第五章
接達控制

5.1 接達控制的重要性

5.1.1 用戶應按照「有需要知道」原則來發出學校資料接達權限。這是為了避免用戶未經授權接達到敏感資料、資料被破壞的安全風險，以及違反《個人資料（私隱）條例》。

5.2 接達控制的要求

5.2.1 建議學校在向用戶及技術支援人員分配資訊系統的資源及權限時，應確保能遵從最小權限原則。這項原則將用戶可接達的資訊系統資源（如數據檔案、資訊科技服務及設施或電腦設備）或接達的種類（如讀、寫、執行、刪除），限制在履行其職責所需的最低限度。

5.2.2 資料擁有人應訂立適當的接達控制規則，以及個別用戶職務需要的資料接達權限。除非獲相關資料擁有人授權，否則不得接達。應定時審查接達控制規則，並應至少每年一次，特別是在新學年開始之前，因學科和職能委員會常有人事變動。

5.2.3 接達儲存機密或敏感類別資料的資訊系統，應受邏輯接達控制限制。邏輯接達控制是指除實體接達控制（例如限制出入放置系統的地方）以外對資訊科技資源的控制。一般來說，邏輯接達控制包括四大元素：用戶／用戶群組、資源、認證和授權。

(a) 用戶／用戶群組是指已登記及經確定可接達資訊科技資源的人員。

(b) 人員將獲授權接達系統資源，例如網絡、檔案、目錄、程式和數據庫。

(c) 認證是指核實用戶身分。認證通常基於三個要素進行：用戶所知的資料（例如個人辨認號碼或用戶名稱／密碼）、用戶擁有的憑證（例如權標或智能卡）或用戶的特徵或行為的資料（例如指紋、面部特徵、視網膜和聲音等生物特徵），如採用其中兩個要素（一般稱為雙重認證），可加強認證控制。

(d) 用戶／用戶群組經過認證後，便會獲授權接達系統資源。

5.3 用戶接達管理

5.3.1 應按「有需要知道」原則授予資料接達權限，並應明確界定、記錄和定期覆檢。

5.3.2 對於擁有特別接達權限的帳戶或用戶（例如管理員或系統帳戶），須考慮以下事項，以限制及控制特別權限的使用：

(a) 應確定每個系統或應用系統所涉及的特別權限和數據接達權限，以及需獲分配有關權限的用戶。

(b) 應根據最小權限原則及職務分工向用戶授予特別權限和數據接達權限。

(c) 應將特別權限和數據接達權限授予有別於常規業務活動所使用的用戶名稱。

(d) 不應以高權限用戶名稱進行常規業務活動。

(e) 應制訂特定程序，以防預設的管理員用戶名稱被未獲授權人士擅用。

5.3.3 所有用戶權限和數據接達權限（包括暫時及緊急的接達）如在一段預定時間內無任何操作都應註銷。

5.3.4 須註銷不再需要的用戶權限和數據接達權限，例如在終止或更改僱用某人員後。確定用戶權限和數據接達權限的文件須予以更新，以反映接達權限已被移除調整。如離職人員知悉用戶名稱的密碼，而這些名稱將需繼續使用，則應在終止或更改僱用該人員時更改這些密碼。

5.3.5 用戶權限和數據接達權限宜授予群組而非個人，例如群組接達清單。在此情況下，學校應從相關群組接達清單中移除離職人員，並通知相關方面不要與離職人員分享任何資料。

5.3.6 應建立個人問責制，使相關人員為其行動承擔責任。

5.3.7 不建議使用共用或群組用戶名稱。

5.3.8 學校應教育用戶有關資訊保安的重要性，並經常提醒他們保安的良好作業模式。

5.4 用戶責任

5.4.1 用戶只可使用其用戶名稱執行獲授權的工作和功能。

5.4.2 除非有一套能確認用戶身分以確實執行用戶問責制的措施，否則密碼不得共用或外泄。如有需要共用密碼，學校應就系統可能遭受的保安風險說明使用共用密碼的理據。共用密碼無需使用時應立即重設，而需長期共用的密碼則應經常更改，以盡量減低保安風險。

5.4.3 應時刻妥善保護密碼。當儲存密碼時，應採用接達控制及加密等保安控制措施以保護密碼，並在不可信任的通訊網絡進行傳輸時作加密處理。如無法進行密碼加密，學校須推行輔助控制措施，例如經常更改密碼。

5.5 系統及應用系統接達控制

5.5.1 學校應確保資訊系統採取適當及與其保安要求和所接達資料的敏感度相稱的認證機制和措施。

5.5.2 視乎所需的保安控制程度，使用密碼是一個簡單的認證方法。另一種認證方法是使用雙重認證（例如智能卡或權標）。

5.5.3 以下措施可減低密碼因受到如暴力攻擊等密碼猜測活動而外泄的可能性：

(a) 應控制連續嘗試登入失敗的情況，亦應訂立及執行嘗試登入次數、封鎖帳戶時限及封鎖計時器重設時限。在達到嘗試登入次數的上限後，帳戶便會自動失效。

(b) 可考慮採用增長每次連續登入嘗試的間隔時間的機制，以防範密碼猜測活動。

(c) 使用用戶接達記錄分析工具及中央記錄伺服器，以維持記錄的完整性，亦能監察用戶接達活動及協助事故調查。

5.5.4 學校應審慎地為各類帳戶制訂並記錄密碼政策，務求在保安要求和運作效率之間取得平衡。建議如下：

(a) 密碼政策應於所有資訊系統上確實執行。

(b) 密碼政策須至少訂明最短密碼長度、初次密碼設定、受限制字詞及格式、密碼更改周期的要求，以及一套良好的揀選密碼規則。

(c) 學校應使用嚴謹的密碼（例如由至少八個大小寫不一的字母、數字及特殊字符混合組成），並結合採用其他控制措施， 如密碼歷史記錄（例如記下八個密碼）、帳戶封鎖（例如五次嘗試登入失敗後），以及定期更改密碼（例如每 90 天）。

5.5.5 所有用戶均不得擷取或以其他方式取得可容許未獲授權接達的密碼、解密匙或任何其他接達控制裝置。

5.5.6 任何資訊系統啓用前，應更改所有預設密碼。如懷疑密碼已／正外泄，應立即更改密碼。

5.6 流動運算和遠程接達

5.6.1 詳情請參閱「第九章 – 流動裝置與流動應用程式防護」。