

教育部 函

地址：10051 臺北市中山南路5號
承辦人：陳建麒
電話：02-7712-9119
電子信箱：alex@mail.moe.gov.tw

受文者：國立臺灣藝術大學

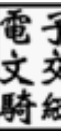
發文日期：中華民國110年9月22日
發文字號：臺教資(四)字第1100128345號
速別：普通件
密等及解密條件或保密期限：
附件：無附件

主旨：為降低資安風險，請各校落實資通系統及資訊之盤點，並進行應有資通安全防護及控制措施，請查照。

說明：

一、近期學校經外界通報多起漏洞情資，如資通系統存取控制失當或存在重大漏洞，並經確認為資安事件，為避免敏感資訊外洩，保障教職員生權益，請各校應依資通安全管理法及其子法各項規範要求辦理安全防護及控制措施，包含下列項目：

- (一)依資通安全管理法施行細則第6條第1項第6款規定，落實全校資通系統及資訊之盤點，資通系統盤點範圍至少包含行政、教學單位自行或委外開發之資通系統，以及學校採購及公務使用之物聯網設備（如網路印表機、網路攝影機、門禁設備、環控系統、無線網路基地台、無線路由器等）。
- (二)依資通安全管理法施行細則第6條第1項第7款及第8款規定，落實全校資通安全風險評估、資通安全防護及控制措施。針對前開盤點之資通系統清單，應檢核不得使用



弱密碼、廠商預設密碼，並符合規範之密碼複雜度要求，以及依業務需求設定適當網路存取限制。

(三)依資通安全責任等級分級辦法附表十有關漏洞修補規定，資通系統避免軟體常見漏洞（如Injection、XSS等OWASP Top 10安全弱點），落實漏洞修復並定期更新。

二、未依前述規定辦理，致使學校發生資安事件，情節重大者，學校應依「公務機關所屬人員資通安全事項獎懲辦法」規定予以懲處。

正本：各國立大專校院

副本： 2021/09/22 15:24:40 電子公文交換



裝

訂



線

附表十 資通系統防護基準修正規定

系統防護需求 分級		高	中	普
控制措施				
構面	措施內容			
存取控制	帳號管理	<p>一、機關應定義各系統之間置時間或可使用期限與資通系統之使用情況及條件。</p> <p>二、逾越機關所許可之間置時間或可使用期限時，系統應自動將使用者登出。</p> <p>三、應依機關規定之情況及條件，使用資通系統。</p> <p>四、監控資通系統帳號，如發現帳號違常使用時回報管理者。</p> <p>五、等級「中」之所有控制措施。</p>	<p>一、已逾期之臨時或緊急帳號應刪除或禁用。</p> <p>二、資通系統間置帳號應禁用。</p> <p>三、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。</p> <p>四、等級「普」之所有控制措施。</p>	<p>建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。</p>
	最小權限	<p>採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。</p>		<p>無要求。</p>
	遠端存取	<p>一、遠端存取之來源應為機關已預先定義及管理之存取控制點。</p> <p>二、等級「普」之所有控制措施。</p>	<p>一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。</p> <p>二、使用者之權限檢查作業應於</p>	

			<p>伺服器端完成。</p> <p>三、應監控遠端存取機關內部網段或資通系統後臺之連線。</p> <p>四、應採用加密機制。</p>
事件日誌與可歸責性	記錄事件	<p>一、應定期審查機關所保留資通系統產生之日誌。</p> <p>二、等級「普」之所有控制措施。</p>	<p>一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。</p> <p>二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。</p> <p>三、應記錄資通系統管理者帳號所執行之各項功能。</p>
	日誌紀錄內容	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	
	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。	
	日誌處理失效之回應	<p>一、機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。</p> <p>二、等級「中」及「普」之所有控制措施。</p>	資通系統於日誌處理失效時，應採取適當之行動。
	時戳及校時	<p>一、系統內部時鐘應定期與基準時間源進行同步。</p> <p>二、等級「普」之所有控制措施。</p>	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調

			時間(UTC)或格林威治標準時間(GMT)。
	日誌資訊之保護	<p>一、定期備份日誌至原系統外之其他實體系統。</p> <p>二、等級「中」之所有控制措施。</p>	<p>一、應運用雜湊或其他適當方式之完整性確保機制。</p> <p>二、等級「普」之所有控制措施。</p>
營運持續計畫	系統備份	<p>一、應將備份還原，作為營運持續計畫測試之一部分。</p> <p>二、應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。</p> <p>三、等級「中」之所有控制措施。</p>	<p>一、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。</p> <p>二、等級「普」之所有控制措施。</p>
	系統備援	<p>一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。</p> <p>二、原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。</p>	<p>一、訂定系統可容忍資料損失之時間要求。</p> <p>二、執行系統源碼與資料備份。</p>
識別與鑑別	內部使用者之識別與鑑別	<p>一、對資通系統之存取採取多重認證技術。</p> <p>二、等級「中」及「普」之所有控制措施。</p>	<p>資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。</p>
	身分驗證管理	<p>一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。</p> <p>二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。</p> <p>三、等級「普」之所有控制措施。</p>	<p>一、使用預設密碼登入系統時，應於登入後要求立即變更。</p> <p>二、身分驗證相關資訊不以明文傳輸。</p> <p>三、具備帳戶鎖定</p>

			<p>機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。</p> <p>四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。</p> <p>五、密碼變更時，至少不可以與前三次使用過之密碼相同。</p> <p>六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。</p>
	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。	
	加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	無要求。
	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	
系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求(含機密性、可用性、完整性)進行確認。	
	系統發展生命週期設計階段	<p>一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。</p> <p>二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。</p>	無要求。
	系統發展生命週期開	一、執行「源碼掃描」安全檢測。	<p>一、應針對安全需求實作必要控制措施。</p> <p>二、應注意避免軟體常見漏洞及實作必</p>

	發階段	<p>二、系統應具備發生嚴重錯誤時之通知機制。</p> <p>三、等級「中」及「普」之所有控制措施。</p>	<p>要控制措施。</p> <p>三、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。</p>	
	系統發展生命週期測試階段	<p>一、執行「滲透測試」安全檢測。</p> <p>二、等級「中」及「普」之所有控制措施。</p>	執行「弱點掃描」安全檢測。	
	系統發展生命週期部署與維運階段	<p>一、於系統發展生命週期之維運階段，應執行版本控制與變更管理。</p> <p>二、等級「普」之所有控制措施。</p>	<p>一、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。</p> <p>二、資通系統不使用預設密碼。</p>	
	系統發展生命週期委外階段	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。		
	獲得程序	開發、測試及正式作業環境應為區隔。	無要求。	
	系統文件	應儲存與管理系統發展生命週期之相關文件。		
系統與通訊保護	傳輸之機密性與完整性	<p>一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。</p> <p>二、使用公開、國際機構驗證且未遭破解之演算法。</p> <p>三、支援演算法最大</p>	無要求。	無要求。

		<p>長度金鑰。</p> <p>四、加密金鑰或憑證應定期更換。</p> <p>五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。</p>		
	資料儲存之安全	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	無要求。	無要求。
系統與資訊完整性	漏洞修復	<p>一、定期確認資通系統相關漏洞修復之狀態。</p> <p>二、等級「普」之所有控制措施。</p>		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
	資通系統監控	<p>一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。</p> <p>二、等級「中」之所有控制措施。</p>	<p>一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授权使用。</p> <p>二、等級「普」之所有控制措施。</p>	發現資通系統有被入侵跡象時，應通報機關特定人員。
	軟體及資訊完整性	<p>一、應定期執行軟體與資訊完整性檢查。</p> <p>二、等級「中」之所有控制措施。</p>	<p>一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。</p> <p>二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。</p> <p>三、發現違反完整性時，資通系統應實施機關指定之安全保護措施。</p>	無要求。

備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之系統防護基準。