張貼日期：2022/04/07

【資安訊息】請各單位全面盤點含有個人資料之系統，並遵守資通系統防護基準規範。

- 主旨說明：請各單位全面盤點含有個人資料之系統，並遵守資通系統防護基準規範。

- 內容說明：
  - 為防範各單位於系統開發與維護過程產生疏漏，導致個資外洩之資安事件發生，籲請各校積極落實系統開發之維護管理作業，並應遵守安全軟體開發生命週期(SSDLC)與符合資通系統防護基準規範。
- 影響平台:
  N/A
- 建議措施:
  1. 應全面性盤點含有個人資料之系統，檢視儲存個人資料之適法性與必要性，並納入資訊安全管理制度(ISMS)
  2. 應落實核心系統資產盤點、帳號清查及定期進行備份作業，如有變更需即時更新ISMS相關文件。
  3. 在進行系統開發與維護時須遵守「資通安全責任等級分級辦法」之「附表十資通系統防護基準」規範，提供適當之資安防護措施。
  4. 在系統發展生命週期之「開發階段」應執行「源碼掃描」安全檢測。針對安全需求實作必要控制措施。應注意避免軟體常見漏洞及實作必要控制措施。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。
  5. 在系統發展生命週期之「測試階段」應執行「弱點掃描」與「滲透測試」安全檢測，並於系統上線前完成弱點修補。在確認無中、高風險弱點後方可上線。
  6. 在系統發展生命週期之「部署與維運階段」應執行版本控制與變更管理。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。所開發資通系統不使用預設密碼。
  7. 在維護系統時如需更新系統版本，應確認所更新程式是否為正確上架版本，避免因上架錯誤版本造成機敏資料外洩風險。建議採用雙人複核機制，確認版本無誤後再進行上架作業。
  8. 在系統發展生命週期之「委外階段」若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。
  9. 各單位之資通系統應每年度進行滲透測試，檢測項目應包含系統弱點分析、網站弱點分析OWASP Top 10 檢測、人工邏輯檢測等作業，並且應強化人工邏輯檢測作業項目。滲透測試需經初、複掃雙重驗證方式來確認弱點修補品質，並透過專家指導快速排除已知之風險與問題。
- 參考資料:
  - 「資通安全責任等級分級辦法」之附表十資通系統防護基準.pdf
    https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030304

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20220407_02

Last update: **2022/04/07 09:30**