內所有聯絡資訊應使用 NYCU Email	不適用／符合／未符合
資 訊 安 全	網站使用 HTTPS 加密連線	安裝 SSL 憑證。	符合／未符合
		強制導入 HTTPS。	符合／未符合
		排除混合內容。	符合／未符合
	網頁防護	使用本中心之 WAF 服務並提交當年度 WAF 服務申請表或 GCP、Microsoft Azure、AWS、中華電信 hcloud 等四大公有雲平台提供的 WAF 服務並提供佐證資料。	符合／未符合
	弱點掃描	請至弱點掃描平台 (https://va.nycu.edu.tw) 下載平台上的弱點掃描報告進行改善修補，並在平台填寫中、高、重風險的漏洞處理方式，由資訊中心審核是否已排除中、高、重弱點。(詳細「網站健檢弱點檢測計畫」請參考附錄)	符合／未符合

註：※ 該年度首次納入網站健檢及更新域名的受檢單位網站，應加檢此項。

115 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 許世平、廖期鈞
E-MAIL: business255work@nycu.edu.tw、lio221@nycu.edu.tw
連絡電話：03-5712121#52856、#52861

四、檢測範圍

針對網頁評鑑之網站，包含行政單位、教學單位、研發中心、附設醫院網站主機進行弱點掃描，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評鑑網站之安全性測試。

※注意事項

1. 因網站弱掃工具掃描時，會產生一定的流量，建議在網站使用人數較少時進行掃描。
2. 檢測期間，請確保受測網站之防火牆將掃描機 140.113.27.150、140.113.27.151、140.113.27.152、140.113.27.153、140.113.27.134 與 140.113.27.234 設成白名單。

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 Broken Access Control
 - A2 Cryptographic Failures
 - A3 Injection
 - A4 Insecure Design
 - A5 Security Misconfiguration
 - A6 Vulnerable and Outdated Components

- A7 Identification and Authentication Failures
- A8 Software and Data Integrity Failures
- A9 Security Logging and Monitoring Failures
- A10 SSRF(Server-Side Request Forgery)

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

此次弱點檢測計畫皆會使用弱點掃描平台(<https://va.nycu.edu.tw/>)進行。初次弱點掃描由網路系統組統一進行，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登入弱點掃描平台下載報告並進行修補。

修補完成後，請單位自行於平台上操作重新掃描，確認漏洞是否正確修補。若有漏洞無法修復或存在誤判，請至平台填寫技術面合理說明或其他因應策略，網路系統組在收到回覆之後會對回覆內容進行審查，決定是否同意。

九、檢測期程

- (一) **【弱點掃描說明會】**：網路系統組將於 115 年 1 月 7 日(三) 上午 09:30 舉辦說明會，講解弱點掃描平台使用說明及常見弱點排除方向，請網站負責人務必參加。
- (二) **【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 115 年 1 月 13 日(二)前完成網站資料備份作業，並對掃描主機 IP 140.113.27.150、140.113.27.151、140.113.27.152、140.113.27.153、140.113.27.134 與 140.113.27.234 開設防火牆白名單。
- (三) **【初次弱點掃描期間】**：115 年 1 月 14 日(三) 至 2 月 26 日(四) 網路系統組將用弱點掃描平台統一對各單位網站進行弱掃作業。
- (四) **【通知檢測結果】**：於 115 年 3 月 2 日(一)前，以 E-Mail 方式通知各單位網站負責人員弱點掃描結果。
- (五) **【限期完成修補作業】**：網站管理單位收到通知後，自行於弱掃平台下載報告並修補漏洞，限期於 115 年 4 月 30 日(四)完成修補並審核通過。弱掃平台提供網站管理單位自行複掃確認漏洞是否修補完成。若有漏洞無法修復或存在誤判，請至平台填寫技術面合理說明狀況與其他因應策略，網路系統組在收到回覆之後會對回覆內容進行審查，決定是否同意。
- (六) **【審查給分標準】**：單位需確認弱掃平台上，修補計畫標示之中高重風險均已同意審核，若於 115 年 4 月 30 日(四)前有其中一項未通過審核，健檢之弱點掃描項目將不允給分。

十、修補作業

- (一) 中高重風險弱點修補，除有技術面合理說明或其他因應策略，經單位主管確認者後填報

至系統，均應進行修補；低風險若未完成修補，需自行評估風險是否修補。

- (二) 中高重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) 針對中高重風險弱點，各業務負責人應確實登入平台下載報告後修補，並於修補後重新掃描，直至無中高重風險弱點。
- (四) 檢測期間，請確保受測網站之防火牆將掃描機 IP 140.113.27.150、140.113.27.151、140.113.27.152、140.113.27.153、140.113.27.134 與 140.113.27.234 設成白名單。
- (五) 若對風險排除有問題請於說明會上提出，後續若對風險排除有問題，請依照流程填寫資訊服務申請單至資訊中心櫃台，將由承辦人回覆處理。