NTU IT Rules for Student User Accounts

1. These NTU IT Rules for Student User Accounts ("**Rules**") apply to all student users ("**Users**") of NTU's ("**the University**") computing facilities ("**Computing Facilities**"). The Computing Facilities include, but are not limited to:

    1.1. computer hardware or software owned, leased or operated by the University, including those purchased from research funds unless otherwise specified in the research grant or contract;

    1.2. physical location housing computing equipment, computer networks and communications systems involving computers;

    1.3. all networking and communications provision, including connections to external computers;

    1.4. computer hardware or software connected to the University network ("**Network**") by whatever means; and

    1.5. systems accessed through reciprocal, commercial or other arrangements made by the University.

2. Any act prohibited by the Rules shall be construed as misconduct as defined under Statute 6 Student Discipline of the University Statutes and Regulations and shall constitute grounds for disciplinary action, which may result in fines, suspension of the User's account, and expulsion or suspension of the User from the University, whether permanently or temporarily, or constitute grounds for the suspension or termination of the User's account. Such action may be in addition to any prosecution action taken by the relevant law enforcement authorities in the prosecution of any breaches of the applicable laws, which prosecution may result in the imposition of fines and/or custodial sentences upon conviction.

3. The following acts are specifically and **STRICTLY PROHIBITED** in the use of the Computing Facilities:

    Uses in violation of law

    3.1. Anything that might be considered illegal. The Computing Facilities may not be used to perform, or facilitate or abet the performance of, any act that will violate any civil or criminal law in 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), as may be amended from time to time;

3.2. 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, vulgar or sexually suggestive electronic text, pictures, graphics or videos prohibited by the laws of Singapore;

3.3. 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;

3.4. 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);

3.5. Where the User has been provided with any software by the University, the doing of any act in contravention of the terms and conditions of use as stated in the relevant software licences; and

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

Uses that undermine system integrity

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

3.8. 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;

3.9. 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;

3.10. 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 lawful authority; and

3.11. Tapping the use of the Computing Facilities or its Network without the written permission from the Chief Information Officer of the University.

Unauthorised access or use

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

3.13. Concealment of 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;

3.14. Use of the Computing Facilities for commercial activities for the benefit of private individuals or other organisations without prior authorisation from the University;

3.15. Use which denies other users of usage through the forms of excessive traffic;

3.16. Providing personal network connection/ services;

3.17. Providing other services, including but not limited to:

3.17.1. Distribution of IP addresses on the Network e.g. DHCP Server;

3.17.2. Firewall or Router, WINS server, Mail/SMTP server services;

3.17.3. Domain Name Server or Proxy Server services;

3.17.4. Remote modem dial-in access services;

3.17.5. Wireless LAN access services;

3.17.6. Video or audio single-cast or multi-cast services;

3.17.7. Online services such as Game Server, IRC Server, etc;

3.17.8. Web hosting service or FTP Server services; or

3.17.9. Peer-to-peer file sharing services e.g. BitTorrent; and

3.18. Performing intrusive or invasive activities towards other computers within or outside the University. 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.

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

3.19. 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 University or otherwise prohibited by the laws of Singapore;

3.20. Transmitting, displaying or broadcasting any electronic messages:

3.20.1. which denigrate, satirise, degrade or defame any person, family, organisation, nation, race or religious group;

3.20.2. which affect or prevent any registered users' use of the Computing Facilities;

3.20.3. for commercial, political or religious purposes, without obtaining the prior written permission of the Chief Information Officer of the University; or

3.20.4. for or on behalf of any person, party, organisation or principal without obtaining the prior written authorisation of that person, party, organisation or principal, ***and*** of the Chief Information Officer of the University.

4. 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.

5. The User consents to the University 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 undertaking of a course of education at the University, including without limitation for purposes of investigating cases of possible violation of the Rules, NTU policies or procedures, or any laws of Singapore, investigating matters and incidents such as whistleblowing and disciplinary breaches, and for systems maintenance purposes. The University shall also be entitled to disclose to the relevant authorities evidence of any violations of the law, for which offenders may be subject to University disciplinary proceedings, 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.

6. Users must immediately report the following to the hotline of the Centre for IT Services (internet: http://servicedesk.ntu.edu.sg, phone: 67904357(HELP), email: servicedesk@ntu.edu.sg) in the following circumstances:

6.1. When the User receives any transmission or electronic message of a kind that is prohibited;

6.2. When the User has knowledge of any violation of the Rules by another User; or

6.3. When the User believes that the security of his/her computer account has been compromised.

7. Users who believe that their copyright has been infringed by any User may submit a report to the Centre for IT Services at servicedesk@ntu.edu.sg containing the following information:

    7.1. A statement on the ownership of the copyright or authorization to act on behalf of the owner of the copyright;

    7.2. Identification of the copyrighted work(s) claimed to have been infringed;

    7.3. 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;

    7.4. Identification of User who infringed copyright (if possible); and

    7.5. Information sufficient to enable the University to contact the User who made the report.

8. Upon receipt of such reports under Rules 6 or 7 above, the Centre for IT Services shall investigate the matter and, if appropriate, refer the matter to the University's disciplinary body and/or the relevant law enforcement authorities. Any failure to report the incidents stated in Rules 6.1 and 6.2 above 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 Rules.

9. Users who connect their computers to the Network shall ensure that their computers are:

    9.1. compatible with the Network;

    9.2. configured to use TCP/IP protocol only and the IP address automatically assigned by the Centre for IT Services; and

    9.3. protected with up-to-date anti-virus software. 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.

10. Users shall consent to the Centre for IT Services performing background scans of the Network for virus detection, intrusion attacks and system vulnerabilities. The Centre for IT Services 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.

11. Where Users are issued with University email addresses:

    11.1. Users shall consent to the University listing the email address and the Users' display name on the University's email directory. Users acknowledge and consent to receiving official emails from the University, other users of the University's Computing Facilities, or external parties;

11.2. Users shall not collect and/or share University email addresses with external parties without prior authorisation from the University;

11.3. Users shall not use the University's email system to:

11.3.1. perform any acts which are prohibited under these Rules;

11.3.2. send annoying, abusive, or unwanted messages to others; and

11.3.3. send unsolicited spam mail to other users of the University's Computing Facilities, or external parties.

12. Whilst every care would be taken in the provision of the Computing Facilities, the University disclaims all liability whatsoever for any loss of data howsoever caused, including without limitation, non-deliveries, misuses, misdeliveries 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 User Account. The University also disclaims all liability whatsoever for any hardware damage during the use of this Network, as a result of any electrical disruption, acts of God or other service interruption. The University further disclaims all liability for any indirect or consequential loss or for any loss of profit or opportunity howsoever arising from the use of the Computing Facilities.

13. Whilst the University will take 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 University 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 the unauthorized use of the Computing Facilities (including through hacking) or the deliberate deployment of malware.

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

15. The User acknowledges the possibility that the University will cooperate in any official investigations resulting from any breach of the Rules or of the 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 University may disclose such information to the relevant authorities or requesting parties in the University's sole and absolute discretion.

16. The University reserves the right to amend these Rules or implement additional policies periodically. Although the Centre for IT Services will inform Users of policy changes, Users must share the responsibility of staying informed about the University's policies

regarding the use of Computing Facilities and complying with all other applicable policies and rules that are in force at all times.