資訊安全宣導教育訓練

資訊技術服務中心

111年

目錄

資安法規及政策

- 校園網路使用規範
- 資通系統安全管理規範
- 資安法其他配合事項
- 資通系統委外注意事項

校園網路使用規範

1. 避免侵害智慧財產權
2. 避免惡意使用網路資源
3. 資安事件通報及處理
4. 網路違規使用處分
5. 其餘網路使用注意事項

校園網路使用規範

- 110年6月2日於行政會議通過後實施
- 參考：https://it.nycu.edu.tw/about-us/services-regulations/

1.避免侵害智慧財產權

- 使用校園網路時應避免下列可能涉及侵害智慧財產權之行為：
  - **違法下載**、**拷貝**受著作權法保護之著作。
  - **未經**著作權人之**同意**，將受保護之著作上傳於公開之網站上。
  - BBS、社群媒體或其他線上討論區上之文章，經**作者明示禁止轉載**，而仍然任意轉載。
  - 架設網站供公眾違法下載受保護之著作。
  - 其他可能涉及侵害智慧財產權之行為。

2.避免惡意使用網路資源1/2

- 使用校園網路時應**避免**下列濫用網路資源之行為：
  - **散布電腦病毒**或其他干擾或破壞系統機能之程式。
  - 擅自截取網路傳輸訊息。
  - 以**破解**、**盜用**或**冒用他人帳號**及**密碼**等方式，未經授權使用網路資源。
  - 無故將帳號借予他人使用，或無故洩漏他人之帳號及密碼。
  - 隱藏帳號或使用虛假帳號。但經明確授權得匿名使用者不在此限。
  - **窺視**他人之電子郵件或相關電腦資訊。

2.避免惡意使用網路資源2/2

- 以任何方式**濫用網路資源**，包括以電子郵件大量傳送廣告信、連鎖信或無用之信息，或以灌爆信箱、掠奪資源等方式，影響系統之正常運作。
- 以電子郵件、線上談話、電子佈告欄（BBS）或類似功能之方法散布詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息。
- 利用校園網路資源**從事**非教學研究等相關之活動或**違法行為**。
- **洩漏公務機敏**資料。

3.資安事件通報及處理

- 網路使用者應隨時留意任何疑似資安問題，以確保網路使用安全。舉凡經教育機構資安通報平台及正式函文提報之資安事件處理原則如下：
  - 經教育機構資安通報平台提報之 IP，經查證屬實，**第一次違反資安規範較輕者**，**封鎖 IP 位址兩週**；**違反情節較重或再犯者**，**封鎖 IP 位址一個月**，並依本校獎懲規定處分。
  - 檢警正式來文，因校方無檢調權，若查案有此需求，應請檢警人員提出搜索票，校方方能全力配合調查。

4.網路違規使用處分1/2

- 對於網路違規使用者依下列情況處理：
  - 對網路使用有**立即性影響**或**威脅者**，**立即阻斷**異常主機之網路連線，另**通知所屬單位的網路管理人員**及**單位主管**，該使用者或所屬單位網路管理人員需於一週內將處理情形回覆資訊中心，經確認解決問題後，再由資訊中心管理人員解除網路封鎖。
  - 對網路使用無立即性影響或威脅者，通知該使用者或所屬單位之網路管理人員。網路管理人員於接獲通知**三日內**須完成通知事項的查證、輔導改善或處置，並將處理情形回覆資訊中心，未於三日內回覆處理情形時，資訊中心得阻斷異常主機之網路連線。

4.網路違規使用處分2/2

- 網路使用者違反本規範者，將受到下列處分：
  - 暫時停止使用網路資源(**封鎖 IP 一週**)。
  - 若情節嚴重者，延長暫時停止使用網路資源時間，並依校規及相關獎懲辦法查處。
  - 依前兩項規定之處分者，其另有**違反法令行為**時，行為人尚應依民法、刑法、著作權法或其他相關法令，**自負法律責任**。

5.其餘網路使用注意事項

- 對於無故佔用大量網路資源或流量異常者，致**影響網路正常運作者**，管理單位得以**採用流量管制**或**暫停該使用者之權利**。經確認恢復正常狀態，始恢復其網路連線。

- 使用者若發現系統安全有任何缺陷或漏洞，應儘速通知管理單位處理。

- 校園網路原則**禁止使用 P2P 軟體**，若因學術、教學及其他特殊需求，可提出申請。但若使用 P2P 軟體而影響校園網路服務，將逕行封鎖。

資通系統安全管理規範

1. 資通系統管理要求
2. 資通系統委外要求

資通系統安全管理規範

- 110年6月2日於行政會議通過實施，並於111年9月14日行政會議修訂通過。
- 參考：https://it.nycu.edu.tw/about-us/services-regulations/

1.資通系統管理要求

- 各單位自行開發公務資通系統須提供系統開發安全之文件與弱點掃描報告，交付本校資訊技術服務中心（以下簡稱資訊中心）。經確認無高、中風險者始可正式啟用；若審查不合格，資訊中心將提供弱點驗證結果，通知系統管理單位限期改善。

- 各單位**應定期盤點**自行或委外開發之資通系統，依據資通安全管理法之資通安全責任等級分級辦法的分級原則與防護基準確實落實執行。

- 各單位管理之重要資通系統，須以防火牆或其他安全設施防護，控管外界與內部網路之資料傳輸及存取，防止被侵入破壞、竄改、刪除及未經授權之存取，並應定期確認防火牆管控政策之適用性。

2.資通系統委外要求1/3

- 各單位委外開發資通系統時，應依「資通安全管理法施行細則」第四條第一項第二款：**要求廠商應配置**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**。

- 各單位委外開發資通系統時，應於RFP加註「**資安需求**」
  - 本專案之系統開發或維運，廠商必須依據本校對該系統訂定等級(**普/中/高**)，完成「資通安全責任等級分級辦法」附表十「**資通系統防護基準**」之該等級全部適用項目要求。
  - 本專案之受託廠商必須於服務建議書提出時附上「廠商資安管理作業自我評估表」

2.資通系統委外要求2/3

- 各單位委外開發資通系統時，應於事前審慎評估可能的潛在安全風險，並**與廠商簽訂**適當的資訊安全協定，確實遵守本校對資訊相關服務之安全要求及應負的責任，相關內容請參照「**委外服務資訊安全責任契約附加條款**」。

- **委外期間**應適當**控管委外人員之資通系統使用權限**；**委外結束**後，應**立即收回**該項權限。

2.資通系統委外要求3/3

- 委外廠商進行遠端維護資通系統，應採「**原則禁止、例外允許**」方式辦理(參考行政院資通安全處110年3月2日院臺護字第1100165761號函)，開放遠端存取期間原則以短天期為限，連線控制應由主機管理員從主機端或VPN進行管控，並填寫「委外廠商連線紀錄表」紀錄廠商之連線時間、用途說明，作業完畢應即關閉連線；並應定期送權責主管審查。

資安法其他配合事項

資安法其他配合事項

- 使用中之**中國廠牌資通訊產品**(含網路設備、電子看板、跑馬燈、門禁監控、監視器等)，因存有潛在的資安風險，請**儘速規劃替代方案或汰換**。

- 各單位應依據資通安全管理法之要求，配合資訊中心推動於個人電腦安裝**政府組態基準(GCB)**之設定。

- 為落實資安管理政策，資訊中心將訂定週期性稽核計畫，請各單位配合資訊中心之資安稽核作業。

資通系統委外採購注意事項

資通系統委外採購注意事項

- 依據資通系統安全管理規範要求廠商。
  - 將附件一、委外服務資訊安全責任契約附加條款加入採購契約
  - 與廠商簽訂保密協定
  - 與廠商人員簽訂保密切結書

- 資通系統委外若涉及個資處理
  - 須要求廠商簽訂個人資料委外監督條款範本，請依據委外內容調整
  - 委外結束時，須要求廠商簽訂個人資料歸還與銷毀切結書

PS.檔案請下載使用，雲端編輯格式會跑掉