



Information Technology Security

Scout Association of Hong Kong (“the Association”) attaches great importance to information technology security and personal data privacy protection. All Scout Units and members are responsible for the security of the Association’s electronic information to prevent any loss, leakage and misuse when using electronic information systems, computers and communication devices.

2. This circular sets out the principles and basic requirements of information technology security for the Association. All Scout Units and members must pay attention to and strictly comply with them when handling the Association’s electronic information in order that such information is properly managed and used in a secure manner.

Core Principles of Information Technology Security

3. When processing, transmitting and storing electronic information of or that related to Scout Units, the confidentiality, integrity and availability of the information must be secured in accordance with the following principles :

- Confidentiality : Set user accounts and access rights on a "need-to-know" basis in order to allow authorised access to the information concerned only.
- Integrity : Protect the accuracy, consistency and reliability of information from unauthorised changes.
- Availability : Ensure electronic information systems, computers and communication devices to operate fully and normally, enabling timely and reliable access to and use of information.

Personal Data Privacy

4. The Association’s Personal Data Privacy Policy Statement shall be observed when managing electronic personal information in Scouting events and daily operations. For details, please refer to the Policy Circular No. 11/2018 “Scout Association of Hong Kong Personal Data Privacy Policy Statement”.

Security Classification of Electronic Information

5. The Association’s electronic information is classified into the following four security levels and the corresponding information technology security measures have to be taken :

Security Level	Classification Principle	Example
Public	Applicable to information accessible by the public. Disclosure of such information should present no risk to the Association / Scout Unit.	General information on Scouting; policies, guidelines, circulars and statistics published on the Association's website
Internal	Applicable to information for internal reference by designated members of the Association and non-sensitive operational information shared with partners. Disclosure of such information may lead to an adverse impact at moderate level but does not cause serious harm to the Association / Scout Unit.	Training materials, member handbooks, internal policies and operational procedures
Restricted	Applicable to sensitive information that is intended for use by specific group of authorised persons. Unauthorised disclosure, modification or destruction of such information may cause inconvenience to members, adversely affect the operation of the Association / Scout Unit, and even result in certain level of financial loss or damage to the reputation of the Association / Scout Unit.	Members' personal information and scouting records (e.g. date of birth, phone number, address, training record); tendering documents and records
Confidential	Applicable to information that is very sensitive in nature and is strictly restricted. Such information is critical to the operation of the Association / Scout Unit. Loss, damage or unauthorised disclosure of information may cause a significant adverse impact on the reputation and operation of the Association / Scout Unit, and cause inconvenience, threat or loss to data subjects (i.e. those persons to whom the personal information concerned belongs to).	Members' sensitive personal information (e.g. Hong Kong Birth Certificate / Hong Kong Identity Card number); sensitive management information of the Association / Scout Unit

6. The system / information owners in the Association are responsible for classifying the electronic information they own into the appropriate security levels and grant the corresponding access right to suitable persons on a “need-to-know” basis. In general, if the information is at “Internal”, “Restricted” or “Confidential” security level, the system / information owners must display clearly the security level in an appropriate location of the information in order to remind the users of taking the corresponding security measures.

User Responsibility

7. In handling information using computers, the Internet, email, instant messaging apps, etc., users should ensure the environment is not subject to security risk and make effort to protect the security and privacy of information (including but not limited to personal data). Users should also maintain information technology security habits and alertness at all times, and pay attention to the latest security news to fulfill their responsibilities. The Annex to this circular provides lists of common “DO's” and “DON'Ts” in information technology security on the use of electronic information systems for all Scout Units and members to read and follow.

Enquiries and Support

8. To further understand the contents of this circular, please enquire through the following email address :

Region / Branch & Subsidiary	Email Address
Hong Kong Island Region	it_enquiry@hkirscout.org.hk
Kowloon Region	kritadmin@krscout.org
East Kowloon Region	it@hkscout-ekr.org
New Territories Region	ntrscout.it@gmail.com
New Territories East Region	it.nterscout.official@gmail.com
Branch & Subsidiary	itoffice@scout.org.hk

9. In case of information technology security incident requiring special support, contact can also be made to the Information Technology Office directly (Tel: 2957 6433, Email: itoffice@scout.org.hk).



Desmond SAM
Assistant Chief Commissioner (Support)

Common DOs and DON'Ts in information technology security on the use of electronic information systems

A. Use of computers and mobile devices

DOs	DON'Ts
<p>(i) Install and properly configure anti-virus software, regularly update virus definition files, and schedule automatic scanning.</p> <p>(ii) Regularly update the operating system and software to fix security vulnerabilities.</p> <p>(iii) Use a personal firewall for network traffic control to reduce the risk of being hacked or attacked.</p> <p>(iv) Personal accounts should be protected by password or other means of authentication to prevent others from using the device with your personal account.</p> <p>(v) If sensitive information is managed on the Unit's computers, the Unit should set up individual member accounts for use as needed. Members should also completely remove the relevant files after use (including cleaning up the "recycling bin" on the computer).</p> <p>(vi) Portable storage devices should be under safe custody to avoid loss, and protection by encryption software¹ and password to ensure the stored information is only accessible by authorised persons.</p> <p>(vii) Make regular backups, especially before major system or software installation / upgrade, or hardware repair. Backup copy can support data recovery to minimise data loss in the event of virus infection, hacking or hardware failure.</p>	<p>(i) Do not use files obtained from other parties directly and they must be scanned by anti-virus software before use.</p> <p>(ii) Do not use software from unknown sources or not officially authorised.</p> <p>(iii) Do not use administrator account for daily operations to prevent malicious software from installing itself with administrator privileges.</p> <p>(iv) Do not leave logged-in account unattended. No matter how long the leave is, screen lock, log-off or shut down should be adopted before leave.</p> <p>(v) Do not use public computer or public account of the Unit's computers to manage sensitive information.</p> <p>(vi) Mobile devices should not be left unattended in public places to prevent from being stolen.</p> <p>(vii) Computers or mobile devices should not be sent for repair or disposal without removing the storage unit in order to prevent any theft of stored information. For repair or disposal of storage unit, all stored information should be completely and permanently removed² beforehand.</p>

¹ Encryption software includes Bitlocker of Windows Platform, FileVault of MAC platform, etc.

² e.g. DBAN for harddisk data removal (www.dban.org) or FileShredder for file deletion (www.fileshreder.org)

B. Management of electronic system accounts and passwords

DOs	DON'Ts
<p>(i) Use a complex password consisting of a combination of at least eight numbers, letters and symbols, or set the password based on the requirements prompted by the website.</p> <p>(ii) Two-factor authentication should be used to enhance security where available.</p> <p>(iii) Change password regularly and keep it safe.</p>	<p>(i) Passwords should not be set using birthday date, user name, phone number, common words, etc.</p> <p>(ii) Do not disclose personal accounts and passwords to others, and do not share system accounts.</p> <p>(iii) Do not use the same password on different systems.</p>

C. Use of Internet and set-up of website / social media accounts

DOs	DON'Ts
<p>(i) When browsing websites which contain sensitive information or handling scouting matters through web systems (such as membership systems, emails, social media, etc.), make sure the website is enabled with encrypted transmission protection (i.e. web address preceded by "https").</p> <p>(ii) Encrypted transmission protection should also be adopted to provide users with a secure browsing environment when setting up a Unit's website.</p> <p>(iii) Beware of websites that prompt for personal information to protect personal data privacy.</p> <p>(iv) The Unit's internal wireless network (Wi-Fi) should be protected with password (e.g. WPA2) to secure data transmission. If a public Wi-Fi is made available to non-members, it should be set up separately and isolated from the Unit's internal Wi-Fi.</p>	<p>(i) Websites / social media accounts of obsolete Units / activities should not be retained and should be removed after backup (if required).</p> <p>(ii) The web administrator account should not be shared with third party. If such information has to be given to service provider for troubleshooting purpose, the password should be changed before and after the troubleshooting to ensure the security of system and data.</p> <p>(iii) No web account login and password should be kept on a non-private computer.</p> <p>(iv) Do not visit suspicious websites or download software / files from unknown sources.</p>

D. Use of cloud storage, email and instant messaging apps³

DOs	DON'Ts
<p>(i) When storing and sharing sensitive information with cloud storage, the share permission should be granted to particular users (e.g. authorised by email accounts) and no one who has the shared link would be allowed to view / edit.</p> <p>(ii) When sending information through email or instant messaging apps (especially sensitive information is involved), “need-to-know” basis should be adopted.</p> <p>(iii) Personal information (e.g. contact phone numbers, email addresses) of participants for completed events should be removed from cloud storage, email accounts and instant messaging apps.</p>	<p>(i) Do not transmit sensitive information through email or instant messaging apps. If such information has to be sent, it should be in the form of a file with encryption⁴ while the decryption password should be sent to the recipients via other channels.</p> <p>(ii) Attachments and hyperlinks in suspicious emails should not be opened. When in doubt, check with the sender.</p> <p>(iii) Personal information such as contact phone numbers or email addresses should not be disclosed without the explicit consent of the individuals concerned⁵.</p>

³ Instant messaging app examples : WhatsApp / LINE / WeChat / Telegram / Facebook Messenger

⁴ e.g. Use of Microsoft Office password encryption or 7-ZIP AES256 password encryption

⁵ Use of bcc in email, broadcast function in WhatsApp, etc. may help avoid unnecessary disclosure of personal data.