超文字安全傳輸通訊協定(HTTPS)

什麼是HTTPS

- 超文字安全傳輸通訊協定 HTTPS（HyperText Transfer Protocol Secure）
  - 是HTTP的安全版本， 而HTTP 是用於在 Web 瀏覽器和網站之間傳送資料的主要通訊協定， HTTPS 則經過加密，以提高資料傳輸的安全性。
- HTTPS 使用的加密技術
  - 目前 HTTPS 採用的加密通訊協定為傳輸層安全性協定（Transport Layer Security, TLS）。
- 安全性與效益
  - 有效防範常見的網路攻擊，例如封包擷取（Packet Sniffing）與中間人攻擊（Man-in-the-Middle Attack）。
  - 符合法規規定與資安標準。
  - 提升資料傳輸過程中的安全性， 保護資料的完整性與機密性。

政策

1. 依行政院國家資通安全會報第31次委員會議決議，持續辦理網站導入安全傳輸協定(HTTPS)
   - 教育部 107年3月21日臺教資(五)第1070041450號函及108年10月24日臺教資(五)字第1080154973號函辦理。
2. 臺灣學術網路管理規範第七點第六項，法規
   - 訂定單位所提供各式網路應用服務之相關管理辦法，且對外提供服務之 資通系統應採加密機制，並使用公開、國際機構驗證且未遭破解之演算法。另對內提供服務之資通系統如未使用加密傳輸機制，應採實體隔離措施。
3. 根據ISMS，NDHU-I-B-08_通訊安全管理程序書，網路之資通管理
   - 敏感等級以上之業務資料或文件不得存放於對外開放之資通系統中，若因特殊業務功能之需求，必須採取加強之安全管控機制，如：資料加密等。
   - 對外開放的資通系統所提供之網路服務，如：HTTPS、FTP等，應採取適當之存取控管機制。
   - 對外開放之資通系統，如存放個人資料檔案，其傳輸過程應考量以加密方式處理，並妥善保管資料，防止被竊取或移作他途之用，以致侵犯個人隱私。

憑證導入必要項目說明

1. 各單位官網應導入HTTPS並自動轉址為HTTPS。
   - 加密後的網站，會採SSL/TLS來傳送加密封包，如瀏覽HTTPS網站時，瀏覽器會出現安全(Secure)，並且網址是以https://開頭。
2. 網站應設定為TLS1.2以上的協議，應關閉 TLS1.0、TLS1.1、SSLv2、SSLv3。
   - TLS 檢測
3. 對校外提供網頁服務應導入安全性憑證(SSL)，且憑證申請需事先申請網域名稱(Domain name)。
4. 有套用網域名稱的服務提供者，應設定IP自動轉址Domain。
5. 委外建置之網站應在招標規格中，規範廠商需安裝SSL憑證，並導入HTTPS。
   - HTTP SSL檢測

常見付費、免費憑證及設定參考

- 付費憑證
  - 台灣網路認證公司(TWCA)
  - DigiCert
  - Certum
- 免費憑證
  - Linux (Ubuntu)
    - Let‘s Encrypt 官網 (憑證有效期限為90天，每90天需續期一次)
    - 在Ubuntu系統上的Apache：How To Secure Apache with Let's Encrypt on Ubuntu
    - 在Ubuntu系統上的Nginx：How To Secure Nginx with Let's Encrypt on Ubuntu
  - Windows
    - Let‘s Encrypt 官網 (憑證有效期限為90天，每90天需續期一次)
    - 免費 Let’s Encrypt SSL 自動更新憑證，自架 IIS 站台適用
    - Install Let’s Encrypt with IIS on Windows Server 2019