Acceptable Use Policy (AUP) for Information Technology (IT) Resources

A. Purpose and scope

SIT's IT resources are extensively used by students, faculty, staff and authorised users who are expressly approved by CIT Division ("IT users" or "Users"). This policy is intended to prescribe the appropriate usage behaviour of IT users.

Usage of IT resources includes but is not limited to any access to, monitoring, usage, alteration, modification, adaptation or duplication of SIT IT resources, i.e. any IT-related facilities, services, equipment, network, communications, setup, hardware, software, programs, files, information and/or data.

Revisions to the AUP may be promulgated from time to time; IT users must consult and comply with the latest AUP available at: https://aup.singaporetech.edu.sg/File/SIT_ITPolicy.pdf

SIT may impose penalties, initiate disciplinary procedures or pursue legal actions against IT users who violate the AUP.

IT users are reminded that unauthorized access to or abuse of IT resources, may result in criminal offences under various statutory acts, in particular, Computer Misuse and Cybersecurity Act (Cap 50A, Revised Edition 2007) and the Penal Code (Cap. 224, Revised Edition 2008).

The AUP is set out below.

B. General

1. Users are to use only SIT IT resources authorised for their individual use.

2. Users are to use SIT IT resources only for legitimate work-related activities. IT users shall not use SIT IT resources for any commercial purposes or personal gain, unless specific activities are duly authorised by SIT in writing.

3. Users are to use SIT's computing and communicating facilities in a manner which is not detrimental to the reputation of SIT. For example, Users are to refrain from using SIT systems or devices for anything that is confidential, provocative, distasteful, fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or which incites religious or racial intolerance onto the local or international bulletin boards, the World-Wide-Web, and Internet communication channels.

4. Users are to respect the integrity of computing systems and data. For example, they are to refrain from intentionally developing programs or making use of already existing programs, with or without modification, to harass other users, infiltrate a computer or computing system, damage or alter the software components of a computer or computing system, or to gain unauthorized access to other facilities accessible via the network.

5. Users are to respect the rights and privacy of others by not accessing another user's files without proper and appropriate permission, and not tampering with their files, passwords or accounts, or falsely impersonating another user when e-mailing, messaging, conferencing or using any other kind of communications.

6. Users who have access to personal data (i.e. data, whether true or not, about an individual who can be identified from that data or from that data and other information which an organisation has or is likely to have access) in the care, custody, control and possession of SIT in the course of using any of SIT's IT resources are to comply with the Personal Data Protection Act 2012. Users are to protect personal data in their possession or control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, taking into consideration the nature of the Personal Data, the form in which the Personal Data has been collected, and the possible impact to the individual if an unauthorised person obtained, modified or disposed of the Personal Data. Users should refer to the Employee Policy on Handling Personal Data issued by SIT's Data Protection Officers and as may be updated from time to time for more information on compliance with the Personal Data Protection Act 2012.

7. Users are not to use SIT's computing facilities for any unlawful purposes. This would include but not be limited to, vice, gambling or other immoral or criminal purpose whatsoever or for sending to or receiving from any user or site any message which is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or which incites religious or racial intolerance.

8. Users are not to install or remove parts from SIT IT resources without prior authorisation from the CIT department.

9. Users are to seek approval from the CIT department on the use of software and hardware, such as diagnostic and vulnerability scanning tools, which can be used to compromise the security of the SIT systems.

10. Users shall NOT engage in any of the following activities:

    a. accessing unauthorized data or applications

    b. masquerading as another user

    c. attempting to circumvent security systems

    d. attempting to exploit or probe for security loop holes in SIT's network or other organization networks

    e. attempting to attack or to degrade the performance of SIT's network or that of other organizations

    f. colluding with other users to cause damage to SIT's network or systems

11. Users shall log off or enable password protected screen lock when they are not attending to their personal computers (PCs) to prevent unauthorized access to their computers.

12. All IT security incidents shall be reported to the IT HelpDesk.

13. Users shall use SIT furnished computers and any non-connected or connected peripherals for official purposes only.

C. Computer Accounts and Passwords

1. Users shall use only their computer accounts which each is duly authorized for use. Users shall not give or carelessly or negligently allow any other user access to his/her computer account or any computer account which does not belong to him/her. Users shall not publicize the details of their computer accounts or passwords.

2. Users shall not attempt to tailgate, crack, guess and/or capture another user's computer passwords or personal identification numbers (PINs).

3. Users shall be required to change his/her initial passwords on a minimum period basis. Passwords need to be at least 8 characters in length, without leading or trailing blanks; and alphanumeric in nature, with at least one uppercase character, one lowercase character and one numeric character.

4. Users who are granted [1]privileged rights shall
   a. exercise due diligence to keep their user IDs and password safe and secure.
   b. be responsible for protecting SIT's information from unauthorized access, modification, duplication, destruction, or disclosure whether accidental or intentional.
   c. be accountable for their SIT-issued computers, including all computing activities originating from and ending at their computers.

D. Computer Viruses

1. Users shall not write or deliberately or carelessly spread computer viruses and hoaxes on SIT systems.

2. Users shall report to the IT HelpDesk immediately if they are aware their PCs are infected by malicious codes or viruses.

E. Copyrighted Materials and Licensed Software, Programs and Data

1. Users must not transfer, duplicate, make available or obtain illegally, any copyrighted material including, but not limited to, agreements, licensed software, programs and data in SIT computers and systems.

2. Users must respect the rights of others by complying with all policies regarding intellectual property when using copyrighted materials and licensed software, programs and data in SIT computers and systems.

3. Users shall not install unlicensed or unauthorized software in the local hard disk or server drives of SIT computers and systems.

[1] Privileged rights may include local (computer) administrative rights and application access rights approved and granted based on users' supervisory functions.

4. Users may be investigated by external regulatory bodies such the Business Software Alliance (BSA) for any violation of software licensing and improper usage of whatever they install on their own into SIT-issued computers.

F. Use of Computers and Portable Storage Media

1. PCs used to access SIT IT resources are equipped and kept up-to-date with the latest operating system software patch or service pack known to address published security vulnerabilities. Users shall not disable such software patches or service packs.

2. PCs used to access SIT IT resources are equipped and kept up-to-date with the latest version or update of anti-virus software (i.e. virus signature or definition file and the scanning engine). The virus detection software shall be memory-resident and enabled at all times.

3. PCs used to access SIT IT resources via the Internet are equipped with a personal firewall that will protect against scanning by unauthorized computers and infection with malicious codes or active content. Users shall not disable such firewalls.

4. Users shall seek the requisite approvals if they require access to any sensitive data in the PCs not accessible by unauthorized personnel.

5. Staff shall **not** store sensitive information, or official documents and staff/student information, on Portable Storage Media. Portable Storage Media includes thumbdrives, flash memory cards, portable hard disks and optical storage media.

G. Network Connection Policy

1. Users shall not tamper with the network outlets in any way such as extending the cable to relocate the outlet to another room or open area temporarily or permanently, blocking it from access by other users if it is on a shared basis, or to connect certain devices for wiretapping, etc.

2. Users are to note that no sharing of any network addresses is allowed.

3. Users are to note that no computer to computer file sharing is allowed.

4. Users shall not tamper with the computer network name and IP address without the permission of the CIT staff.

5. Users shall not install or run any peer to peer software without prior approval from the CIT department.

H. Use of E-mail

1. Users shall not mis-use email systems. Mis-use includes, but is not limited to, the following:

   a. masquerading as another person or sending e-mail anonymously

   b. harassing anyone with language, frequency, or size of messages

   c. forwarding or otherwise propagating chain letters and other unsolicited type of messages

   d. flooding a user or site with very large or numerous pieces of e-mail

   e. using email systems for purposes of defamation or personal attack

   f. using email systems to post potentially offensive information that will impinge on another's culture, ethics, morality and religion

   g. obtaining or sending offensive and seditious material

   h. sending software and material that violates copyright laws

   i. sending, knowingly, a program intended to damage or place excessive load on a computer system or network, such as viruses, Trojan horses and worms

2. Users shall not use public internet email systems such as Yahoo, Gmail and Hotmail to send official email messages.

3. Users are reminded that sending documents across the internet is not secured and hence if there is a need to send such document, then the document must be either encrypted or password protected.

I. Use of Internet and Intranet

1. Users shall not engage in activities that waste SIT computing resources. These activities include, but not limited to, sending unauthorized mass emails, electronic chain letters, blogs, social networking or unauthorized participation in online chat groups.

2. Users shall not communicate material on the internet or intranet that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or which incites religious or racial intolerance. Users shall not knowingly download such material from the Internet.

3. Users shall not knowingly issue search instructions and download data manually or via automated intelligent agents that may potentially consume large amount of network/Internet bandwidth and IT resources, or which may degrade the network, system and/or database performance.

4. Users shall comply with the following regulatory requirements when they copy, reference and use material from the Internet:

    a. Computer Misuse and Cybersecurity Act (Chapter 50A)
    b. Copyright Act (Chapter 63)
    c. Sedition Act (Chapter 290)
    d. Spam Control Act (Chapter 311A)
    e. Personal Data Protection Act (No.26 of 2012)

5. Users shall not knowingly download files from the Internet without scanning them using the virus scan software provided by SIT.

6. SIT shall have the right to block user from accessing any web sites that are deemed to be unlawful or inappropriate.

7. Whilst using SIT's resources, users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. SIT is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

8. SIT prohibits the conduct of a business enterprise, political activity, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials. Other activities that are strictly prohibited include, but are not limited to:
    a. Accessing company information that is not within the scope of one's work.
    b. Misusing, disclosing without proper authorization, or altering personnel information.
    c. Unauthorised and deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites.
    d. Any conduct that would constitute or encourage a criminal offense, leading to civil liability, or otherwise violating any regulations.
    e. Unauthorised transmission of any proprietary, confidential information.
    f. Engage with any form of Cryptocurrency or Blockchain mining activities, using SIT resources for personal gains.

J. Use of SIT Data

1. Users shall be mindful when using sensitive data such as Name, NRIC, Address, Mobile number, exam grades and bank account details. If these fields are to be used, users shall ensure at the data is duly secured, and comply with the PDPA regulations.

K. Sharing Information on Social Platforms

1. Users shall be cautious when sharing any sensitive information on social media platforms; share only on a need to basis. Users are advised to act responsibly with the information that they are entrusted with.

2. Users shall be held responsible for any social media posts that adversely affect the reputation of SIT, and shall be accountable for such posts, regardless of whether the post explicitly mentions SIT or not, may be liable for disciplinary action.