NIE Acceptable IT Usage Policy – ACIS/IFS/POL/004

Issued: Apr 2022
Last review: Apr 2022
Next review: Apr 2025

Access Category: General

1. INTRODUCTION

1.1 Policy Statement

1.1.1 This Acceptable IT Usage Policy ("AIUP") serves to protect the Institute's information and IT resources and minimises risks and damage to the Institute by governing the usage of all its IT resources, including computers and email accounts, mobile devices and IT systems.

1.2 Background and Rationale

1.2.1 This AIUP is to:

- Establish a governance framework for using the Institute's IT resources.
- Establish a process framework for accountability and responsibility in protecting the Institute's IT resources, in compliance with Institute policies, standards, guidelines and procedures, and Singapore laws.

1.3 Scope

1.3.1 This AIUP shall apply to all users ("Users") of Institute's computing facilities ("Computing Facilities").

1.3.2 The Users include but are not limited to:

- Faculty, staff, students, part-time staff & tutors
- Alumni
- Vendors and industrial partners who use the Institute's Network (as defined below) account
- Authorised users to the Institute's Network

1.3.3 The Computing Facilities include, but are not limited to:

- Computer hardware or software owned, leased or operated by the Institute, including those purchased from research funds unless otherwise specified in the research grant or contract.

- Physical location housing computing equipment, computer networks and communications systems involving computers.
- All networking and communications provision, including connections to external computers.
- Computer hardware or software connected to the Institute Network (as defined below) by whatever means; and
- Systems accessed through reciprocal, commercial or other arrangements made by the Institute.

1.4 Definitions

1.4.1 The definitions of terms used in this document are as follows:

- Institute - Refer to all Institute Colleges/Schools/Institutes (including Autonomous Institutes) and Administrative Departments.
- Institute's IT Resources – Refers to all IT resources owned and provided by the Institute and/or managed by Academic Computing and Information Services ("ACIS") which shall include but not be limited to

  a. Computers (servers, workstations, and laptops)

  b. Printers

  c. Software & applications

  d. Mobile Devices

  e. Email accounts (named and role-based accounts)

  f. Web content

- Chief Information Officer (CIO) – Refers to the Divisional Director of ACIS, which form part of the Institute Leadership.
- Network - Refers to wired network connections, wireless network connections and remote connections to access the Institute's Computing Facilities.
- Computer Account – Refers to an account with username and password to access ITsystems for Users to perform dedicated tasks associated with their job functions.
- Email – Refers to the transmission of text messages and file attachments over a Network.

- SPAM Email or Phishing Email – Refers to:

  a. Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple e-mail lists, individuals, or newsgroups, junk e-mail.

  b. A scam communication to steal valuable information including credit card and social security numbers, user IDs and passwords.

- Mobile Device – Refers to those devices supporting remote work or telecommuting. They include mobile phones, smart-phones (e.g. iPhone), tablets (e.g. iPad) and application software that could be used to access Institute IT Resources.

- Domain Name – Refers to a name used in the hierarchical Domain Name System (DNS) to denote the owner of DNS resource records, a hostname (computer or server), an alias, or a sub-hierarchy group of other related domain names or web address (URL). Examples are dns.Institute.edu.sg (a DNS server) and www.Institute.edu.sg (official Institute website).

- Domain Name System (DNS) – Refers to a service that resolves a domain name to an IP address. It serves as a directory for the Internet by translating human readable domain name to IP addresses.

- Service Desk – Refers to an online service for users to report incidents.

  a. Faculty, Staff and Student shall use ServiceNow@NTU for incident reporting.

  b. Alumni, Vendor, Public shall submit Service Desk Web form at NTU Public Website for incident reporting.

2 POLICY

2.1 Principles

2.1.1 The objective of this AIUP is to:

- Minimise risks and damage to the Institute

- Protect the Institute's Information and IT Resources

2.2 General

2.2.1 Users shall not engage in any unlawful activities, in breach of any applicable Singapore laws, when using any of the Computing Facilities and Institute's IT Resources.

2.2.2 Users shall not engage in any activities which violate any Institute policies and regulations.

2.2.3 Computing Facilities and Institute's IT Resources shall be used for the purposes of all Institute- related businesses/activities.

2.3 Computer Account

2.3.1 At all times, Institute reserves the right to review, suspend or terminate any Computer Account.

2.3.2 The Computer Facilities provided to user account holders by Institute shall include software and computing domains under the control of Institute including the provision of Computing Facilities to remote Users.

2.3.3 Any act prohibited by the AIUP shall constitute a ground for the suspension or termination of the User's account. Such action may be in addition to any:

- internal disciplinary action the Institute may take against the User;
- legal proceedings the Institute may initiate against the User; and/or
- any prosecution action taken by the relevant law enforcement authorities for the breach of any of the applicable Singapore laws.

2.3.4 There should not be any sharing of User accounts whether that other person is a registered or unregistered User, unless approval is obtained in writing from the CIO.

2.3.5 The User account holder is required to keep his/her computer account and password confidential at all times. If the User account holder suspects that another person is using his/her account, he/she shall change the password immediately and report the incident via Service Desk.

2.3.6 For security reasons, the User account holder is advised to change his/her password regularly. The password shall comply with the password criteria in Annex A of the Access Management Policy.

2.3.7 Connection to peer-to-peer networks (eg. Bit-torrent) using a Institute Computer Account is strictly prohibited.

2.3.8 There shall not be any fraudulent, obscene, distasteful, derogatory, vulgar, or sexually suggestive or discriminatory communication using the Institute Computer Account.

2.3.9 Only licensed software shall be used with the Institute Computer Account.

2.3.10 All Computer Accounts shall be installed with the Institute approved end-point protection software with up-to-date malware signatures.

2.4 Email Messaging

2.4.1 This applies to both named accounts and role-based accounts.

2.4.2 The Institute Email shall be used for all official Email communication.

2.4.3 Retention of Institute email account for staff who have left the Institute and the retention period will require approval from Academic Group (“AG”) or Department Heads or above.

2.4.4 All Institute Email accounts, and their content shall remain the property of the Institute.

2.4.5 Extraction of the contents of an Email account shall be carried out only with endorsement by the Institute Unit Heads and approval from Chief Information Officer of the Institute (“CIO”).

2.4.6 Institute-wide mass Emails to faculty, staff, students, and alumni may only be sent via designated role-based Email accounts and their content must be cleared by a member of the President’s Council. Because of their reach, mass Emails have potential implications for the Institute’s safety, security, reputation and branding, and particularly so in this digital age where internal information can be shared externally at great speed. The mass emails shall be sent using Blind Carbon Copy (BCC) in the address field to prevent all other recipients from receiving unnecessary replies through the reply all feature.

2.5 Internet Advertising

2.5.1 Any marketing or selling of non-Institute products and services which have not been authorised by the Institute in the Institute’s corporate website and Institute Units’ websites is strictly prohibited.

2.6 Domain Name

2.6.1 ACIS is responsible for the Institute’s central Domain Name System (DNS) and the registration of domain names. All DNS registration requests shall be approved by CIO.

2.6.2 Usage of the domain name shall comply with the following standards:

- Duplicate domain names shall not be used[1].
- Institute Units shall ensure that their respective domain names comply with the Institute domain name standard for their websites and computer

resources. These websites and computer resources shall be hosted within the Institute unless approved by the CIO.

- Domain name owners shall notify ACIS immediately if any domain name is no longer in use.

- Institute domain name shall be hosted by central Domain Name System. Any request for external Domain Name hosting of Institute domain shall be approved by the CIO.

- Relevant parties implementing the policy shall refer to the Domain Name Procedure.

[1] Prior to applying for any new domain name, the website owner of the relevant Institute Unit shall check against this online registry to avoid using the same domain name.

2.7 Uses in violation of Law

2.7.1 The following acts are STRICTLY PROHIBITED when using the Computing Facilities:

2.7.2 The Computing Facilities may not be used to perform, facilitate or abet the performance of, any act that will violate any laws of Singapore, including but not limited to the Computer Misuse and Cybersecurity Act (Cap. 50A), Copyright Act (Cap. 63), Penal Code (Cap. 224), Personal Data Protection Act (Act No. 26 of 2012), Sedition Act (Cap. 290), Spam Control Act (Cap. 311A), the Undesirable Publications Act (Cap. 338) and the Remote Gambling Act (Act No. 34 of 2014);

2.7.3 Accessing, storing, sharing, distributing or downloading from any source or displaying, creating or transmitting in any form or language, of any obscene or pornographic materials or other materials depicting distasteful, discriminatory, derogatory, vulgar or sexually suggestive electronic text, pictures, graphics or videos prohibited by the laws of Singapore.

2.7.4 Accessing, storing, sharing, distributing or downloading any seditious or other materials that is likely to give rise to or incite feelings of enmity, hatred, ill-will or hostility between different social, racial or religious groups.

2.7.5 Making any unauthorised reproduction, communication to the public, distribution, downloading, publication, storage or transmission of any copyrighted material (including but not limited to music, images, videos, books, games and/or software).

2.7.6 Where the User has been provided with any software by the Institute, the doing of any act in contravention of the terms and conditions of use as stated in the relevant software licence; and

2.7.7 Disclosing to any external party any data, materials and/or information which is confidential, restricted or proprietary to the Institute, unless the prior written authorisation of the Institute has been obtained or such disclosure is in accordance with the Institute's policies.

2.7.8 The provision of on-line services disseminating information regarding politics and religion without the proper licences from the Info Communications Media Development Authority (IMDA).

2.8 Uses that undermine system integrity

2.8.1 The following acts are STRICTLY PROHIBITED in the use of the Computing Facilities:

2.8.2 Cracking, unravelling or capturing another person's password without the relevant internal Institute approvals and/or lawful authority, including but not limited to the use of programmes that bypass system security measures and steal passwords or data.

2.8.3 Introducing 'viruses' or 'worms' or any software program designed to alter any data or software in the Computing Facilities, or introducing anything that may potentially cause performance degradation, service instability, or compromise operational efficiency, security or fair use of resources.

2.8.4 Issuing massive search instructions or downloading data manually or via automated intelligent agents which may potentially consume large amounts of network/internet bandwidth or which may degrade the Network, system and/or database performance.

2.8.5 Undermining or attempting to undermine the security of the Computing Facilities, for example by destroying, deleting or modifying files of other users, or of data or software components of the Computing Facilities without the relevant internal Institute approvals and/or lawful authority; and

2.8.6 Tapping the use of the Computing Facilities or its Network without the written permission from the CIO.

2.9 Unauthorised Access or Use

2.9.1 The following acts are specifically and STRICTLY PROHIBITED in the use of the Computing Facilities:

2.9.2 Sharing of a User's individual online identity with another person (User ID and password or other authenticator such as a token or certificate).

2.9.3 Concealment of User's personal identity when using the Network (except where the option of anonymous access is explicitly authorised) or masquerading as or impersonating others or otherwise using a false identity when using the Network.

2.9.4 Use of the Computing Facilities for commercial activities for the benefit of private individuals or other organisations without prior authorisation from the Institute. For the avoidance of doubt, Users are to apply for a separate account for industrial consultancy purposes. The rates and AIUP governing such accounts can be found in the computer account application form for industrial partners.

2.9.5 Use which denies other Users of usage through forms of excessive traffic.

- Providing personal network connection/ services.
- Providing other services, including but not limited to:
  a. Distribution of IP addresses on the Network e.g. DHCP Server.
  b. Firewall or Router, WINS server, Mail/SMTP server services.
  c. Domain Name Server or Proxy Server services.
  d. Remote modem dial-in access services.
  e. Wireless LAN access services.
  f. Video or audio single-cast or multi-cast services.
  g. Online services such as Game Server, relay services, etc.
  h. Web hosting service or FTP Server services.
  i. Peer-to-peer file sharing services e.g. BitTorrent.

2.9.6 Performing intrusive or invasive activities towards other computers within or outside the Institute. Such activities may include but are not limited to performing port scans on other computers, sending spam mails to other internet users, and depositing or connecting to Trojan horse type of software on other computers.

2.9.7 Unauthorised access, copying, destroying or deleting and altering or amending of data or software programs.

2.9.8 Copying, storage, transmission and use of unlicensed copyrighted software or materials.

2.9.9 The transmission, display or broadcasting of electronic messages or the use of Computer Facilities in any manner:

- To denigrate, satirise, degrade, or defame any person, family, organisation, nation, race or religious group;
- To affect or prevent any registered users' use of the computer facilities;

- For commercial, political, or religious purposes, without obtaining prior written permission from the CIO; or

- For or on behalf of any person, party, organisation or principal without obtaining prior written authorisation from the person, party, organisation or principal AND the written permission from the CIO.

2.9.10 Anything that violates the rules, regulations and policies applicable to any wired and wireless network, Institute server, computer database, website or newsgroup that any Institute visitor or User accesses.

2.9.11 Anything that sends, or facilitates the sending of, unsolicited bulk Email to any User or system in a way that may adversely impact the Institute's Network or User's facilities, or to send Email-bombs (masses of Email or other data) to any person or system, soliciting replies to Email-bombs for commercial or unofficial purposes.

2.9.12 Use of the Institute wired or wireless services to attempt to break computer security or in fact, break the security of any computer network, or to access an account without authorisation.

2.9.13 Forges, removes, or modifies identifying network header information or employs any other methods in connection with the transmission of Email used to forge, disguise, and mislead any legitimate Institute User.

2.9.14 Impersonating other Users by forging his/her Email address.

2.9.15 Flooding, spoofing, harassment, or otherwise hindering the ability of others to use the Institute Network and Internet services.

2.9.16 Conducting any other activities or to relay any systems which Institute determines as injurious, or prejudicial to Users, Institute operations or their reputation.

2.9.17 Attempt to resell Institute Network services or using bandwidth in excess of limits imposed by the Institute Network.

2.9.18 Users shall be personally liable for the maintenance of their Computer Account to prevent the occurrence of any of the above-mentioned events.

2.10 Uses in violation of the Institute's policies or that damage the reputation of the Institute

2.10.1 The following acts are specifically and STRICTLY PROHIBITED in the use of the Computing Facilities:

2.10.2 Emailing or posting on public blogs, social networking sites, websites, mobile phone applications or any other publicly accessible communication platform or channel, any content that is abusive, distasteful, derogatory, defamatory, discriminatory, vulgar, sexually suggestive, prejudicial to the good name of the Institute;

2.11 Users Responsibilities

2.11.1 The User shall be personally liable for the maintenance of his/her User account and computer to prevent the occurrence of any of the above-mentioned events.

2.11.2 The User consents to the Institute collecting, using, accessing and disclosing the User's personal data, files or stored information for any purpose related to or arising from the User's use of the Computing Facilities and/or the User's employment with the Institute, including without limitation for the purposes of investigating cases of possible violation of the AIUP, Institute policies or procedures, or any laws of Singapore, investigating matters and incidents such as whistleblowing and disciplinary breaches, and for systems maintenance purposes. The Institute shall also be entitled to disclose to the relevant authorities' evidence of any violations of the law, for which offenders may be subject to criminal prosecution and/or civil liability. Users are reminded that unauthorised access to, and unauthorized modification or interception of computer programmes or data are offences under the Computer Misuse and Cybersecurity Act which are punishable with fines and/or imprisonment.

2.11.3 Users must immediately report to ACIS in the following circumstances:

- When the User receives any transmission or electronic message of a kind that is prohibited under this AIUP;
- When the User has knowledge of any violation of the AIUP by another User; or
- When the User believes that the security of his/her Computer Account has been compromised.

2.11.4 Users who believe that their copyright has been infringed by any User may submit a report to Service Desk containing the following information:

- A statement on the ownership of the copyright or authorization to act on behalf of the owner of the copyright;
- Identification of the copyrighted work(s) claimed to have been infringed;
- Identification of material that is claimed to be infringing or to be the subject of infringing activity that is to be removed or access to which is to be disabled;
- Identification of User who infringed copyright (if possible); and
- Information sufficient to enable the Institute to contact the User who made the report.

2.11.5 Upon receipt of report of violation to the AIUP, ACIS shall investigate the matter and refer the matter to be handled in accordance with the Institute's disciplinary policies, where appropriate, and/or the relevant law enforcement authorities. Any failure to report the incidents stated in AIUP may result in the User being deemed to be a party or abettor to the prohibited act(s) and may render the User liable to the sanctions referred to in these AIUP.

2.11.6 Users who connect their own personal devices, which are not NTU-issued, to the Network shall ensure that their personal devices are:

- Compatible with the Network;
- Protected with up-to-date End Point Protection (eg. Anti-virus). In addition, Users must also apply the latest software security patches and service packs to their computers to guard against network intrusions or attacks exploiting the weaknesses of the computers;
- Secure with appropriate authentication (eg Password, PIN or biometrics). It must be complex and having adequate length (eg Minimally 8 characters with numbers, symbols, upper- and lower- case letters.)
- Activate screen lock when not in use or inactive;
- Protected with encryption tools (eg. bitlocker, filevault) that store sensitive Institute data;
- Not altered to bypass security controls (eg. rooting and jailbreaking);
- Ensure that Institute Data are securely removed from your Personal Device before disposal;
- The Institute may block personal devices from connecting to the Network, if the personal devices are compromised or found to be in violation of the AIUP.

2.11.7 Users who use personal devices to access Institute IT Resources shall note on their responsibilities to:

- Use Virtual Private Network (VPN) or secure transmission method when accessing Institute network or data;
- Report all stolen or lost devices that contain Institute data and;
- Report suspected unauthorized access to Institute data stored in a Personal Device.

2.11.8 Users shall consent to ACIS performing background scans of the Network for virus detection, intrusion attacks and system vulnerabilities. The ACIS may also inspect the files on computers connected to the Network for evidence of any violations of the laws of Singapore or any other applicable laws.

2.11.9 Where Users are issued with Institute Email addresses:

- Users shall consent to the Institute listing the Email address and the Users' display name on the Institute's Email directory. Users acknowledge and consent to receiving official Emails from the Institute, other Users of the Institute's Computing Facilities, or external parties.

- Users shall not collect and/or share Institute Email addresses with external parties without prior authorisation from the CIO.

- Users shall not use the Institute's Email system to:

  a. Perform any acts which are prohibited under these AIUP.

  b. Send annoying, abusive, or unwanted messages to others; and

  c. Send unsolicited spam mail to other Users of the Institute's Computing Facilities, or external parties.

- Users shall stay vigilant to spot sign of phishing attack and take appropriate measures to prevent their account from being compromise. They should report any phishing email to Service Desk.

2.11.10 The Institute does not guarantee the suitability of its Computer Facilities for any specific application or purpose intended by the User. Signal strength may vary or fail due to factors which are not within Institute control. The Institute shall not be liable for any loss or damage arising from any interference or failure.

2.11.11 Due to the nature of wireless access, there is an inherent risk of wrongful, illegal, or unauthorised access by a third party to the User's computer and/or Computer Account. The User hereby acknowledges and accepts all the risks of such wrongful, illegal, or unauthorised access and hereby agrees that Institute shall not be liable for any loss or damage arising from such access.

2.11.12 Whilst every care would be taken in the provision of the Computing Facilities, the Institute disclaims all liability whatsoever for any loss of data howsoever caused, including without limitation, non-deliveries, misuses, mis-deliveries or for the contents, the accuracy or quality of information or resources available, received or transmitted as a result of any disruption, interruption, suspension, and including termination of the Computer Account.

2.11.13 The Institute disclaims all liability whatsoever for any interruptions experienced and/or hardware damage with the use of the Network, as a result of war, acts of terrorism, epidemics, pandemics, general labour disturbances such as lockout, go-slow or occupation of premises, acts of Gods and/or natural catastrophes such as cyclone, volcanic activity, landslide, tsunami, flood, blizzard, earthquake, explosion, or fire.

2.11.14 Whilst every care would be taken in the provision of the Computing Facilities and Institute's IT Resources, the Institute disclaims, to the fullest extent permissible by law, any and all liability, loss or damage, including but not limited to loss of profits, loss of use, loss of data (including personal data) and loss of production, or any other direct, indirect, consequential, punitive, incidental or special loss or damage, however caused (and whether arising out of contract, strict liability, or tort or under any legal or equitable theory of liability) which any User of the Computing Facilities and Institute's IT Resources may suffer or incur as a result of, or in connection with, his or her use of the Computing Facilities and Institute's IT Resources.

2.11.15 Whilst the Institute will make reasonable efforts to take appropriate preventive measures to ensure that Users' personal data is adequately protected and secure, the User shall fully and unconditionally release, waive and discharge the Institute from any and all liability for any disclosure of his/her personal data, including but not limited to disclosure of personal data by reason of User's use of the Computing Facilities and Institute's IT Resources (including but not limited to User's use leading to hacking, phishing and deployment of malware) and/or the User's unauthorized use of the Computing Facilities and Institute's IT Resources in breach of the Institute's prevailing Cyber Security Policy, this AIUP and other IT related policies.

2.11.16 The User shall indemnify and hold the Institute harmless from any and all claims, damages, losses, costs and expense resulting from, or in connection with, the User's use of the Computing Facilities and Institute's IT Resources (including but not limited to User's use leading to hacking, phishing and deployment of malware and/or the User's unauthorized use in breach of the Institute's prevailing Cyber Security Policy, this AIUP and other IT related policies).

2.11.17 Failure by Users to observe the AIUP may result, directly or indirectly, in the Institute being involved in claims and/or suffering damage, losses and expenses. As such, the User shall hold harmless and indemnify the Institute and its officers from any such claims, damages, losses and expenses resulting from the User's failure to observe any provisions of this AIUP.

2.11.18 The User acknowledges the possibility that the Institute will cooperate in any official investigations resulting from any breach of this AIUP or any law, and may where it deems necessary, furnish the relevant authorities or requesting parties with information of or concerning the User. In that event, the User agrees that the Institute may disclose such information to the relevant authorities or requesting parties in the Institute's sole and absolute discretion.

2.11.19 The Institute reserves the right to amend this AIUP or implement additional policies periodically. Although ACIS will inform Users of policy changes, Users must share the responsibility of staying informed about the Institute's policies regarding the use of Computing Facilities and Institute's IT Resources and comply with all other applicable policies and this AIUP that are in force at all times