國立新化高級中學

存取控制管理

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1 目的

為保護資訊資產，降低未經授權存取系統之風險，以達成國立新化高級中學（以下簡稱「本校」）安全控管之目的。

2 適用範圍

本校資訊資產之存取控管原則。

3 權責

本校相關人員、約聘（僱）人員與委外人員：遵守本程序書之相關規定，以確保本校相關軟體與資料等資訊資產之安全。

4 名詞定義

無。

5 作業說明

5.1 存取控制政策

5.1.1 資訊資產之存取應與本身業務相關之範圍為主，任何人未經授權不得存取業務範圍外之資訊資產。

5.1.2 應正確地使用資訊資產，以維護資訊資產之可用性、完整性與機密性。

5.1.3 非因業務需求不得將系統存取帳號提供給外部人員，若因業務需要開放帳號予外部人員，應有適當安全控管措施，該安全控管措施應考量業務需求及資訊資產之機密性，授與適當之存取權限及有效日期。

5.1.4 被賦予系統管理最高權限之人員、掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

5.1.5 因處理系統當機與異常狀況需視狀況授與適當存取權限，並避免共用帳號。

5.1.6 可攜式電腦儲存媒體，例如：筆記型電腦、隨身碟、外接式硬碟、

光碟、磁帶等，應採取適當之控管措施，以防止未經授權之資料、系統、網路存取或病毒傳播。

5.1.7 資料、資訊之存取，必須符合「個人資料保護法」、「電子簽章法」及「智慧財產權」等相關法規、法令之規定，或契約對資料保護及資料存取使用控管之規定。

5.1.8 系統主機之公用程式路徑之存取權限應適當控管，禁止一般使用者存取。

5.1.9 針對無人看管的資訊資產設備，應有適當控管程序，以防未經授權之存取或濫用。

5.1.10 個人桌上型電腦、可攜式電腦應設定於一定時間不使用或離開後，應自動清除螢幕上的資訊並登出或鎖定系統，以避免被未經授權之存取。

5.2 帳號與密碼管理

5.2.1 新購置之應用軟體或系統，安裝完成後應立即更新預設之密碼，並刪除或關閉不必要之帳號。

5.2.2 使用者帳號管理

5.2.2.1 使用者帳號申請應填寫「資訊服務申請表」，經部門主管核准後，由帳號管理人員進行使用者帳號建立作業。

5.2.3 管理者帳號管理

5.2.3.1 系統管理者應避免共用系統管理者帳號，系統管理者帳號與密碼應存放於安全之處。

5.2.3.2 系統管理者密碼設置，至少 8 碼，且應符合密碼設置原則。

5.2.4 密碼管理

5.2.4.1 使用者首次使用系統時，應要求更改密碼設定，並妥善保管帳號與維持密碼之機密性，保存帳號密碼之檔案應以加密方式處理。

5.2.4.2 使用者應避免將帳號密碼記錄在書面上，張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。

5.2.4.3 使用者禁止共用帳號密碼。

5.2.4.4 使用者發現密碼可能遭破解時，應立即更改密碼。

5.2.4.5 使用者每次存取系統時應輸入密碼登入系統，避免使用記錄密碼功能，導致開機時自動登入系統。

5.2.4.6 資訊資產價值為 4 以上之資訊系統，系統管理者應至少 3 個月更換密碼一次，學籍系統之使用者(學校行政人員)應至少 6 個月更換密碼一次，並禁止重複使用相同的密碼。

5.2.4.7 使用者密碼設置至少 8 碼，且應符合密碼設置原則。

5.2.4.8 密碼設置原則

應儘量避免使用易猜測或公開資訊為設定，例如：

A. 個人姓名、出生年月日、身分證字號

B. 機關、單位名稱或其他相關事項

C. 使用者 ID、其他系統 ID

D. 電腦主機名稱、作業系統名稱

E. 電話號碼

F. 空白

密碼設定可考慮下列原則：

A. 參雜數字、英文字母、特殊符號、大小寫

B. 特殊意義詞彙

5.2.4.9 使用者遺忘密碼時，須填具「資訊服務申請表」，經部門主管核准後，由帳號管理人員重新設定。

5.3 使用者存取管理

5.3.1 各項系統資源使用權限之申請、註冊及註銷應遵循作業管理程序，並維護相關之申請、註冊、註銷資料與紀錄，以備查核。

5.3.2 使用者職務異動或離職時，部門主管應即時通知相關單位調整或終止使用者之存取權限。

5.3.3 特殊權限之使用者必須與一般權限之使用者區分管理；針對特殊權限帳號，應妥善管理。

5.3.4 特殊權限之授權管理，必須依執行業務系統別之需求，例如作業系統、資料庫管理系統、網路服務系統、監控管理系統等賦予系統存取特殊權限的授權，且以執行業務及職務所必要的最低資源存取授權為限。

5.3.5 系統相關作業人員需經正式授權存取業務相關之資訊資產，其識別資料與帳號必須為唯一，禁止借用他人之帳號或共用帳號。

5.3.6 各項設備與系統相關之使用權限（例如使用者帳戶與作業權限）應留存紀錄。

5.3.7 應妥善管理久未登錄系統之帳戶，若超過 6 個月未曾登錄，則視需要清除閒置帳號。

5.3.8 應要求使用者變更初始密碼並定期變更密碼；重要資訊系統及特殊權限之存取帳號之密碼變更期間應較一般權限之帳號頻繁。

5.3.9 使用者存取權限應定期審查，週期不得超過 6 個月。

5.3.10 重要系統稽核資料應由專人定期審核，系統管理者不得新增、刪除或修改稽核資料，審查週期不得超過 6 個月。

5.3.11 每半年將學籍系統、主機、網路設備等帳號權限設定資料印出，或填寫於「帳號清查紀錄表」，進行帳號權限清查，並將查核結果記錄於「帳號清查結果報告」呈資訊安全官審查。

5.4 作業系統存取控制

5.4.1 系統設定應避免於終端機登入程序中以明碼方式顯示密碼相關資訊。

5.4.2 只有在完成所有的登入資料輸入後，系統才開始查驗登入資訊的正

確性；若登入發生錯誤，系統不應顯示錯誤發生之原因。

5.4.3 在系統登入被拒絕後，應立即中斷登入程序，並不得給予任何的協助。

5.4.4 應設定系統登入程序之時間限制，如果超出時間限制，系統將自動中斷登入。

5.4.5 使用者帳號避免顯示任何足以辨識使用者特別權限的訊息，例如：顯示其為管理者或監督者。

5.4.6 系統管理人員結束系統維護作業後，應結束應用系統及網路連線，清除螢幕上的資訊，登出系統，並鎖定主控台螢幕。

5.4.7 系統之存取使用應留存查核紀錄。

5.5 應用系統之存取控制

5.5.1 資訊存取之限制

5.5.1.1 應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制。例如：新增、刪除或執行等。

5.5.1.2 應用系統之敏感與機密性資訊，應與一般資訊作適當區隔，並加強權限控管措施。

5.5.2 原始程式資源之存取控制

5.5.2.1 應用程式原始碼，應集中存放，並由系統負責人管理程式之增修作業。

5.5.2.2 開發中之原始程式碼，應與線上程式碼分開放置與控管。

5.5.2.3 舊版的原始程式應妥慎保管，並詳細記錄使用的明確時間，以備新版失敗回復使用。

5.5.2.4 應用程式之異動需經適當控管。

5.5.2.5 應用程式管理人員，應檢視程式目錄清單，如有異常情形，應即查明原因及處理。

5.6 網路存取控制

5.6.1 網路系統應依其性質之不同，分開成不同的領域，各領域應以特定的安全設施（如防火牆及網路閘門）加以保護，以降低可能的安全風險。

5.6.2 網路管理人員應定期檢視網路存取之紀錄，並留存查核紀錄。

5.6.3 對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

5.6.4 網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

5.7 遠端存取之限制

5.7.1 所有資訊資源使用者，非經主管授權或允許，禁止執行遠端存取作業。

5.8 資料庫存取控制

5.8.1 資料庫之存取權限，應經適當程序之授與及移除，且須使用獨立之帳號及密碼登入。

5.8.2 資料庫存取之身分驗證機制，須由系統內部安全機制提供。

5.8.3 資料庫使用者之帳號密碼設定必須符合本程序書及相關系統之帳號密碼管理規範之要求。

5.8.4 資料庫公用程式路徑之存取權限應適當控管，禁止一般使用者存取。

5.8.5 資料庫最高權限帳號之存取授權應僅限於資料庫管理員。

5.8.6 資料庫預設帳號應變更密碼，或是關閉使用。

5.8.7 資料庫之存取紀錄應留存查核紀錄。

5.9 系統被入侵時的異常處理

5.9.1 立即拒絕入侵者任何存取動作（例如關閉可疑帳號），防止災害繼續擴大。

5.9.2 關閉受侵害的主機，或立即與網路離線。

5.9.3 檢查防火牆及系統紀錄，研判入侵管道之方式，必要時作安全漏洞修補。

5.9.4 通知主機供應商提供必要的回復協助。

5.9.5 如伺服主機的完整性受侵害，應將完整的系統備份資料存回受害主機上，並測試其功能，直至完全回復為止，最後再將該主機重新上線。

6 相關文件

6.1 個人資料保護法

6.2 智慧財產權相關法令

6.3 電子簽章法

6.4 資訊服務申請表

6.5 帳號清查紀錄表

6.6 帳號清查結果報告