

網上校管系統 系統保安及常規保安措施簡介會

內容概覽

(一) 現時雲端服務計劃的運作情況

(二) 雲端服務保安措施及數據加密安排

(三) 雲端平台安全使用錦囊

(四) 網上校管系統安全使用錦囊

(五) 問答時間

(一) 現時雲端服務計劃的運作情況

- 現時全港使用「網上校管系統」的學校，分別於 2018 年、2019 年、2020 年、2021 年及2022 年轉用了雲端服務來運行系統，整體運作暢順。
- 現時雲端服務平台如下：

參與雲端服務年份	2019 / 2020	2018 / 2021 / 2022 (雲端服務整合平台)
雲端服務承辦商	HKBN JOS Limited	SunnyVision Limited
數據中心數目	1	2
學校數目	150 / 150	75 / 301 / 300

(一) 現時雲端服務計劃的運作情況

- 雲端服務平台整合計劃目標：
 - 統一雲端平台的技術運作及行政管理
 - 更有效運用雲端平台資源
 - 採用雙數據中心架構：
 - 攤分日常運行負荷，避免同時受災風險
 - 互為後備，無需使用學校原有伺服器作後備用途
- 於2024 - 2025，會將2019和2020參與雲端服務計劃的「網上校管系統」，遷移至整合平台。

(一) 現時雲端服務計劃的運作情況

- 網上校管系統開放時間
 - 星期一至日 6:00am – (翌日)1:00am
 - 其他時間為平台維護時段
- 承辦商負責伺服器日常維護，軟件更新等工作。
- 雲端服務求助台, 供學校聯絡人提出服務請求。
 - 服務時間同上
- 中央模式處理網上校管系統版本升級
- 每天維護時段內製作備份
 - 每日備份保存一個月
 - 每月最後一天的備份保存一年

(二) 雲端服務保安措施及數據加密安排

■ 數據中心的保安措施

- 承辦商已取得相關資訊安全管理的 ISO 認證
- 承辦商必須遵守由政府資訊科技總監辦公室(OGCIO) 制定的資訊科技安全指引
- 定期委託第三方進行保安風險評估及審計(Security Risk Assessment and Audit)，審視及完善保安措施
- 由專業人員負責系統管理及維護，定期更新系統軟件及實時監測系統運作狀況

(二) 雲端服務保安措施及數據加密安排

- 數據中心的保安措施
 - 採用私有雲模式，安裝獨立雲端平台設備，不與其他系統的雲端服務共用
 - 任何外掛系統 / 程式，均不可連接雲端平台，或在雲端平台上安裝，以保障系統穩定及安全
 - 每所學校的網上校管系統和數據都是獨立間隔運行

(二) 雲端服務保安措施及數據加密安排

- 雲端平台的加密 (encryption) 安排
 - 各學校的「網上校管系統」數據被個別加密，只有學校負責人擁有解密密碼。
 - 學校使用網上校管系統時為HTTPS加密連線。
 - 供下載的數據備份 zip 檔，用學校自設的密碼加密。
 - 重要系統功能，需要虛擬私人網絡(VPN)保密連線。

(三) 雲端平台安全使用錦囊

■ 重要物品及密碼

- 學校應妥善保管以下物品，及定期更新密碼。

服務	用戶名稱/密碼/密鑰	遺失時的處理方法
學校數據	BitLocker密碼# / Data Encryption 密碼 視窗管理員密碼# BitLocker修復金鑰#	聯絡SLO要求重置
求助台服務	聯絡人的身份認證系統用戶名稱及密碼 電話熱線服務識別碼 (PIN)	聯絡求助台安排重置

只適用於雲端服務計劃 2019及 2020。

* 若三位聯絡人的身份認證系統名稱 / 密碼皆已遺失而無法聯絡求助台，請聯絡網上校管系統學校聯絡主任。

(三) 雲端平台安全使用錦囊

■ 各密碼及重要物品

服務	用戶名稱/密碼/密鑰	遺失時的處理方法
VPN連線	VPN 用戶名稱 VPN 密碼	聯絡求助台安排重置
	VPN 實體保安編碼器 #	聯絡求助台刪除該保安編碼器權限及安排補領
	VPN 流動保安編碼程式啟動碼 (啟動前) ^ VPN 流動保安編碼裝置 (已啟動)	聯絡求助台安排重發啟動電郵

只適用於雲端服務計劃 2019及 2020。

^ 使用過一次的啟動碼便失去效用，學校可適時刪除。

(三) 雲端平台安全使用錦囊

■ 學校人事變動

- 若BitLocker密碼# / Data Encryption 密碼、視窗管理員密碼#、BitLocker修復金鑰# 等的持有人離職
 - 學校應盡快更改密碼 (需要原本密碼)。
 - 如學校忘記原本密碼，應盡快通知SLO安排重置。

- 若學校聯絡人離職
 - 盡快通知教育局更新聯絡人資料，承辦商會：
 - 撤銷已離職學校聯絡人的雲端服務求助台用戶
 - 並開設新用戶予新聯絡人

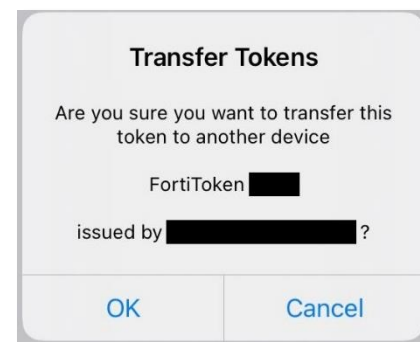
只適用於雲端服務計劃 2019及 2020

(三) 雲端平台安全使用錦囊

■ 學校人事變動

■ 若VPN用戶/保安編碼器# /流動保安編碼裝置持有人離職

- 學校應儘快更改VPN密碼及妥善交接保安編碼器/流動保安編碼裝置。
- 如需要轉用新保安編碼裝置，學校可使用「Transfer Tokens」功能，自行轉移裝置。(過程需校長協助)
- 如忘記密碼，請通知承辦商重置密碼。
- 如遺失保安編碼器#，請向承辦商申請補領。
- 如遺失保安編碼裝置，請通知承辦商重發流動保安編碼程式啟動電郵，以便學校在新裝置上安裝及啟動流動保安編碼程式。



只適用於雲端服務計劃 2019及 2020

(三) 雲端平台安全使用錦囊

■ VPN服務安排

- 採用VPN用戶(名稱和密碼)及保安編碼作雙重認證。

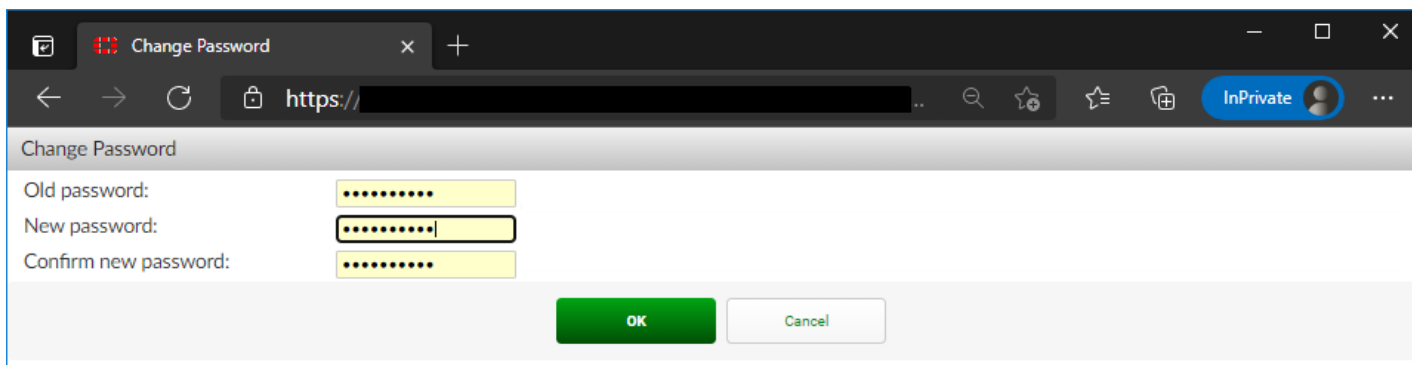
參與雲端服務年份	2019 / 2020	2018 / 2021 / 2022 (雲端服務整合平台)
每所學校 VPN 用戶數目	2	2
每所學校 VPN 保安編碼	實體保安編碼器 及 流動保安編碼程式	全面採用流動保安編碼程式
VPN 保安編碼程式啟動 電郵有效時限	3 日	10日

(三) 雲端平台安全使用錦囊

■ VPN密碼更改及有效期限

(只適用於雲端服務平台整合計劃)

- VPN密碼有效期限為180日。
- 學校如欲更改密碼，可登入相關網站。

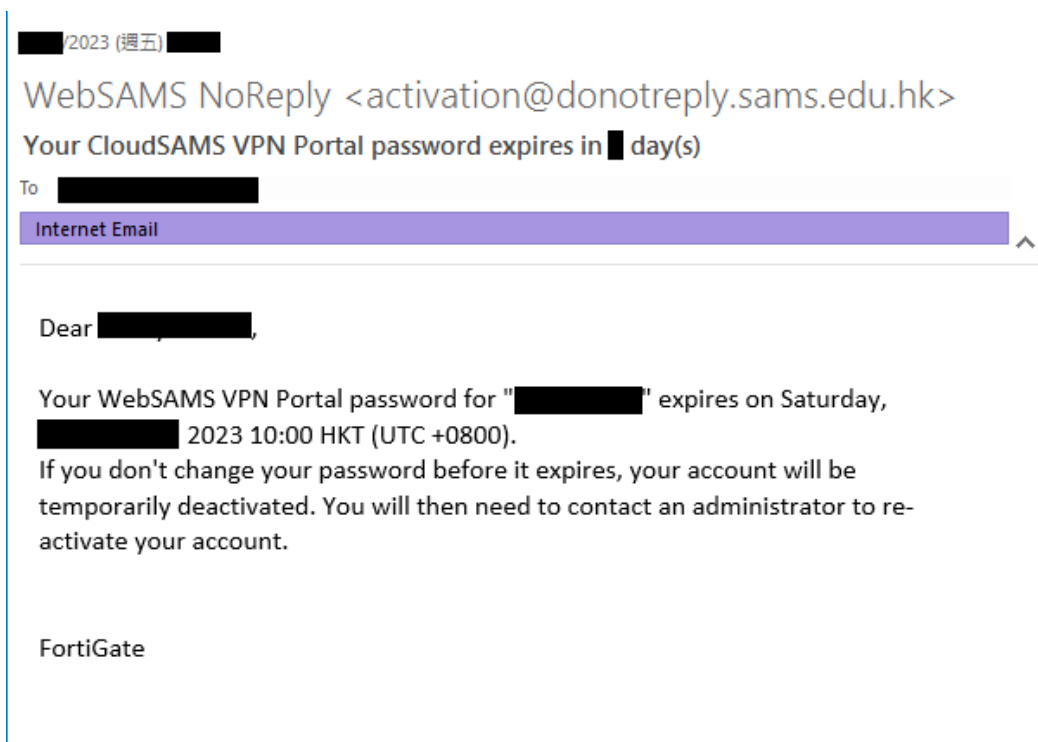


The screenshot shows a web browser window with the title 'Change Password'. The address bar shows 'https://'. The form contains three input fields: 'Old password:', 'New password:', and 'Confirm new password:'. Each field is represented by a yellow box with black dots. Below the fields are two buttons: a green 'OK' button and a white 'Cancel' button with a green border. The browser's address bar and navigation buttons are visible at the top.

- 密碼過期前數天，會有提示電郵傳送至校長電郵地址。
- 密碼過期後，學校必須提交表格申請重置密碼。

(三) 雲端平台安全使用錦囊

- VPN密碼更改及有效期限
(只適用於雲端服務平台整合計劃)
 - 提示電郵



(三) 雲端平台安全使用錦囊

■ 使用VPN注意事項

- 定期更新相關軟件至最新版本，以確保軟件安全：
 - FortiClient – VPN連線軟件
 - FortiToken – 流動保安編碼程式
- 安裝軟件的流動裝置，亦要做好保安措施。
- 經常留意VPN相關電郵(校長電子郵箱)，例如密碼過期提示。

(三) 雲端平台安全使用錦囊

- 使用雲端服務求助台注意事項
 - 只有學校聯絡人，才有權聯絡求助台。
 - 如致電求助台，必須輸入電話PIN碼，才可接通。
 - 如發電郵至求助台，必須用學校聯絡人的電郵地址發送。
 - 部份操作要求(例如重啟網上校管系統)，必須登入求助台的身份認證系統做確認。

(三) 雲端平台安全使用錦囊

■ 求助台身份系統登入密碼更改及有效期限

(只適用於雲端服務平台整合計劃)

- 密碼有效期限為180日。
- 可以直接登入求助台系統更改密碼。
- 密碼過期前數天，學校聯絡人會收到提示電郵。
- 密碼過期後，登入系統時，會強制要求即時更改密碼。

From: noreply@sunnyvision.com

Subject : Your WebSAMS Cloud Helpdesk system password will expire in XX day

Content :

Dear XXX,

The login password of your WebSAMS Cloud Helpdesk system (<https://websams.sunnyvision.com>) account (account name: XXX) will expire after XX day from now.

To change your password, you can follow to the following steps:

1. Login to WebSAMS Cloud Helpdesk system (<https://websams.sunnyvision.com>)
2. Click "Profile" button at the top rightmost of Support Center homepage
3. You can retype your current password and type new password twice under "Access Credentials" session
4. Click "Update" button to complete password changing action

The original password was sent to school from EDB by CDS message in WebSAMS, before your school WebSAMS migrate to the cloud platform.

If you have lost or forgotten your password, please fill in and submit Form C to the Cloud Helpdesk:

<https://cds.websams.edb.gov.hk/cloud>

常用申請表 --> 雲端服務計劃2022 --> 雲端服務求助台客戶服務表格(表C)

For enquiry, please contact the Cloud Helpdesk by calling tel: 2802-0218 or sending email to websams.helpdesk@sunnyvision.com.

SunnyVision Limited, WebSAMS Cloud Contractor

(三) 雲端平台安全使用錦囊

■ 辨別求助台

- 因承辦商不同，分別有兩個雲端服務求助台。

參與雲端服務年份	2019 / 2020	2018 / 2021 / 2022 (雲端服務整合平台)
雲端服務承辦商	HKBN JOS Limited	SunnyVision Limited
聯絡方法	<p>☎ : 2201 7268</p> <p>✉ : ms-helpdesk@hkbn.com.hk</p>	<p>☎ : 2802 0218</p> <p>✉ : websams.helpdesk@sunnyvision.com</p>

(三) 雲端平台安全使用錦囊

■ 辨別求助台

- 雲端服務求助台只處理雲端服務相關事宜，如VPN連線問題，協助重啟系統等等。
- 網上校管系統內的功能問題，請聯絡一直以來原有的網上校管系統求助台。

網上校管系統求助台
(WebSAMS Helpdesk)

電話：2166 1150 傳真：5801 1284
電郵：websams_support@ges.com.hk
辦公時間：
星期一至五 上午8:30至下午5:30
星期六 上午8:30至下午1:00

- 各求助台的聯絡方法可在網上校管系統資料庫(CDR)網站找到：

<https://cdr.websams.edb.gov.hk/聯絡我們>

(三) 雲端平台安全使用錦囊

■ 不同工作站的權限

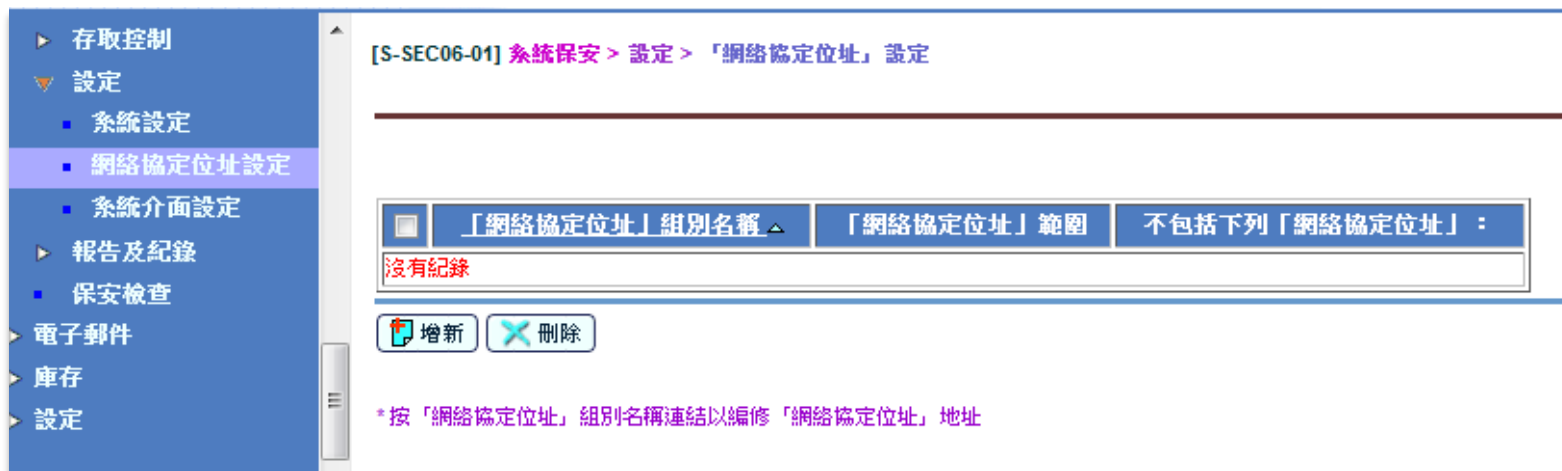
- 沿用網上校管系統三種工作站的設定，各種工作站擁有不同登入權限。
 - VPN 工作站 (權限等同網上校管系統網絡內工作站)
 - 校內工作站 (權限等同 ITED 工作站)
 - 校外工作站 (權限等同 Internet 工作站)

(三) 雲端平台安全使用錦囊

■ 設定學校Internet IP Address

- 系統保安模組 → 設定 → 「網絡協定位址」設定 (IP Config)

必須連接VPN



[S-SEC06-01] 系統保安 > 設定 > 「網絡協定位址」設定

「網絡協定位址」組別名稱 ▲	「網絡協定位址」範圍	不包括下列「網絡協定位址」：
沒有紀錄		

* 按「網絡協定位址」組別名稱連結以編修「網絡協定位址」地址

- 學校在遷移至雲端平台後，應已設定互聯網服務供應商(ISP)提供的Internet IP Address，以辨認校內/校外工作站。

(三) 雲端平台安全使用錦囊

- 設定學校Internet IP Address
 - 轉換互聯網服務供應商(ISP) 或校舍搬遷
 - 盡快在系統內更新Internet IP address
 - 並通知學校聯絡主任 — SLO
 - 留意以下類別的瀏覽器功能或插件(plugin) :
 - 節省網絡流量
 - 第三方 VPN
(不是網上校管系統雲端平台的 VPN)

這類功能，有可能會影響網上校管系統辨認工作站。

(三) 雲端平台安全使用錦囊

■ reCAPTCHA 驗證措施

- 如使用校外工作站，網上校管系統的登入畫面便會要求使用者進行 reCAPTCHA 驗證。



學校行政及管理系統
School Administration & Management System

 網上校管系統

[Central Document Repository](#)
網上校管系統資料庫

[Log on using CLO](#)
使用統一登入系統登錄

User ID
Password

☐ I'm not a robot 

Login

WebSAMS Version 3.1.6
(RESTRICTED) Access to this system and the information / materials contained therein are restricted to authorized users only.
(限制) 只容許已授權的用戶使用此系統及存取其資料
Best viewed with 800X600 resolution
Copyright © 2009, Education Bureau, The Government of the HK SAR.
All Rights Reserved.

(三) 雲端平台安全使用錦囊

■ 關於工作站的安全措施 (特別是連接 VPN)

- 不要使用公眾工作站。
- 注意學校的使用工作站安全指引。
- 安裝最新Windows Updates。
- 安裝防毒軟件，下載最新病毒定義，定期掃描病毒。
- 避免安裝不知名軟件。
- 使用最新版本瀏覽器。
- 避免在瀏覽器使用不需要的插件(plugin)。

(三) 雲端平台安全使用錦囊

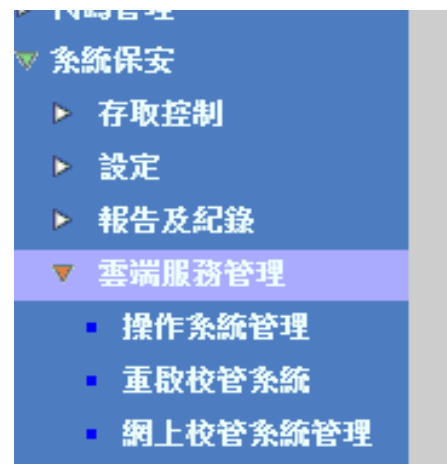
■ 雲端服務管理頁面

■ 系統保安模組 → 雲端服務管理

必須連接VPN

■ 系統用戶必須屬於以下用戶組別：

- 校長 (SCHOOL_HEAD)
- 雲端服務管理員 (CS_ADMIN)
- 雲端服務支援人員 (CS_SUPP)



(三) 雲端平台安全使用錦囊

■ 下載資料庫

- 如校務工作需要，學校可自行下載資料庫zip檔。

系統保安模組 → 雲端服務管理 → 網上校管系統管理



必須連接VPN



- zip檔是用學校自行設定的密碼加密
(BitLocker密碼# / Data Encryption 密碼)
- 學校必須小心保管，注意資料庫保安，避免資料洩漏。

只適用於雲端服務計劃 2019及 2020

(三) 雲端平台安全使用錦囊

■ 下載資料庫

- 更改zip檔解密密碼 (*BitLocker*密碼# / *Data Encryption* 密碼)

系統保安模組 → 雲端服務管理 → 操作系統管理

必須連接VPN



[S-SEC28-01] 系統保安 > 雲端服務管理 > 操作系統管理

更改Data Encryption密碼

輸入Data Encryption舊密碼

輸入Data Encryption新密碼

再輸入新密碼以作確定

重置Data Encryption密碼

輸入Data Encryption新密碼

再輸入新密碼以作確定

- 每次更改，只會影響此後製作的zip檔。此前已製成的zip檔，仍然要用舊密碼解密。

只適用於雲端服務計劃 2019及 2020

(三) 雲端平台安全使用錦囊

■ 重啟校管系統

- 如學校需要，可自行重啟網上校管系統。

系統保安模組 → 雲端服務管理 → 重啟校管系統

必須連接VPN

[S-SEC29-01] 系統保安 > 雲端服務管理 > 重啟校管系統

重啟校管系統

確定

- 如學校不能自行重啟網上校管系統，可聯絡雲端服務求助台。

(三) 雲端平台安全使用錦囊

■ 系統版本升級

- 每個新版本的升級日期宣布後，如學校想在延緩的日期才升級，可在以下頁面按「確定」。

系統保安模組 → 雲端服務管理 → 網上校管系統管理



必須連接VPN

[S-SEC30-01] 系統保安 > 雲端服務管理 > 網上校管系統管理

並沒有延緩部署日期

網上校管系統版本升級	
現行網上校管系統版本	3.1.6
目標網上校管系統版本	
正常部署日期	
延緩至部署日期	
延緩網上校管系統版本升級	<input type="button" value="確定"/>

(三) 雲端平台安全使用錦囊

■ 嚴重事故後備方案

參與雲端服務年份	2019 / 2020	2018 / 2021 / 2022 (雲端服務整合平台)
數據中心數目	1	2
數據中心發生嚴重事故時的後備方案	學校須保留校內原有系統伺服器作後備用途	兩個中心互作後備 學校不須保留校內原有系統伺服器
後備設施維護	<ul style="list-style-type: none"> 建議每月進行一次伺服器軟件更新，包括： <ul style="list-style-type: none"> Windows Update Antivirus Software & Definition Update HTTP Server Update 不需要進行 WebSAMS build upgrade 	由承辦商負責

(三) 雲端平台安全使用錦囊

■ 常見疑問

- 學校轉換了互聯網服務供應商 (ISP)，有甚麼需要注意？
 - 必須使用固定及專用的Internet IP address，不能與ISP的其他客戶共用。
 - 若ISP有提供網站過濾/篩選功能，可能會使用代理伺服器(web proxy)技術連接網站，這會影響網上校管系統辨別校內/校外工作站。遇上這類情況，請與ISP商討解決辦法。

(三) 雲端平台安全使用錦囊

■ 常見疑問

■ 校長及兩名聯絡人提供電郵地址有甚麼主要用途？

主要用途如下：

- VPN相關電郵如密碼過期提示、流動保安編碼程式啟動碼等，會傳送至校長的電郵地址。得到啟動碼，便得到VPN用戶的流動保安編碼程式使用權。
- 由校長或聯絡人發出的電郵，雲端服務求助台才會受理。
- 如向雲端服務求助台提出操作指示如重啟系統，會有電郵傳送至相關聯絡人的電郵地址，要求登入身份認證系統。
- 若學校要求重置VPN用戶密碼、雲端服務求助台用戶的密碼或電話熱線PIN，新密碼或PIN會傳送至校長的電郵地址。

(三) 雲端平台安全使用錦囊

■ 參考文件及手冊

- <https://cdr.websams.edb.gov.hk/cloud/cloudref/>
- 請點選學校所屬的雲端服務計劃。

參考資料

主頁 > 參考資料

雲端服務計劃2019

雲端服務計劃2020

雲端服務計劃2022

雲端服務平台整合計劃










(三) 雲端平台安全使用錦囊

■ 參考文件及手冊

■ 較常用的文件或手冊包括：

- VPN連線程序指引
- 承辦商雲端服務求助台用戶手冊
- 雲端服務管理頁面用戶手冊
- Computer Operating Procedures Manual For School

用戶手冊及指引

VPN連線程序指引 (VPN Connection Guide)	英 	 下載
VPN 客戶端軟件 (VPN Client)		
數據遷移程序指引 (User Guide for Migration Toolkit)	英 	 下載
數據遷移程式 (Migration Toolkit)		
數據遷移操作示範短片		
承辦商雲端服務求助台用戶手冊	中 	
雲端服務管理頁面用戶手冊 (User Manual for Cloud Service Management Page)	中 	
Troubleshooting on Data Migration	英 	
Computer Operating Procedures Manual For School	英 	

(三) 雲端平台安全使用錦囊

■ 常用申請表

- <https://cdr.websams.edb.gov.hk/cloud/cloudform/>
- 請點選學校所屬的雲端服務計劃。

常用申請表

主頁 > 常用申請表

雲端服務計劃2019

雲端服務計劃2020

雲端服務計劃2022

雲端服務平台整合計劃

(三) 雲端平台安全使用錦囊

■ 常用申請表

啟用重設密碼功能申請表 (表A)



更改學校聯絡人申請表 (表B)



雲端服務求助台客戶服務申請表 (表C)



[申請更改學校聯絡人個人資料／重置身份認證系統登入密碼／重置電話識別碼(PIN)適用]

VPN連線客戶服務申請表 (表D)



[申請重置虛擬私人網路(VPN) 登入密碼／重發流動保安編碼程式啟動電郵(Activation Email)適用]

(三) 雲端平台安全使用錦囊

■ 學校個案分享

- 一部手機上同時使用了兩個保安編碼程式啟動碼。
- VPN連線設定，輸入了其他雲端服務計劃的VPN Gateway。
- 一部電腦連接VPN後，嘗試在校內另一部電腦使用VPN工作站限定的網上校管系統功能。
- 嘗試連接VPN不成功，原來有同工曾用同一用戶連接了VPN，沒有解除連線。
- 使用不相對應的VPN用戶和VPN保安編碼器/裝置。
- 負責老師離職後，所有密碼/PIN/保安編碼器/裝置失傳，沒其他人知道。

(三) 雲端平台安全使用錦囊

■ 學校個案分享

- 學校使用whatismyipaddress.com或類似的網站找出自己學校的Internet IP address。但使用網上校管系統時，系統偵測到的IP address卻不相同。
- 雲端平台監測系統發現網上校管系統登入畫面不能正常顯示，CPU用量頗高。與學校溝通後，發現原因是學校在DAT模組執行SQL，但SQL沒有正確地 join tables。

(四) 網上校管系統安全使用錦囊

(I) 資訊保安

(I)資訊保安

■ 資訊保安4A

- 認證 (Authentication)
- 授權 (Authorisation)
- 紀錄 (Accounting)
- 審計 (Audit)

■ 認證 (Authentication)

- 小心計劃及設定用戶登入政策
- 容許錯誤登入的最高次數
- 自動重啟已鎖用戶時限
- 自動登出時限
- 密碼到期時限
- 帳戶到期時限
- 曾用密碼紀錄之數目

■ 妥善設定系統保安預設值

[S-SEC01-01] 系統保安 > 設定 > 系統設定

一般設定	
容許錯誤登入最高次數 〔下限: 3, 上限: 5, 預設值: 5〕	5
自動重啟已鎖用戶時限 〔下限: 12 分鐘, 上限: 120 分鐘, 預設值: 60 分鐘〕	12 分鐘
在虛擬私人網絡內自動登出時限 〔下限: 5 分鐘, 上限: 120 分鐘, 預設值: 15 分鐘〕	120 分鐘
在虛擬私人網絡外自動登出時限 〔下限: 5 分鐘, 上限: 60 分鐘, 預設值: 5 分鐘〕	60 分鐘
密碼到期時限 〔下限: 30 日, 上限: 365 日, 預設值: 100 日〕	365 日
曾用密碼紀錄之數目 〔〔下限: 1, 上限: 5, 預設值: 1〕〕	1
容許多人同時登入同一戶口 〔預設: 不容許〕	<input checked="" type="checkbox"/>
啟動容許從互聯網登入 〔預設: 不容許〕	<input checked="" type="checkbox"/>
啟動容許從學校網絡登入 〔預設: 不容許〕	<input checked="" type="checkbox"/>
啟動容許已到期密碼登入 〔預設: 不容許〕	<input checked="" type="checkbox"/>
啟動容許從統一登入系統登入 〔預設: 不容許〕	<input checked="" type="checkbox"/>

設定用戶及權限

- 設定帳戶到期日，防止過期帳戶登入
- 設定用戶密碼到期日，規定用戶更改密碼

設定用戶及權限

- 及時移除過期/無效帳戶(包括離職人員/離校學生及其家長)
- 開設學生、家長戶口前必須考慮周詳，並作出周全的運作安排(包括限制用戶使用範圍及時段)

養成良好習慣，承擔操作責任

- 學校應編訂及頒布用戶使用守則和程序，以便遵循及協助用戶正確使用網上校管系統，增加學校行政管理效能
- 用戶必須養成良好使用網上校管系統習慣，並為名下戶口的登入狀況和操作承擔責任

(I) 資訊保安

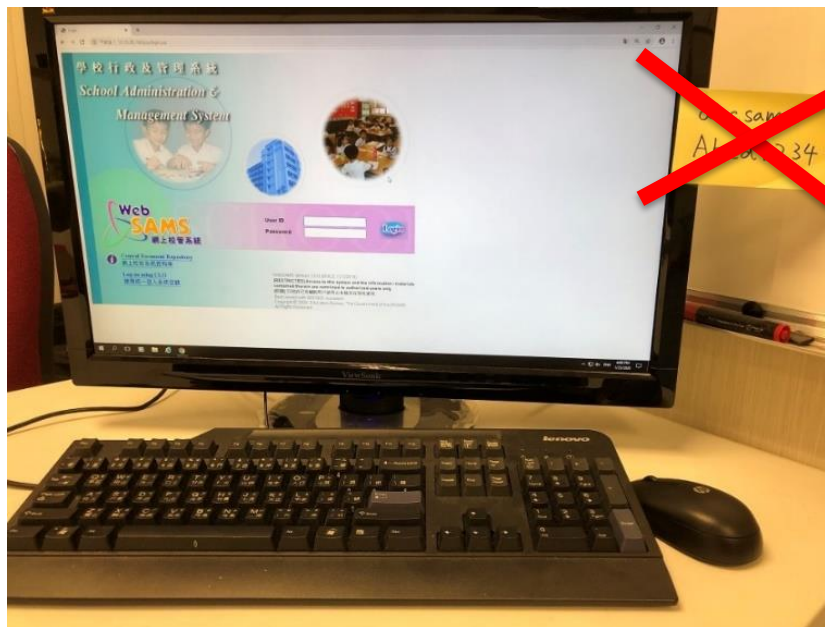
- 用戶只可用名下戶口登入，切勿同一戶口多人共用(例如 sysadmin)

(I) 資訊保安

- 為保障帳戶安全，完成操作後應登出系統及關閉瀏覽器
- 設定合理的鎖定系統時間
- 可啟用螢幕保護程式

(I) 資訊保安

- 妥善保管用戶資料及密碼，切勿置於開放及當眼地方



(I) 資訊保安

定期更改各類密碼

[S-SEC04-02] 系統保安 > 存取控制 > 用戶 > 搜尋用戶

搜尋用戶 新增個人用戶 新增學生/家長用戶
更改用戶資料

最後登入日期時間：07/12/2017 11:58

學校級別/授課制 (* 只用於教職員和其他用戶的資料層面的控制)

學校級別 小學 學校授課制 全部

用戶類別 ☐ 教職員 ☐ 學生 ☐ 家長 ☒ 其他

用戶代碼 到搜尋頁

* 「教職員」用戶類別的用戶代碼為「教職員編號」，「學生/家長」用戶類別則為「學生註冊編號」，用戶代碼不適用於「其他」用戶類別

用戶名稱 (* 用作登入) aaaaaa

密碼 *****

輸入新密碼

確認密碼

密碼到期 ☒ 永不到期 ☐ 密碼到期日

(DD/MM/YYYY)

英文用戶姓名 AAAAAA

中文用戶姓名 甲甲甲甲甲甲

使用語言 中文

用戶存取時限

* 實際存取時限，會受「系統存取時限」的設定所影響

星期一至六 ☐ 00 : 00 至 00 : 00 ☐ 24 小時

星期日 ☐ 00 : 00 至 00 : 00 ☐ 24 小時

用戶到期 ☒ 永不到期 ☐ 用戶到期日

(DD/MM/YYYY)

已編配用戶組 ☐ STA_ADMIN

☐ STAFF_OR_OTHERS

編配用戶組 退出用戶組

已編配互聯網存取時限概況

☐ STAFF_OR_OTHERS

編配概況 退出概況

重設 儲存 返回前頁

密碼格式：

- 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)
- (密碼須符合以上四項條件中的任何三項)
密碼長度：8-40字元
不能以用戶名稱作為密碼

[S-SEC13-01] 設定 > 更改密碼

輸入舊密碼

輸入新密碼

再輸入新密碼以作確定

儲存

密碼格式：

- 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)
- (密碼須符合以上四項條件中的任何三項)
密碼長度：8-40字元
不能以用戶名稱作為密碼

[S-CDS08-01] 聯通系統 > 學校密碼匙管理 > 更改學校密碼匙

更改學校密碼匙 學校密碼匙更改紀錄

現時學校密碼匙

有效期間

27/06/2017 - 27/06/2018

新學校密碼匙

再輸入新學校密碼匙

重設

儲存

調整學校密碼匙

調整聯通系統資料表

請注意：學校密碼匙

- 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)
- (學校密碼匙須符合以上四項條件中的任何三項)
密碼長度：8-20字元
新學校密碼匙與舊密碼匙最少有兩個字元不同

(I) 資訊保安

- 如非必要，切勿使用公用電腦操作系統
- 若在特殊情況下須使用公用電腦操作系統，切勿設定自動儲存帳戶資料，並注意下載資料可能涉及的風險

(I) 資訊保安

- 可使用瀏覽器的**無痕式視窗**功能(啟用功能後，視窗不會儲存瀏覽記錄、**cookie**和曾在表單輸入的資料)

(I) 資訊保安

- 系統管理員設定時需要考慮的因素：
 - 設定為寬鬆的準則時，系統保安的憂慮
 - 設定為嚴謹的準則時，行政上的不便

(I) 資訊保安

- 請學校檢查 “sysadmin” 及 “asysadmin” 戶口及其他用戶的密碼到期日，並適時更改密碼

[S-SEC13-03] 設定 > 用戶資料

用戶類別	<input type="radio"/> 教職員 <input type="radio"/> 學生 <input type="radio"/> 家長 <input type="radio"/> 其他	
用戶代碼		
用戶名稱	sysadmin	
密碼到期	<input type="radio"/> 永不到期 <input checked="" type="radio"/> 密碼到期日 19/01/2019 (DD/MM/YYYY)	
英文用戶姓名	System Administrator	
中文用戶姓名	系統管理員	
使用語言	英文	
用戶存取時限		
*實際存取時限，會受「系統存取時限」的設定所影響		
星期一至六	24 小時	
星期日	24 小時	
用戶互聯網存取時限		
*實際互聯網存取時限，會受「在虛擬私人網絡外的互聯網存取時限」的設定所影響		
用戶到期	<input checked="" type="radio"/> 永不到期 <input type="radio"/> 用戶到期日 (DD/MM/YYYY)	
已編配用戶組	SCORE_CAPTURE_TEAM TSI_ADMIN SYSTEM_ADMIN	

- 授權 (Authorisation)
 - 嚴禁/預防教職員在未經許可下披露或取用系統的個人資料

- 授權 (Authorisation)
 - 小心計劃及設定各系統用戶及用戶組的權責
 - 經常檢視「用戶組」權責及編配用戶入組的設定

(I) 資訊保安

- 系統管理員對於WebSAMS中「預設」和「用戶設定」用戶組別內權限如何規劃
避免每人一組/所有人在同一組

(I) 資訊保安

- 紀錄 (Accounting)
 - 每天檢視「用戶不成功登入紀錄」，以便監察系統使用情況
 - [S-SEC09-06] 系統保安 > 報告及紀錄 > 報告

(I) 資訊保安

■ 紀錄 (Accounting)

- 經常檢視審計追蹤紀錄(audit trail) ，特別是「教職員資料」及「財務管理及策劃」的審計追蹤紀錄，留意不尋常的登入狀況，需要VPN登入才能查看
- [S-SEC21-01] 系統保安 > 報告及紀錄 > 教職員資料審計紀錄 > 檢視
- [S-SEC20-01] 系統保安 > 報告及紀錄 > 財務管理及策劃審計追蹤 > 檢視

紀錄 (Accounting)

[S-SEC21-01] 系統保安 > 報告及紀錄 > 教職員資料審計紀錄 > 檢視

檢視 庫存 刪除庫存檔案

審計追蹤類型

- ☒ 日常紀錄
☐ 編配入用戶組紀錄
☐ 存取控制紀錄

由
(DD/MM/YYYY)

23/01/2008



至
(DD/MM/YYYY)

13/03/2023



瀏覽

[S-SEC20-01] 系統保安 > 報告及紀錄 > 財務管理及策劃審計追蹤 > 檢視

檢視 庫存 刪除庫存檔案

審計追蹤類型

- ☒ 日常紀錄
☐ 編配入用戶組紀錄
☐ 存取控制紀錄

由
(DD/MM/YYYY)

08/02/2022



至
(DD/MM/YYYY)

08/02/2022



瀏覽

(I) 資訊保安

- 系統管理員對於審計追蹤及紀錄 (AUDIT TRAIL & LOG) 檔案保留或清理的考慮

審計追蹤及紀錄檔案容量控制	
儲存在資料庫的審計紀錄的容量上限(MB) [0 代表沒有限制, 預設值 : 1 MB]	<input type="text" value="0"/>
儲存在伺服器的庫存審計追蹤紀錄的容量上限(MB) [0 代表沒有限制, 預設值 : 1 MB]	<input type="text" value="0"/>
儲存在伺服器的資料庫備份/復原操作紀錄的容量上限 (MB) [0 代表沒有限制, 預設值 : 1 MB]	<input type="text" value="0"/>
儲存在伺服器的伺服器備份/復原操作紀錄的容量上限(MB) [0 代表沒有限制, 預設值 : 1 MB]	<input type="text" value="0"/>

▲最上

(I) 資訊保安

- 紀錄 (Accounting)
 - 伺服器日誌(server log)
 - 備份紀錄(backup log)
 - 防毒掃描紀錄(anti-virus log)

(I) 資訊保安

■ 審計 (Audit)

- 如有需要，進行系統保安檢查(SRAA)，以檢測系統保安漏洞

(II) 網絡保安

1. 如需要可設定 限制可使用WebSAMS時間
系統保安 > 設定 > 系統設定 > 在虛擬私人網絡外的系統存取時限，例如：學校網絡或互聯網

- ▶ 香港考評局程序
- ▶ 財務管理及策劃
- ▶ 學位分配
- ▶ 在職家庭及學生資助事務處(學)
- ▶ 報告管理
- ▶ 資料管理
- ▶ 資料選取工具
- ▶ 人才資料庫
- ▶ 時間表編排(網上版)
- ▶ 時間表編排(介面)
- ▶ 代碼管理
- ▼ 系統保安
 - 存取控制
 - 用戶組別
 - 特別組別

在虛擬私人網絡內的系統存取時限	
星期一至五 [預設值 : 0700-2300]	<input type="radio"/> 00 : 00 至 00 : 00 <input checked="" type="radio"/> 24 小時
星期六 [預設值 : 0700-2300]	<input type="radio"/> 00 : 00 至 00 : 00 <input checked="" type="radio"/> 24 小時
星期日 [預設值 : 0700-1800]	<input type="radio"/> 00 : 00 至 00 : 00 <input checked="" type="radio"/> 24 小時

在虛擬私人網絡外的系統存取時限, 例如：學校網絡或互聯網	
星期一至五 [預設值 : 0700-2300]	<input checked="" type="radio"/> 07 : 00 至 23 : 00 <input type="radio"/> 24 小時
星期六 [預設值 : 0700-2300]	<input checked="" type="radio"/> 07 : 00 至 23 : 00 <input type="radio"/> 24 小時
星期日 [預設值 : 0700-2300]	<input checked="" type="radio"/> 00 : 00 至 00 : 00 <input type="radio"/> 24 小時

(II) 網絡保安

2. 設定不同的互聯網存取時限給不同的用戶群組
系統保安 > 存取控制 > 互聯網存取時限概況

[S-SEC22-01] 系統保安 > 存取控制 > 互聯網存取時限概況

<input type="checkbox"/>	<u>互聯網存取時限概況</u> ▲	<u>概況說明</u>
<input type="checkbox"/>	PARENT	家長用戶的預設互聯網存取時限概況
<input type="checkbox"/>	STAFF_OR_OTHERS	教職員/其他用戶的預設互聯網存取時
<input type="checkbox"/>	STUDENT	學生的預設互聯網存取時限概況
<input type="checkbox"/>	STUDENT_Mon-Fri	STUDENT Mon-Fri ←

(II) 網絡保安

[S-SEC22-04] 系統保安 > 存取控制 > 互聯網存取時限概況 > 互聯網存取時限概況詳情

互聯網存取時限概況 編配用戶入概況

更改互聯網存取時限概況

互聯網存取時限概況

STUDENT_Mon-Fri

概況說明

STUDENT Mon-Fri

中文概況說明

<input type="checkbox"/>	星期	時限	時間
<input type="checkbox"/>	全部	由 (DD/MM/YYYY) <input type="text"/>  至 (DD/MM/YYYY) <input type="text"/> 	<input checked="" type="radio"/> 24 小時 <input type="radio"/> 00 ▾ : 00 ▾ 至 00 ▾ : 00 ▾
<input checked="" type="checkbox"/>	星期一至五	由 (DD/MM/YYYY) 25/02/2019  至 (DD/MM/YYYY) 31/08/2020 	<input checked="" type="radio"/> 24 小時 <input type="radio"/> 00 ▾ : 00 ▾ 至 00 ▾ : 00 ▾
<input type="checkbox"/>	星期六	由 (DD/MM/YYYY) <input type="text"/>  至 (DD/MM/YYYY) <input type="text"/> 	<input checked="" type="radio"/> 24 小時 <input type="radio"/> 00 ▾ : 00 ▾ 至 00 ▾ : 00 ▾
<input type="checkbox"/>	星期日	由 (DD/MM/YYYY) <input type="text"/>  至 (DD/MM/YYYY) <input type="text"/> 	<input checked="" type="radio"/> 24 小時 <input type="radio"/> 00 ▾ : 00 ▾ 至 00 ▾ : 00 ▾

 重設  儲存  返回前頁

備註：

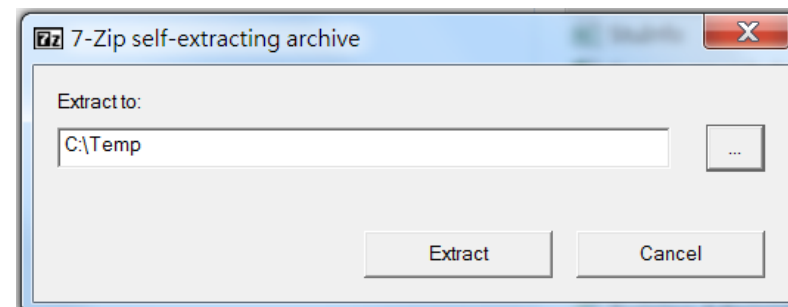
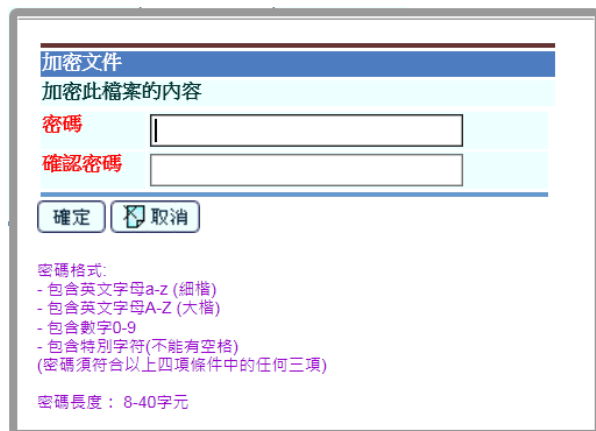
1. 互聯網存取時限概況長度：1-20 字母
2. 互聯網存取時限概況只能包含 a-z, A-Z, 0-9, "-" 或 "_"

■ 數據保安

- 使用**加密工具/功能**加密內含敏感資料的檔案 (例如使用BitLocker 加密 USB，使用MS Word和Excel的內置加密功能，或將檔案壓成加密zip檔)

數據保安

- 用戶從網上校管系統匯出資料並儲存於電腦或其他流動裝置時，須為檔案加密，以減低資料外洩風險。



(III)數據保安

數據保安

[S-SEC30-01] 系統保安 > 雲端服務管理 > 網上校管系統管理

下載資料庫備份

下載資料庫備份

下載


即時資料庫下載

由於網上校管系統存放的學生資料屬個人私隱資料，學校在收集、持有、處理或使用這些學生資料時，必須遵守《個人資料（私隱）條例》的規定。有關條例的詳細內容，學校可以瀏覽個人資料私隱專員公署網頁及由私隱公署發出的最新《資訊及通訊科技的保安措施指引》。

JBoss偵錯模式

JBoss偵錯模式

☒

 儲存

網上校管系統日誌

下載網上校管系統日誌

☐

傳送網上校管系統日誌至求助台

☒

案例號碼:

確定

培訓系統

培訓系統

停止

啟動培訓系統

☐

停止培訓系統

☐

備份當前培訓系統快照

☐

恢復早前備份的培訓系統快照

☐

執行

■ 數據保安

- 由於網上校管系統存放的教職員及學生資料屬個人私隱資料，學校在收集、持有、處理或使用這些個人資料時，必須遵守《個人資料（私隱）條例》的規定。有關條例的詳細內容，學校可以瀏覽個人資料私隱專員公署網頁。學校亦可掃描上述二維碼，以獲取最新資訊及通訊科技的資料保安措施指引。



(III)數據保安

- 在個人電腦上，更新防毒軟件及操作系統(OS)
 - 定期更新防毒軟件及執行整個操作系統防毒掃描 (full system scan)
 - 每月執行Windows update

■ 注意事項 1

需要經常審視、登入及檢查**重要用戶**或**擁有重要權限的用戶**，及每三個月至六個月更改密碼。

用戶

- sysadmin
- asysadmin

用戶組別

- SYSTEM_ADMIN
- SCHOOL_HEAD
- CS_ADMIN
- CS_SUPP

■ 注意事項 1

系統設有報告供學校查閱存取權限

- (R-SEC001) 用戶組別內用戶名單
- (R-SEC003) 用戶組別存取權限

■ 注意事項 2

- 當使用特別權限的使用時，不應進行常規活動包括但不限於閱讀電郵、瀏覽互聯網和下載檔案。
- 特別是高權限帳戶，應定期審計在系統的使用情況以確保這些帳戶是正確使用。

■ 注意事項 3

對需要使用WebSAMS的個人電腦，應注意以下事項

- 設定及開啟防火牆。
- 不應在工作站安裝及執行未獲授權軟件。
- 啓動即時偵測以掃描現行程式、執行程式及正在處理的檔案是否附帶惡意軟件。此外，根據操作需要定期對系統進行全面掃描。
- 在使用前，檢查儲存媒體上的任何檔案及經網絡收到的檔案是否附帶惡意軟件。
- 避免開啓可疑的電子訊息，不要點擊來源不可信任的位址連結，以免被引導至惡意網站。

■ 注意事項 3

- 在使用前，檢查附件及下載檔案是否附帶惡意軟件。
- 在安裝任何軟件前，先驗證軟件的完整性（例如比較校驗和值）及確保軟件並無附帶惡意軟件。在安裝任何執行程式 / 軟件（包括經電子訊息收到或自互聯網下載的執行程式 / 軟件）前，應先得到學校指定人員的批准。
- 應通過主硬磁碟啟動工作站。不應通過抽取式裝置啟動工作站。
- 切勿使用來源或源頭不明的儲存媒體和檔案，除非已檢查並清除儲存媒體和檔案上的惡意軟件。

■ 注意事項 4

對需要使用WebSAMS的瀏覽器，應注意以下事項

- 使用最新版本的瀏覽器，並安裝最新的保安修補程式。
- 關閉自動輸入密碼或密碼記憶功能。
- 除與可信任網站通訊外，啟動攔截彈出視窗功能。
- 定期刪除瀏覽器內的快取檔案或臨時檔案，以保障資料私隱。
- 關閉自動安裝外掛程式、附加元件或軟件的功能。

■ 注意事項 5

在WebSAMS下載的檔案及報告，不應長期儲存在流動裝置或抽取式媒體。在使用後應立即刪除或加密保護該檔案。

(四) 網上校管系統安全使用錦囊

(IV) 聯絡與支援

(IV) 聯絡與支援

- 經常瀏覽相關網頁，自我增值，檢視系統是否已符合保安要求
 - **政府資訊科技總監辦公室(OGCIO)網頁**
[<https://www.ogcio.gov.hk>]
[主頁>我們的工作>資訊及網絡安全]
 - **資訊安全網(InfoSec)**
[<https://www.infosec.gov.hk>]
 - **教育局網上校管系統資料庫(CDR)**
[<https://cdr.websams.edb.gov.hk>]
 - **教育局資訊科技教育(IT in Education)網頁**
[<https://www.edb.gov.hk>]
主頁 > 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 > 學校資訊保安建議措施(2019年9月修訂版)]



[← 返回](#)

網絡安全態勢認知

網絡安全態勢認知是指對網絡環境的威脅、其相關風險和影響，以及風險緩解措施是否充分的認識。對網絡安全具備敏銳觸覺有助企業和個人更深入了解相關漏洞，從而盡早採取適當的緩解措施。我們鼓勵業界和專業團體積極分享資訊，與本港和全球可信的持份者合作，適時分享網絡威脅的情報。

政府電腦保安事故協調中心發出的保安警報

最新警報

[...昔日警報](#)

20

一月

高危保安警報 (A20-01-05): Microsoft Internet Explorer 漏洞

Microsoft 發布了一個安全公告 (ADV200001) 以減低 Microsoft Internet Explorer 中 JScript.dll 的一個遠端執行程式碼漏洞的影響。

15

一月

保安警報 (A20-01-04): Oracle Java 及 Oracle 產品多個漏洞 (2020年1月)

Oracle 發布了重要修補程式更新公告，包括一系列應對 Java SE 和不同 Oracle 產品中多個漏洞的安全修補程式。

15

一月

高危保安警報 (A20-01-03): Microsoft 產品多個漏洞 (2020年1月)

Microsoft 發布了安全性更新以應對多個影響 Microsoft 產品或元件的多個漏洞。



資訊安全網
SEC

主頁

關於本網站

最新消息

消息及活動

宣傳及公眾教育

資訊保安

病毒及惡意程式碼

資訊保安自衛術

保護您的個人電腦

保護您的公司機構

電腦相關罪行

防範「仿冒詐騙」

技術參考資料

相關條例

公共服務

有用資源

詞彙表

English 繁體版 简体版

常見問題 搜尋: 去

字型大小: A A A

 一般使用者
  青少年及學生
  家長及老師
  資訊科技專業人員
  中小型企业

主頁 > 關於本網站  列印

關於本網站

「資訊安全網」網站的內容

資訊科技及互聯網的使用大幅增長，為我們帶來了極大的方便，但同時亦為犯罪分子製造了濫用有關科技的潛在危機。基於這虛擬領域的跨境、開放平台及高度互相連通的特性，電腦相關罪行實在影響深遠，故需有關各方的共同努力，才能有效地打擊這種罪行。

中華人民共和國香港特別行政區政府(以下簡稱為"政府")深切了解有關教育大眾資訊保安的重要性。這個「資訊安全網」旨在為社會大眾提供一個一站式的入門網站，讓市民有效地獲得資訊保安方面的資訊和資源，以及有關防止電腦相關罪行的措施和良好作業模式。

瀏覽「資訊安全網」

在「資訊安全網」中，你可以找到有關資訊保安的各項有用資料及資源，例如：最新資訊保安消息及活動、資訊保安技術文件及報告、近期仿冒詐騙攻擊、最新電腦病毒警告以及其他相關的資料。

你也可以找到一個互動式的指南，可以讓你簡易地查詢有關一般使用者、青少年及學生、家長及教師、資訊科技專業人員以及中小型企业使用資訊保安的相關文章。此外，「資訊安全網」還提供一個有效的搜尋器幫助搜尋網站內特定資訊和資源。

系統保安及系統事宜

主頁 > 系統保安及系統事宜

- 系統保安
- 系統操作
- 設備保養

參考文件



網上校管系統系統保安簡介及基本安全措施
WebSAMS Security Guide and Recommended Practice

中 英

WebSAMS System Operation Task List

英

System Security Setting Checklist for WebSAMS

英

如何使用WebSAMS系統保安設定檢查功能

中

系統保安模組 - 更改密碼的常見問題及答案

中

安裝網上校管系統的系統保安簡介

中

參考資料

主頁 > 參考資料

雲端服務計劃2019

雲端服務計劃2020

雲端服務計劃2022

雲端服務平台整合計劃



學校通訊模組訊息

2023年01月06日 網上校管系統「雲端服務平台整合計劃」學校遷移時段分配通知書

中

用戶手冊及指引

VPN連線程序指引 (VPN Connection Guide)

英

VPN 客戶端軟件 (VPN Client)

下載

承辦商雲端服務求助台用戶手冊

中

雲端服務管理頁面用戶手冊 (User Manual for Cloud Service Management Page)

中

Computer Operating Procedures Manual For School

英

常見問題及答案

中

簡介

本文件旨在供學校參考，以助學校在推行電子學習時保護其資料及資訊科技資產。學校有責任採取適當的資訊科技保安措施，以保護學校的資訊科技系統和數據。本文件為資訊科技保安提出建議做法，以供學校參考。學校可因應各自需要，採取適合其校情的做法。本文件所建議的做法並非詳盡無遺。學校可參考其他資訊科技保安措施，如本文件的第十二章「資訊科技保安的參考資料」，以保護資訊科技資產。

第一章	文件簡介	PDF
第二章	保安管理	PDF
第三章	保安事故處理	PDF
第四章	實體保安	PDF
第五章	接達控制	PDF
第六章	數據保安	PDF
第七章	網絡及通訊保安	PDF
第八章	網頁及網上應用程式保安	PDF
第九章	流動裝置與應用程式防護	PDF
第十章	惡意軟件的防護	PDF
第十一章	雲端服務	PDF
第十二章	資訊科技保安的參考資料	PDF

(IV) 聯絡與支援

- 推動用戶養成良好使用系統習慣
- 參加教育局、業界及資訊科技界所舉辦的培訓課程
- 積極推廣與資訊科技保安相關的活動

(IV) 聯絡與支援

- WebSAMS 求助台服務
 - 查詢模組設定及應用
- 網上校管系統(WebSAMS)學校聯絡主任(SLO)
 - 其他查詢

(IV) 聯絡與支援

■ WebSAMS資源

■ 網上校管系統資料庫CDR:

- <https://cdr.websams.edb.gov.hk>

■ WebSAMS用戶手冊:

- <https://cdr.websams.edb.gov.hk/模組資料/>
 - > 主頁 > 模組資料

(IV) 聯絡與支援

- 向學校聯絡主任(SLO)登記學校IP
瀏覽常用SQL 等資料
- <https://cdr.websams.edb.gov.hk> >
主頁 > 常用電話/電郵/地址 > 網上
校管系統學校聯絡主任名單及聯
絡方法

請注意，你現時未獲授權進入此網

如須下載最新系統文件，執行「系統」升級 / 「獨立版時間表編排工
料，請聯絡所屬的學校聯絡主任 (白里元「聯絡我們」為要)，並提供學校 IP
地址。

查找學校 IP 地址方法

登入學校網上校管系統伺服器，前往 <https://whatismyipaddress.com/> /
<https://www.whatismyip.com> 讀取網站所顯示的學校 IP 地址。

My IP Address Is:

IPv4: 203.██.██.██
IPv6: Not detected

My IP Information:

ISP: ████████
City: Central
Region: Central and Western District
Country: Hong Kong

Make My IP Address Private
[Click Here](#)

Click for more details
about 203.██.██.██

Location not accurate? [Update your IP location](#)

[Show Me More About My IP](#)

(IV) 聯絡與支援

■ WebSAMS資源

■ WebSAMS 討論區(香港教育城校管系統討論區)

- <https://forum.hkedcity.net/forumdisplay.php?fid=71>

■ WebSAMS 求助台服務

- 支援熱線: 2166-1150 傳真: 5801-1284
- 電郵: websams_support@ges.com.hk
- 請提供學校ID (School ID), 來電者名稱及聯絡電話

(五) 問答時間

Q&A