本(110)年教育體系重大資安事件相關根因分析及建議措施

項次	重大資安事件相關根因	建議措施
1	**弱密碼**及身分驗證缺失 • 案例：本部某機關委託某大學辦理X系統，X系統管理人員使用弱密碼，該弱點遭利用致管理人員帳號遭未授權登入，洩漏多筆個人資料。	一、依資通安全責任等級分級辦法第11條規定（附表十資通系統防護基準），資通系統應依其防護需求等級，落實身分驗證管理措施內容之相關要求。 二、資通系統使用密碼進行驗證時，應強制最低密碼複雜度。**密碼複雜度規範對象，應包含所有具管理權限之帳號。密碼複雜度檢查程序，應被納入所有密碼變更功能。** 三、機關宜訂定密碼複雜度共通規範，如**禁止使用與帳號名稱相同、身分證字號、學校/機關代碼、易猜測之弱密碼或其他公開資訊等**。 四、弱密碼及身分驗證缺失問題，建議納入機關安全性檢測項目。 五、針對管理人員因設置弱密碼導致資通安全事件，建議評估予以懲處。
2	未落實**安全軟體發展生命週期**相關要求（SSDLC） • 案例A：某學術單位未落實SSDLC相關要求，忘記密碼功能具有未發現之安全邏輯漏洞，致帳號遭未授權登入，洩漏多筆個人資料。 • 案例B：某大學X系統因應疫情變化緊急上線，未經適當安全性測試程序，存在安全弱點致個資可被他人不當存取。	一、依資通安全責任等級分級辦法第11條規定（附表十資通系統防護基準），資通系統應依其防護需求等級，落實系統與服務獲得構面之相關要求，針對資通系統發展生命週期各階段，完成各項安全要求。如委外辦理，應將相關安全需求明定於委外契約。 二、**資通系統於上線前之測試階段，應進行弱點掃描安全檢測**，並進行中、高風險弱點修補。如因應業務需求緊急上線，仍應保留安全性測試所需時間，避免因重大安全漏洞導致機關嚴重損失。 三、**應針對系統重要功能建立安全檢核機制**，如忘記密碼功能，並於測試階段完成安全測試。
3	重要**資料庫未最小授權** • 案例：某大學重要資料庫提供系統介接功能，惟介接作業未確保最小授權，X系統防護等級較低但具備介接完整資料表權限，致系統被入侵後即取得高權限，洩漏多筆個人資料。	一、依資通安全責任等級分級辦法第11條規定（附表十資通系統防護基準），資通系統存取控制應採最小權限原則。 二、機關應建立系統介接作業之權限審核機制。**重要資料庫應以最小權限原則進行存取授權**，依介接系統之業務功能，提供所需資料表及資料欄位。

本(110)年教育體系重大資安事件相關根因分析及建議措施

項次	重大資安事件相關根因	建議措施
4	人員**未經適當資安教育訓練**或資安職能不足 • 案例：某學校人員個資保護意識不足，將具敏感資訊之個人資料張貼於公開網路。	一、依資通安全責任等級分級辦法第 11 條規定（附表一至八機關應辦事項），機關、學校人員應依所屬人員類型（一般使用者及主管、資通安全專職人員、資通安全專職人員以外之資訊人員）完成對應之資通安全教育訓練法定時數要求。 二、各單位主管應積極督促所轄人員完成資通安全教育訓練，建議由專責單位（如人事單位）定期追蹤管考以確保成效。
5	學校**資安規範適用範圍**未包含重要資通系統 • 案例：某大學負責管理重要資通系統之單位，未納入學校資訊安全管理制度(ISMS)適用範圍，相關系統開發測試流程未有適當規範遵循，因管理不當導致資安事件。	一、依資通安全管理法第 10 條規定，公務機關應訂定資通安全維護計畫，內容包括資訊及資通系統之盤點、資通安全風險評估、資通安全防護及控制措施等項目。 二、學校資通系統之盤點，應包含行政單位、教學研究單位自行或委外開發之資通系統。**學校資通安全防護及控制措施相關規範，即應涵蓋全校前揭資通系統**，並依風險評估結果針對重要資通系統予以適當保護。