網上校管系統
系統保安簡介及基本安全措施

以下是一些關於網上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。

網上校管系統: https://cdr.websams.edb.gov.hk

資訊科技教育: 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. 實體保安

【 資訊科技教育 > 學校資訊保安建議措施】

實體保安是第一道防線，可以阻止外界直接對軟硬件作非許可的接觸及侵略者對保安系統的破壞。實體保安包括：

1.1 放置所有電腦設備如伺服器、工作站、手提電腦、網絡器材、備份／復原媒體和原裝軟件等在設有保安的地方。
1.2 妥善管理電腦設備的存貨目錄及使用紀錄。
1.3 界定學校個別地方不同程度的實體保安要求。

2. 互聯網

【網上校管系統資料庫 > 系統保安及系統事宜 > 系統操作> Kick-Start Guideline for WebSAMS Implementation】

互聯網是一個十分開放的環境，時刻都有受駭客入侵而導致系統停頓或資料外洩的可能。為預防及減低系統受到有意或無意的攻擊，學校應設有路由器 [Router] 和 HTTP 伺服器等硬件及互聯網通訊閘 [Internet Gateway]。路由器及互聯網通訊閘對校管系統，以至學校整個網絡運作的保安都起著十分重要的作用，如沒有這些基本硬件是不應開放網上校管系統在互聯網上使用 (詳情請參閱上述文件 – “Kick-Start Guideline for WebSAMS Implementation”)。

2.1 在使用系統初期，先限制只在校管網絡內使用網上校管系統，待熟習操作後才開放給資訊科技教育網絡使用，最後才考慮開放在互聯網上使用。
2.2 網上校管系統路由器必須已妥善設定，路由器的密碼已交專人保管。
2.3 互聯網通訊閘必須已妥善設定，通訊閘的密碼已交專人保管。
2.4 HTTP 伺服器必須已妥善設定，伺服器的密碼已交專人保管。
2.5 請勿在「網上校管系統」伺服器開啓遠端桌面服務 (Remote Desktop Service)。
2.6 定期檢查上述設定及更改以上各類密碼。

3. 學校每天需執行的系統保安檢查

【網上校管系統資料庫 > 系統保安及系統事宜 > 系統保安 > 安裝網上校管系統的系統保安簡介】

【網上校管系統資料庫 > 系統保安及系統事宜 > 系統保安 > WebSAMS System Operation Task List】

校長需要安排「網上校管系統」的負責老師，監督學校 TSS 定時(最理想每日)作例行工作，檢視「網上校管系統」的操作紀錄及本身的網絡設備，以警覺是否有任何不正常事項及可能受到的系統保安攻擊。只要及早偵察到這些攻擊，通知「網上校管系統」的負責老師，並立刻將受攻擊那部份的服務暫時停止，受到的影響便可減至最低。而需監察的紀錄包括：

3.1 「網上校管系統」的系統審計追蹤、資料庫備份紀錄等。

3.2 HTTP 伺服器紀錄，例如 Linux 及 Apache 系統紀錄，保安紀錄等。

3.3 互聯網通訊閘、路由器及互聯網服務供應商的保安監察服務紀錄 [若適用]。

3.4 「網上校管系統」所提供的「網上校管系統版本升級紀錄」、「聯遞系統(CDS)紀錄」等。

4. 「網上校管系統」的保安模組設定

【網上校管系統資料庫 > 系統保安及系統事宜 > 系統操作> Post-Installation Tasks of WebSAMS Implementation】

「網上校管系統」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：

4.1 小心計劃及設定各系統用戶及用戶組的權責。

4.2 小心計劃及設定用戶登入政策，例如:

4.2.1 容許錯誤登入的最高次數；

4.2.2 自動重啟已鎖用戶時限；

4.2.3 密碼到期時限；

4.2.4 曾用密碼紀錄之數目

4.3 小心計劃及設定「位置存取控制」及「網絡協定位址組別」。

4.4 每天檢視「用戶不成功登入紀錄」，以便監察系統使用情況。

4.5 經常檢視「用戶組」權責及編配用戶入組的設定。

4.6 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。

4.7 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。

4.8 儘快更改過於簡單的密碼。新密碼須符合以下格式要求：

- 符合以下四項條件中的任何三項
  - 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

5. 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。

5.1 校管系統每天都能成功執行資料庫備份。

5.2 定期執行防毒掃描及更新防毒軟件。

5.3 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。

5.4 最少每星期一次到本局的資訊科技教育 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〕及網上校管系統網頁 https://cdr.websams.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。

5.5 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。

5.6 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

5.7 請勿在「網上校管系統」伺服器上安裝非本系統指定的軟件。(有關的指定軟件名單，請參閱文件“Hardware and Software Specification for Upgrading to WebSAMS 3.0 (2014-2015)”)

更新日期: 2020 年 8 月 20 日

WebSAMS Security Guide and Recommended Practice

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

The relevant website / path is provided in bracket 【】

WebSAMS : https://cdr.websams.edb.gov.hk
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. Physical Security

【IT in Education > Information Security in Schools - Recommended Practice】

Physical security is the first line of defense. It can prevent unauthorized access to hardware from outside and damages to the security system by intruders. Physical security measures include:

1.1 place all computer equipment such as servers, workstations, laptops, network equipment, backup/recovery devices and original software, etc in secure areas;
1.2 manage the inventory of computer facilities and usage records properly;
1.3 define the respective levels of physical security requirements for different places of the school.

2. Internet

【網上校管系統資料庫 > 系統保安及系統事宜 > 系統操作> Kick-Start Guideline for WebSAMS Implementation】

The Internet is an open environment which is susceptible to system suspension or data leakage due to hacking attacks. To prevent and reduce intentional or unintentional system attacks, schools should set up hardware including the WebSAMS router and HTTP server, as well as internet gateway. The WebSAMS router and internet gateway play a very important role to protect WebSAMS as well as the entire school network system. WebSAMS should not be opened for access via the internet without these basic hardware (please refer to the document - "Kick-Start Guideline for WebSAMS Implementation" mentioned above for details).

2.1 At the early stage after setting up the system, the use of WebSAMS should be limited to the school's WebSAMS network. After getting familiarized with the system, schools may consider connecting WebSAMS with the IT in Education network and eventually, consider opening it for access via the internet.
2.2 The WebSAMS router needs to be set up properly and the password of the router should be kept by designated person(s).
2.3 Internet gateway needs to be set up properly, and the password of the gateway should be kept by designated person(s).
2.4 The HTTP server needs to be configured properly and the password of the server should be kept by designated person(s).

2.5 Do not enable Remote Desktop Service on the WebSAMS server.
2.6 Perform checking on the above settings and change the passwords mentioned above regularly.

3. Daily System Security Checks by Schools

【網上校管系統資料庫 > 系統保安及系統事宜 > 系統保安 > 安裝網上校管系統的系統保安簡介】
【網上校管系統資料庫 > 系統保安及系統事宜 > 系統保安 > WebSAMS System Operation Task List】

The school head needs to arrange responsible teacher(s) of WebSAMS to supervise the school TSS to regularly (recommended on a daily basis) conduct routine maintenance work to check system logs of WebSAMS and its network devices for early identification of any abnormal events and/or signs of possible attacks on system security. If signs of these attacks are detected early to alert the responsible teacher(s) of WebSAMS to suspend the services of the component under attack immediately, thus minimizing the impact. The records to be monitored include:

3.1 System audit trail of WebSAMS, database backup records, etc;
3.2 HTTP server records, such as Linux and Apache system records and security records;
3.3 Records of Security Surveillance Service for internet gateways, routers and internet service providers (if applicable);
3.4 WebSAMS build version upgrade log, CDS log, etc, which are provided by WebSAMS.

4. Settings in Security Module of WebSAMS

【網上校管系統資料庫 > 系統保安及系統事宜 > 系統操作> Post-Installation Tasks of WebSAMS Implementation】

The security module of WebSAMS 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:

4.1 Plan and set up the rights and responsibilities of users and user groups of WebSAMS carefully;
4.2 Plan and set up the user log-in policies carefully, such as:
  4.2.1 The maximum number of fault log in attempts allowed;
  4.2.2 Auto-unlock period of locked accounts;
  4.2.3 Password expiry period;
  4.2.4 Number of passwords stored in password history
4.3 Plan and set up Location Access Control and IP addresses Group carefully;
4.4 Check Unsuccessful Login Log daily to monitor system usage;
4.5 Check access rights of User Groups and assignment of accounts to groups frequently;
4.6 Check Audit Trail records, particularly that of Staff Module and Financial Monitoring and Planning Module frequently;
4.7 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;
4.8 Change any simple password in use as soon as possible. The new password should meet the minimum complexity requirements as follows:
- The password should fulfill any 3 out of the 4 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

5. 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.

5.1 Ensure successful implementation of WebSAMS database backup on a daily basis.

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

5.3 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】.

5.4 Visit the websites 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】 and WebSAMS Central Document Repository 【https://cdr.websams.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 the EDB.

5.5 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 WebSAMS, accuracy, integrity and consistency of system data should be maintained.

5.6 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】

5.7 Do not install any software which are outside the software specification list for the WebSAMS server (for the list of the specified software, please refer to the document - "Hardware and Software Specification for Upgrading to WebSAMS 3.0 (2014-2015)").