**Scout Association of Hong Kong**
**Standing Circular**
Tel：2957 6433 Fax：2302 1001 Email: it@scout.org.hk

**1 October 2023**
**Circular No. 02/2023**
[Policy]

# Information Technology Security

This Circular supersedes Policy Circular No. 03/2019 issued on 15 December 2019.

2. 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 information systems, computers and mobile devices.

3. This circular sets out the Association's principles and basic requirements on information technology security. 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

4. 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 information systems, computers and mobile devices to operate fully and normally, enabling timely and reliable access to and use of information.

## Personal Data Privacy

5. 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

6. 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 |

7. 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**

8. Scout Units and members may from time to time use computers, information systems, the Internet, email, social media, instant messaging apps, cloud storage, etc. to handle and share their information. They must 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) through :

(a) Ensuring proper security and privacy settings.

(b) Sharing personal and/or sensitive information with trusted and authorised persons on a "need-to-know" basis only.

(c) Staying vigilance against suspicious / unsolicited electronic messages and frauds.

(d) Verifying sender's identity of suspicious / unsolicited electronic messages through alternative means such as phone call.

(e) Confirming the authenticity, credibility and security of electronic messages, attachments, hyperlinks or QR codes before giving any response or taking any action.

(f) Reporting suspicious activities and incidents to the responsible Scout Unit or information technology support team.

(g) Seeking professional assistance to deal with situations where important information has been stolen or defrauded in order to reduce losses and properly carry out remedial work.

9. 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 information systems for all Scout Units and members to read and follow.

10.

**Enquiries and Support**

10. 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 | it@scout.org.hk |

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

Desmond SAM
Assistant Chief Commissioner
(Information Technology and 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 |
|---|---|
| (i) Install and properly configure anti-virus software, regularly update virus definition files, and schedule automatic scanning. | (i) Do not use files obtained from other parties directly and they must be scanned by anti-virus software before use. |
| (ii) Regularly update the operating system and software to fix security vulnerabilities. | (ii) Do not use software from unknown sources or not officially authorised. |
| (iii) Use a personal firewall for network traffic control to reduce the risk of being hacked or attacked. | (iii) Do not use administrator account for daily operations to prevent malicious software from installing itself with administrator privileges. |
| (iv) Personal accounts should be protected by password or other means of authentication to prevent others from using the device with your personal account. | (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. |
| (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). | (v) Do not use public computer or public account of the Unit's computers to manage sensitive information. |
| (vi) Portable storage devices should be under safe custody to avoid loss, and protection by encryption software[1] and password to ensure the stored information is only accessible by authorised persons. | (vi) Mobile devices should not be left unattended in public places to prevent from being stolen. |
| (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. | (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 removed[2] beforehand. |

[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.fileshredder.org)

## B. Management of information system accounts and passwords

| DOs | DON'Ts |
|---|---|
| (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.<br>(ii) Two-factor authentication should be used to enhance security where available.<br>(iii) Change password regularly and keep it safe. | (i) Passwords should not be set using birthday date, user name, phone number, common words, etc.<br>(ii) Do not disclose personal accounts and passwords to others, and do not share system accounts.<br>(iii) Do not use the same password on different systems. |

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

| DOs | DON'Ts |
|---|---|
| (i) When browsing websites which contain sensitive information or handling Scouting matters through web systems (e.g. membership systems, emails, social media, etc.), make sure the website is enabled with encrypted transmission protection (i.e. web address preceded by "https").<br>(ii) Encrypted transmission protection should also be adopted to provide users with a secure browsing environment when setting up a Unit's website.<br>(iii) Beware of websites that prompt for personal information to protect personal data privacy.<br>(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. | (i) Website / social media accounts of obsolete Units / activities should not be retained and should be removed after backup (if required).<br>(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.<br>(iii) No sensitive information (e.g. web account login and password) should be kept on non-private computers and mobile devices.<br>(iv) Do not visit suspicious websites or download software / files from unknown sources. |

## D. Use of cloud storage, email and instant messaging apps[3]

| DOs | DON'Ts |
|---|---|
| (i) When keeping and sharing sensitive information with cloud storage, the permission should only be granted to designated users (e.g. authorised by email accounts) and no one who has the shared link would be allowed to view / edit. | (i) Do not transmit casually 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 encryption [4] while the decryption password should be sent to the recipients via other channels. |
| (ii) When sending information through email or instant messaging apps (especially sensitive information is involved), "need-to-know" basis should be adopted. | (ii) Do not respond casually to suspicious / unsolicited electronic messages that may contain malicious attachments, hyperlinks or QR codes. When in doubt, check with the sender. |
| (iii) Sensitive information (e.g. participants' contact phone numbers, email addresses, etc.) of participants for completed events should be removed from cloud storage, email accounts and instant messaging apps. | (iii) Personal information such as contact phone numbers or email addresses should not be disclosed without the explicit consent of the individuals concerned[5]. |

[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.