The Hong Kong Air Cadet Corps
IT Policies & Guidelines

Introduction

The HKACC IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the organization which must be followed by all staffs and members. It also provides guidelines ITSU will use to administer these policies, with the correct procedure to follow.

ITSU will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all staffs and members.

Ownership of IT Resources

1. All IT resources purchased by ITSU are regarded as the organization property.
2. All software developed by staffs or members is regarded as exclusive intellectual property of the organization.
3. All data and information residing on the organization IT facilities are regarded as exclusive property of the organization.

The Organization Rights on IT Resources

For security enforcement, ITSU reserves the rights

1. To monitor all information flow within the Corps IT network, including emails
2. To disclose information hence discovered to regulatory authorities if required.

Provisioning of IT Resources

1. All IT assets are HKACC assets and managed by ITSU
2. ITSU will be responsible for all IT asset purchase evaluation, approval, tracking, maintenance, redeployment and retirement
3. Wing HQ and HQ staffs should raise Service Request to ITSU for any need of IT equipment, including hardware and software. ITSU will evaluate request and recommend the possible and feasible IT solution. ITSU will provision the equipment accordingly, either through new acquisition or redeployment of existing equipment.

User Responsibility

Protection of IT Resources

1. Wing HQ and HQ staffs are responsible for the protection of IT resources assigned or regularly used by him or her.
2. Wing HQ and HQ staffs are required to take appropriate steps
    a. To minimize possibility of theft, damage, or loss
    b. To protect the integrity of computer application and data
    c. To maintain the equipment in a tidy and clean condition
    d. To ensure information and data are properly protected according to the HKACC information Security Policy

Use of Legal Software

1. Wing HQ and HQ Staffs shall only use software according to its license agreement.
2. Wing HQ and HQ Staffs are not allowed to install software on Corps' PCs without the proper corresponding license

Protection against Computer Virus

1. All ITSU provided personal computer are equipped proper anti-virus software for the proper protection of the healthiness of the HKACC IT environment
2. Wing HQ and HQ Staffs should not disable or deactivate the anti-virus software without prior approval from ITSU
3. Wing HQ and HQ Staffs should report malfunctioning of anti-virus software, it notice, to ITSU following the normal fault reporting procedure

Personal Data (Privacy) on IT Systems

1. Personal data being stored on IT systems are subjected to the same controls as that stored in other forms. Access to personal data stored on IT systems is restricted to specific functional roles for justifiable operation purpose only.
2. Disclosure of personal data without the consent from the data subject is forbidden.

Information Technology Security

Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through {insert relevant security measure here, such as keypad, lock etc.}

It will be the responsibility of ITSU Officers to ensure that this requirement is followed at all times. Any staffs or members becoming aware of a breach to this security requirement is obliged to notify OC ITSU immediately.

All security and safety of all technology, such as desktops will be the responsibility of the staff or member who has been issued with the desktop. Each staff or member is required to use passwords and to ensure the asset is kept safely at all times to protect the security of the asset assigned to them.

Information Security

All Corps member's relevant data is to be backed-up.

It is the responsibility of ITSU Officers to ensure that data back-ups are conducted daily and the backed up data is kept in the NAS hard-drive and offsite in the data center.

All technology that has internet access must have anti-virus software installed. It is the responsibility of ITSU Officers to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

All information used within the organization is to adhere to the privacy laws and the organization's confidentiality requirements. Any staff or member breaching this will be reported to senior management for disciplinary action.

IT Service Agreements

All IT service agreements must be reviewed by ITSU Officers before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by the Commanding Officer.

All IT service agreements, obligations and renewals must be recorded by HQ.

Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorised by Commanding Officer.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, OC ITSU should review and recommended before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Commanding Officer.

In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to OC ITSU who will be responsible for the settlement of such dispute.

IT Hardware Failure

Where there is failure of any of the organization's hardware, this must be referred to ITSU Officers immediately.

It is the responsibility of ITSU Officers to investigate and report the situation to senior management in the event of IT hardware failure.

It is the responsibility of ITSU Officers to undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimise disruption to the organization operations.

Point of Sale Disruptions

In the event that point of sale (POS) system is disrupted, the following actions must be immediately undertaken:

- POS provider to be notified
- ITSU Officers must be notified immediately
- For all manual POS transactions, member's signatures must be verified

Virus or other security breach

In the event that the organization's information technology is compromised by software virus or ransom email such breaches are to be reported to ITSU immediately.

ITSU Officers are responsible for ensuring that any security breach is dealt with within 3 days to minimise disruption to the organization operations.

Website Disruption

In the event that business website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified
- ITSU Officers must be notified immediately

Email Usage

1. The organization email is provided for all adult members with posts.
2. Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation soliciting for illegal pyramid schemes and computer tampering (e.g. spread of computer viruses) are strictly prohibited.
3. All email addresses, associated accounts and work related emails are the property of HKACC.
4. ITSU reserves the right to access the content of messages in connecting with a properly authorized investigation, to meet legal or statutory requirements or to enable the operation to continue.
5. Before forwarding messages – whether externally or internally – staff and members should consider whether the transmission of the information would breach the privacy of an individual or infringe copyright or breach the confidentiality of any business agreement.
6. Automatic forwarding of all emails communications to “external email accounts” (ie. Personal email account) is a MUST.
7. When a staff or member leaves the organization, ITSU reserves the right to wipe the data in the staff’s desktop.

IT Asset Disposition

Disposal of computer hardware is both of environmental and information security concern.

1. IT asset write off must obtain the approval of the Commanding Officer
2. Disposal must be made through government approved handling agents.
3. Sensitive/Highly Sensitive information on storage media must be properly erased to ensure it cannot be reconstituted before disposal.
4. ITSU will be responsible for disposing unnecessary hardware IT asset
5. IT equipment no longer in need should be return to ITSU for redeployment or disposal

Password Policy

1. Staffs and members should never disclose their password to anyone.
2. Sufficient strong password should be used – avoid use of common words, acronyms, names, birth date, phone, etc.
3. All computer systems should enforce password requirements specified by ITSU, i.e password length, characters combination, etc., where technology is available and the solution is practical.

Current Password Requirements

The organization requires that users adhere to the following guidelines on password construction:

	Network / Desktop / Laptop	**Members Mobile Email Account**
Password Minimum Length	10	10
Password Combination	Must comprise of characters from 4 of the following sets: - Upper Case - Lower Case - Numeric - Special Characters	Must comprise of characters from 4 of the following sets: - Upper Case - Lower Case - Numeric - Special Characters