GDM Circular 1/2010

Circular :

Information, Communication & Technology Best Practices

(Version 1.0)

Prepared By :

Geospatial Development Management Section
Survey Division
Lands and Surveys Department Sabah
January 2010

Foreword

This circular is a compilation works over a period of time. The resources for ICT Best Practises are many and we have decided to focus on those being implemented in Malaysia, we have read the recommendations and circulars given by MAMPU, My.CERT, SG.CERT, UKIT and JPKN. This compilation is a summary of all the good practises that we should have when we make use of ICT to do our work. For more details of the Best Practises, you may visit any of the ICT websites that provide more detailed some guidelines and tips.

In this modern age, ICT is a just tool to carry out our daily work and hence we need have to be knowledgeable on how to take care of our tool. Just like how the carpenter will spend time and effort to sharpen his saws and tools before beginning a day of carpentry work, likewise, in this age, it is expected of us when we login to the department network, that we spend time to ensure that our ICT tool is updated with antivirus patterns and that our email accounts do not spam others. In so doing we hope that that we do not burden others by our lack of knowledge when we spread 'virus' and 'worms' to our colleague.

Please bear in mind that Computer Crimes Act 1997 is already enforced in Malaysia. Any failure on our part to observe the ICT Best Practises may result in a breach of the Act and is chargeable in courts of Malaysia. You are hereby advised to read and be familiar with the ICT Best Practises,

Director of Lands and Surveys
Lands and Surveys Department Sabah

Do's and Don'ts

Don'ts

Don't access obscene material or material that could offend others.

Don’t write down or store password electronically.

Don't let anyone else use your log in accounts or tell anyone your login in password.

Don't download videos or music that's copyrighted by others.

Don't use ICT facilities to offend or harass other people.

Don’t use ICT facilities to hack or scan other machines.

Don't install unlicensed or malicious software.

Don't use ICT facilities to advertise goods or services.

Do's

Log out of computer systems when you have finished using them.

Do look after the computer and other ICT equipments under your care properly.

Do backup your files regularly.

Do keep one set of important data outside the office.

Do check your antivirus regularly and make sure its virus definition pattern updated and running.

ICT Environment

Users should be aware and practice the following to ensure a reliable computing environment.

I. Neither food nor beverages are permitted near computer terminals, and ICT equipments.

II. Ensure that the UPS and/or Power Regulator connecting to the computer and peripheral equipment (printers, monitor, plotters, scanners and etc) is always turned on.

III. Refrain from using pen drive for long periods of time or as permanent storage and backup, as this device is meant for transporting and sharing files only.

IV. Ensure that the computer and peripheral equipment (printers, monitor, plotters, scanners and etc) are adequately ventilated.

V. Ensure that the office is pest-free zone by practising high-standard of hygiene, ensure dustbin are not placed next to the ICT equipments and that the office has Pest Control service frequently.

General ICT Usage

I. All computers are to be used in a responsible, efficient, ethical and legal manner. Any attempt to hack into the Department computer system is regarded as a criminal act and will be liable to disciplinary actions.

II. Users should report any software/hardware fault to Unit Sokongan IT, Geospatial Development Management Section as soon as possible.

III. Users should report suspected abuse, especially any damage to or problems with their files.

IV. Users should not copy files from and/or write files onto other's computer Without prior consent.

V. Users should not install unlicensed software.

VI. Users should shut down the computers properly i.e not shutting down computers by simply pressing the 'ON/OFF' button.

VII. In the event of power failure which the UPS will be activated and provide power supply for a limited period of time, users should save all their work before shutting the computers down properly as mentioned in VI.

VIII. Log off computers when you have finished using them.

IX. Lock your screen (using CTRL+ALT+DEL) if you are leaving your computer unattended for a some time.

Antivirus Management

I. All users should be aware that the official antivirus for government computers is **TrendMicro**.

II. Users must ensure that their computers are installed with the antivirus.

III. Users must ensure that the antivirus always stay connected by pointing the cursor over the antivirus icon and checking its status.

IV. It is the responsibility of Unit Sokongan IT to ensure that the antivirus on every computer is pointing to the correct server for updating of latest antivirus definition pattern.

V. Users must contact Unit Sokongan IT whenever the antivirus status is found **'disconnected'**.

VI. Users should always remember that they are not allowed to uninstall the antivirus.

Access to ICT facilities

I. Users may only access those services or parts of the computer systems/applications he or she is given access to.

II. Users must not attempt in any manner to access unauthorised computer systems/applications in the Department's Local Area Network or the WIFI network.

III. For headquarters users, they must ensure they log on to ‘JTUHQ’ domain to enable IPs to be assigned to their computers as follows :-
Username :
Password :
Domain : JTUHQ

IV. For other outstation offices, users must ensure that they log on to the domain with the username and password that is assigned to them.

V. Users must not install Access Points within Wisma Tanah & Ukur or in any of the oustation offices illegally.

VI. Users must not access others’ computers without prior consent.

VII. Always contact Unit Sokongan IT whenever users have difficulties logging on the domain.

Email Usage

I. Email usage is free for all users. For JTU staff, we have two accounts :- Ali.Ahmad@jtu.sabah.gov.my and Ali.Ahmad@sabah.gov.my. However, for official correspondence, users should use their official email accounts eg. **Ali.Ahmad@sabah.gov.my**

II. Users must exercise care when sending an email as the email messages sent become the possession of the receiver which can easily be redistributed.

III. Always double-check the addresses of your intended recipients to avoid the email messages being sent to the wrong recipients.

IV. Never send or forward chain email as it may result in ‘spamming’ which is a waste of computing resources and a nuisance and often offends recipients.

V. Don't pass on unconfirmed rumours especially about viruses because they often only cause needless panic.

VI. Do not send emails of obscene nature i.e containing obscene messages and/or pictures/movie clips.

VII. Do not open files with **.exe** extension as they can be viruses.

VIII. Delete messages that should not be preserved.

IX. Do not share your email passwords with others.

Internet Usage

I. Do not visit sites featuring pornography, terrorism, espionage, theft or drugs, inciting racial hatred or disharmony.

II. Do not engage in online gambling or any other activity in violation of the laws of the Country.

III. Do not conduct unauthorised business.

IV. Do not engage in online subversive activities against the Government.

V. Facebooks may be used but only during stipulated period of time as set forth in the access policy.

VI. Do not propagate deliberately any virus.

VII. Some downloading sites have been blocked by firewall. Do not download programs which will significantly degrade the performance of the Internet facilities.

VIII. Do not send inappropriate email to large numbers of people, via the Internet as this will also degrade the performance of the Internet facilities.

Password Usage

I. Do not write down or store password electronically.

II. Do not hint password to anyone. (e.g. “my family name”, “my pet’s name”, etc.)

III. Do not reveal password in any manner (e.g. over phone, SMS, email, messenger, questionnaires / security forms, etc) to anyone.

IV. Do not enable “Remember Password” feature of applications (e.g. Internet Explorer, Firefox, Opera, Messenger, Netscape, Eudora, Outlook etc.)

V. **A password must be :**

a. at least 8 characters in length.

b. a combination of upper and lower-case alphabets, numbers and special characters.

c. NOT the same as or similar to any personal information of user.

d. NOT a word in any dictionary, language and jargon.

Combination of password may include:

a. Upper case: A – Z

b. Lower case: a – z

c. Numbers: 0 – 9

d. Special characters: ~!@#$%^&*()_+<>?;:[]\

Examples of weak passwords:

a. Names of family, pets, friends, co-workers

b. Computer terms and names, sites, companies, hardware, software

c. Birthday, addresses, phone numbers, car plate number

VI. Always change any new password received immediately upon the first login.

VII. Always change password immediately when suspected of being compromised.

VIII. Always change password at least once in every 6 months.

IX. The same password must never be used more than once.

Backup & Restoration

I. All work related data in any computer must be backup.

II. For standalone computers, network computer, workstations and servers, always backup important data on Pen-Drive, CD, magnetic tapes, external Hard Disk and/or copy important data to the file server.

III. Backup important data daily and weekly.

IV. Keep daily backup on-site.

V. For servers, keep one copy of weekly backup on-site for restoration and the other for off-site safe keeping.

VI. For Headquarters, off-site safe keeping is at Inanam Training School.

VII. All backups must be verified to be restorable.

VIII. All backups must be adequately and appropriately labelled.

Sepuluh Perintah untuk Etika Komputer

1. Jangan menggunakan komputer untuk membahayakan orang lain.
2. Jangan mencampuri pekerjaan komputer orang lain.
3. Jangan mengintip file orang lain.
4. Jangan menggunakan komputer untuk mencuri.
5. Jangan menggunakan komputer untuk bersaksi dusta.
6. Jangan menggunakan sumber daya komputer orang lain tanpa izin.
7. Jangan mengambil hasil intelektual orang lain untuk diri sendiri.
8. Fikirkanlah mengenai akibat sosial dari program yang anda tulis.
9. Bantulah mereka yang memerlukan tunjuk ajar dalam penggunaan komputer.
10. Gunakanlah komputer dengan rasa penghargaan.