

WebSAMS Build Version Upgrade Release Note

WebSAMS Build Version Upgrade Package for **version 3.0.0.13112019** is now available for download at WebSAMS Download Site.

(URL: <http://www.websams.edb.gov.hk/eng/upgrade/Major3.html>).

A simple guideline on how to perform WebSAMS build version upgrade has been placed on the site for your reference.

(URL: http://www.websams.edb.gov.hk/eng/upgrade/doc/WebSAMS_Build_Version_Upgrade_v1.1.pdf).

Enhancements

Nil

Application User Manuals

Nil

The following problem reported has been resolved in this version

1. **SEC**
 - **Fix a vulnerability issue**

The following reports have been added / updated in this version:

Nil

Tips on safeguarding the security of WebSAMS

In order to safeguard the system security, schools are highly recommended conducting the following **important security risk assessment** regularly.

- 1) Ensure successful implementation of **WebSAMS backup** on a daily basis;
- 2) Perform scheduled virus scan and **update anti-virus** software regularly;
- 3) Check Unsuccessful Login Log to **monitor system** (WebSAMS & Windows) usage on a daily basis; and
- 4) Monitor and **block abnormal network traffic** (please consult your network vendor if necessary).

For more details, please refer to [WebSAMS Security Guide and Recommended Practice](#) at the WebSAMS Central Document Repository.

Housekeeping on WebSAMS build version upgrade

The minimum hard disk spaces required to run WebSAMS build version upgrade are:

D: 500MB

E: 1GB

Should you have any queries or need any assistance, please contact WebSAMS support @ 3125 8510, fax number 3125 8999 or email to websams_support@hk.ncs-i.com

Gentle Reminder to WebSAMS Users

With an aim to safeguarding the security of WebSAMS, schools are recommended to follow the guidelines of “Information Security in Schools – Recommended Practice” at the location of:

<https://www.edb.gov.hk/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/information-security/information-security-in-school.html>

Every item included in the IT Security in Schools – Recommended Practice (ITSS) is applicable to WebSAMS and essential for the establishment and maintenance of the IT Security Policy defined by every school.

Schools should install the Important Windows Updates (excluding the “Service Pack” and “Major Version Upgrade”) of Microsoft Windows Server 2012 R2 timely. Please refer to the “Doc 31 – WebSAMS Computer Operation Procedures Manual for School” at the following location for details:

<http://www.websams.edb.gov.hk/files/newschool/Other%20relevant%20information.zip>

In particular to the areas of password management and incident handling procedures, the followings are highlighted in order to assist schools to review their definition and enforcement:

- a) *All WebSAMS users are required to have their own identities, or user accounts, in order to access the system. Passwords should not be shared or divulged unless necessary. The risk of sharing passwords is that it would increase the probability of security being compromised. If individual user account is used and no password is shared, user activities on the system can thus be traceable and accountable to the corresponding person. Schools should also review their own IT security policy or practice to avoid password sharing of the WebSAMS user accounts.*
- b) *Schools should well define their own Security Incident Handling Procedures for IT Systems including WebSAMS and notify the right people accordingly.*

In order to ensure system and data security, schools are also recommended to refer to the “WebSAMS Security Guide and Recommended Practice” (<http://cdr.websams.edb.gov.hk/Files/Security/security.pdf>) and conduct checking of WebSAMS system security settings on a regular basis as well as a need basis by making good use of a) the Security Check function in WebSAMS; b) System Security Setting Checklist for WebSAMS. For details, please refer to the “Tips on using the Security Check function” and the “System Security Setting Checklist for WebSAMS” at the following locations:

<http://cdr.websams.edb.gov.hk/Files/Security/Tips%20on%20using%20the%20security%20check%20function.pdf>

[http://cdr.websams.edb.gov.hk/Files/Security/System%20Security%20Setting%20Checklist%20for%20WebSAMS%20\(in%20English%20version%20only\).pdf](http://cdr.websams.edb.gov.hk/Files/Security/System%20Security%20Setting%20Checklist%20for%20WebSAMS%20(in%20English%20version%20only).pdf)

Last but not least, WebSAMS users are recommended to regularly visit the Information Security website of HKSAR (<http://www.infosec.gov.hk>) for updated information of IT security.