雲端校管系統
系統保安簡介及基本安全措施

以下是一些關於雲端校管系統系統保安及基本安全措施的資料，供學校參考：

括號【】內為相關網址／路徑

雲端校管系統資料庫　：　https://cdrcloudsams.edb.gov.hk/

資訊科技教育網頁　：　https://www.edb.gov.hk
【教育制度及政策 > 小學及中學教育 > 小學及中學教育適用 > 資訊科技教育】

1. 雲端校管系統的保安模組設定

雲端校管系統的保安模組提供了大量重要的保安設定及監控功能，校長應指派專人負責管理。負責保安模組的同工應該：

1.1小心計劃及設定各系統用戶及用戶組的權責。

1.2小心計劃及設定用戶登入政策，例如:

1.2.1 容許錯誤登入的最高次數

1.2.2 自動重啟已鎖用戶時限

1.2.3 密碼到期時限

1.2.4 曾用密碼紀錄之數目

1.3小心計劃及設定「位置存取控制」及「網絡協定位址組別」。

1.4每天檢視「用戶不成功登入紀錄」，以便監察系統使用情況。

1.5經常檢視「用戶組」權責及編配用戶入組的設定。

1.6經常檢視審計追蹤紀錄，特別是「教職員資料」及「財務管理及策劃」的審計追蹤紀錄。

1.7提醒各用戶須不定期或最少每半年一次更改登入用戶的密碼，並小心保管密碼，不要隨便透露密碼給他人使用，及不應從公共電腦登入系統。

1.8儘快更改過於簡單的密碼。新密碼須符合以下格式要求：

- 符合以下全部條件
  - 包含英文字母 a-z（細楷）
  - 包含英文字母 A-Z（大楷）
  - 包含數字 0 - 9
  - 包含特別字符（不能有空格）
- 密碼長度：8 - 40 字元

- 不能以用戶名稱作為密碼

1.9其他參考資料：

【Post-Installation Tasks of WebSAMS Implementation】

2. 保護資料、更新防毒軟件及系統的保安漏洞

電腦病毒泛指一些能夠影響電腦正常運作的有害程式。電腦病毒發作所造成的破壞程度參差不同，其影響可小至僅僅對屏幕的顯示造成滋擾，以至電腦儲存的珍貴資料受到破壞。此外，電腦軟件有機會出現保安漏洞， 學校應採用最新版本的修正檔案，以修補已知的保安弱點。

2.1定期執行防毒掃描及更新防毒軟件。

2.2最少每月一次到香港政府資訊安全網【https://www.infosec.gov.hk】查閱重大保安事件。

2.3 最少每星期一次到本局網頁【https://www.edb.gov.hk】的資訊科技教育【教育制度及政策 > 小學及中學教育 > 小學及中學教育適用 > 資訊科技教育】及雲端校管系統資料庫 【https://cdrcloudsams.edb.gov.hk/】查閱所發放的有關指引，強化各項跟電腦保安有關的措施，以及留意本局發放的相關資訊。

2.4確保用戶在獲授權情況下方可匯入及匯出系統數據，並作出適當措施保護敏感資料，避免外洩。在匯入數據時需維持數據的準確性、完整性和一致性，以保護重要資料。

2.5須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除或其他使用所影響，詳情可參閱「學校資訊保安-建議措施」第 6.4.1 節。有關個人資料(私隱)條例六項保障個人資料原則，學校可參閱以下網址:

【https://www.pcpd.org.hk/tc_chi/data_privacy_law/6_data_protection_principles/principles.html】

更新日期: 2024 年 10 月 24 日

CloudSAMS Security Guide and Recommended Practice

The following information on system security of CloudSAMS and recommended practice in this regard is for the reference of schools:

Relevant website/path is provided in bracket 【】

CloudSAMS CDR	:	https://cdrcloudsams.edb.gov.hk/
Website of IT in Education	:	https://www.edb.gov.hk 【Education System and Policy > Primary and Secondary School Education > Applicable to Primary and Secondary School > IT in Education】

1. Settings in Security Module of CloudSAMS

The security module of CloudSAMS provides a number of important security settings and monitoring functions. The school head should assign specific persons to manage this important module. The responsible staff should:

1.1 Plan and set up the rights and responsibilities of users and user groups of CloudSAMS carefully;

1.2 Plan and set up the user log-in policies carefully, such as:

- 1.2.1 The maximum number of fault log in attempts allowed
- 1.2.2 Auto-unlock period of locked accounts
- 1.2.3 Password expiry period
- 1.2.4 Number of passwords stored in password history

1.3 Plan and set up Location Access Control and IP addresses Group carefully;

1.4 Check Unsuccessful Login Log daily to monitor system usage;

1.5 Check access rights of User Groups and assignment of accounts to groups frequently;

1.6 Check Audit Trail records, particularly that of Staff Module and Financial Monitoring and Planning Module frequently;

1.7 Remind users to change their login password from time to time or at least every six months, keep the password properly, do not disclose the password to others and do not log on the system from public computers;

1.8 Change any simple password being in use as soon as possible. The new password should meet the minimum complexity requirements as follows:

- The password should fulfill all criteria:
  - contain English character(s) a-z (lower case)
  - contain English character(s) A-Z (upper case)
  - contain digit(s) 0-9
  - contain special character(s) ("Space" is not allowed)
- Length of password should be within 8-40 characters
- User ID cannot be used as password

1.9 Other reference material:
【Post-Installation Tasks of WebSAMS Implementation】

2. Protection of Data, Updates for Anti-virus Software and System Security Vulnerabilities

Computer virus refers to some harmful programs that can affect the normal operation of the computer system. Computer virus causes varying degrees of damages, the impact of which range from only a nuisance on the screen display, to a damage of valuable data stored in computers. Furthermore, in general, computer software is susceptible to security vulnerabilities, and schools should apply the latest version update/patch to fix any known security vulnerabilities.

2.1 Perform virus scanning and update anti-virus software regularly.

2.2 Visit the InfoSec website of the HKSAR Government at least once a month to check for major IT security incidents 【https://www.infosec.gov.hk】.

2.3 Visit the EDB websites 【https://www.edb.gov.hk】of IT in Education 【Education System and Policy > Primary and Secondary School Education > Applicable to Primary and Secondary School > IT in Education】 and CloudSAMS Central Document Repository 【https://cdrcloudsams.edb.gov.hk/】at least once a week to check for latest release of the corresponding guidelines to strengthen system security, and pay attention to the relevant information announced by EDB.

2.4 Ensure that users can only import and export system data when they are authorized to do so and appropriate measures have been taken to protect against leakage of sensitive data. To protect important data, when importing data to CloudSAMS, accuracy, integrity and consistency of system data should be maintained.

2.5 Take all feasible measures so as to ensure the personal data collected by data users are protected against unauthorized or accidental access, processing, erasure or use. For details, please refer to Section 6.4.1 of "Information Security in Schools - Recommended Practice". Schools may refer to the following website for the six personal data protection principles under the Personal Data (Privacy) Ordinance:
【https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html】

Updated: 24-10-2024