1. Purpose

The National University of Singapore ('the University') has invested extensively in Information Technology such as computer accounts, personal computers, servers, workstations, disk storage, software, administrative and academic applications, email, public folders, newsgroups, online discussion forums, dialup, network, Internet and databases, etc ('the IT Resources') to facilitate teaching, learning, research, administration, professional development and other functions of the University. This Policy is intended to prescribe the appropriate behaviour and use of IT Resources by students, faculty, staff, alumni and authorised users in an effective, ethical and lawful manner. It sets out the parameters of permitted use of the IT Resources and is in addition to any other policies that govern the use of the IT Resources. In the event of a conflict between other policies and this Policy, this Policy shall prevail.

2. Scope

This Policy applies to the use of the IT Resources owned, controlled or managed by the University. All users who have been granted access to the IT Resources ('Users'), including but not limited to students, faculty, staff and alumni of the University and Extended Account Users, are to comply with this Policy. Contractors, consultants, vendors and contract workers (including their employees, agents and other authorised representatives) ('Contingent Workers') hired by a staff or faculty of the University ('Hiring Manager') are also to comply with this Policy.

3. Waiver

When restrictions in this Policy interfere with their research, educational or administrative activities, Users may request for a written waiver from specific clauses from the Director of Computer Centre. Such waiver shall only be granted in very exceptional circumstances.

4. General Prohibited Uses

4.1 Uses In Violation Of Law

Users shall not engage in any activities relating to the use of the IT Resources that will be in violation of the laws of Singapore, in particular (but not limited to), the Computer Misuse and Cybersecurity Act (Cap 50A), Copyright Act (Cap 63), Spam Control Act (Cap 311A) and Undesirable Publications Act (Cap 338) as may be amended from time to time. By way of illustration only, some examples of such illegal uses are:

(i) Downloading, distribution, sharing or storing of (a) seditious or other materials that is likely to cause feelings of enmity, hatred, ill-will or hostility between different racial or religious groups; or (b) obscene or pornographic materials or other materials depicting sex, horror, crime, cruelty, violence or the consumption of drugs or other intoxicating substances that is likely to be injurious to the public good.

(ii) Downloading, making copies, distribution or sharing of any copyrighted materials or copyright infringing materials without prior permission from the copyright owner and using or making use of the IT Resources to engage in activities which generally infringe copyright and intellectual property rights.

4.2 Commercial Uses

Users shall not use the IT Resources for commercial purposes or to offer any commercial services to external parties, unless it is within their scope of employment with the University or with prior authorisation of the University.

4.3 Undermining System Integrity

Users must not undermine or attempt to undermine the security of the IT Resources, for example, by 'cracking' passwords or modify or attempt to modify the files of other Users or software components of the IT Resources in an unauthorised manner.

4.4 Unauthorised Access Or Use

Users shall not access or attempt to access IT Resources to which they have not been given access or permit others to do so. Users shall not intercept or attempt to intercept or access data or communications not intended for them.
4.5 Tampering Of IT Resources

Users shall not tamper or in any manner modify the IT Resources that may potentially cause performance degradation, service instability, or compromise operation efficiency, security and fair use of resources.

4.6 Massive Search Instructions and Data Download

Users shall not indiscriminately 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.

4.7 Unauthorised Transmission or Disclosure of Proprietary/Confidential Materials

Users shall keep in strict confidence any data which is proprietary and/or confidential to the University and use such data responsibly. Disclosure to any external party is prohibited, unless with the prior written authorisation of the University or in accordance with University’s policies.

5. Specific Uses Of IT Resources

5.1 Personal Responsibility

(i) Users shall not reveal their login, email passwords and NUS Smartcard PIN number to anyone.

(ii) Users shall be responsible for maintaining the security of their passwords, NUS Smartcard and NUS Smartcard PIN number and all functions performed from the accounts and NUS Smartcard PIN number assigned to them.

5.2 Network Connection Policy

(i) Every network connection point shall be connected to one computer only. Users shall not tamper with network points in any way, such as extending the cable to relocate the point to another room or open area temporarily or permanently, thereby blocking it from access by other Users.

(ii) Users shall not share any network addresses assigned.

5.3 Software Licence and Copyright

(i) Users shall not use or install unlicensed software or programs. Users shall not infringe the copyright of any software available over the University network.

(ii) Users shall comply with contractual obligations and terms and conditions of use as stated in the software licenses acquired by the University.

(iii) Software purchased by the University are Academic licences. It may be granted to Users for use at home or other locations on non-University owned computers during the course of work or study with the University. Users shall discontinue use and un-install the software from those non-University owned computer(s) upon cessation or termination of employment or matriculation, or upon notification by the University of its termination of the software license agreement.

5.4 Email

Email is used frequently for correspondence internally and externally for teaching, research, learning, administration or otherwise carry out the functions and purposes of the University.

(i) Users shall not email or transmit defamatory, threatening or abusive messages or any messages that may be reasonably construed as such.

(ii) Users shall not send annoying, abusive or unwanted messages to others.

(iii) Users shall not send unsolicited mass emails within or external to the University, except for purposes specific to the functions and purposes of the University, or which have been approved by a Dean or Director or University representative with equal or higher authority, and in accordance with the requirements of law.

(iv) Users shall not forward messages containing general appeals or warnings like ‘virus warnings’, ‘request for help’, by mass mail or otherwise. Users should instead send these messages to the University’s Computer Centre Helpdesk for verification.

NUS INTERNAL
(v) Users shall not forge the identity of or impersonate another person in an email.

(vi) Users shall not knowingly transmit by email any harmful or malicious content (e.g. viruses) or any other content or material that may otherwise violate the civil and criminal laws of Singapore.

(vii) Users shall not misuse mailing lists to flood an individual, group or the email system with numerous or large emails.

(viii) Where Users are granted extended access to IT Resources beyond their terms of employment, for limited purposes connected to the University (referred to as “Extended Account Users”), all provisions of this Policy shall continue to apply with the same force and effect. In addition, Extended Account Users shall not use the IT Resources, specifically their extended email accounts, to make representations that are calculated to mislead others of the scope of their authority and positions in the University.

5.5 Alumni Email

(i) The alumni email is a good-will service provided by the University for building close bonds and relationship with its alumni. The University reserves the right to terminate or suspend the service with 90 days’ advance notice if it deems impractical to continue with the service at its sole discretion.

(ii) Alumni email users shall not transmit messages containing representations that they are current staff or students of the University or are authorized to represent the University in any transaction or matter and/or otherwise to speak on behalf of the University.

5.6 Hiring Manager

A Hiring Manager applying for an account on behalf of a Contingent Worker to access the IT Resources as part of and in the course of the Contingent Worker’s work shall ensure that such use by the Contingent Worker is in compliance with this Policy.

6. University’s Access

6.1 Conditions of Access

The University respects privacy and recognises its critical importance in an academic setting. As such, the University does not, in general, intend nor wish to access Users’ data except in the following limited circumstances:

(i) For identification or diagnosis of systems or security vulnerability and problems in order to preserve the integrity of the IT Resources;

(ii) Where there are reasonable grounds to believe that a violation of law or a breach of the University’s policies may have taken place, and such access, inspection or monitoring may produce evidence of such violation or breach; or

(iii) Where specifically allowed or required under the laws of Singapore.

In the above situations, the University or its representatives may access all aspects of the IT Resources (excluding Users’ owned computers), without User consent.

Consistent with privacy interests of the Users, University access without the consent of the User will occur only with the approval of President, Provost, or Deputy President or their authorised delegates.

6.2 User’s Assistance

Where required, Users agree to provide all necessary assistance to the University or its representatives in relation to the activities stated in paragraph 6.1.

6.3 Use Of Security Scanning Systems

Notwithstanding paragraph 6.1, Users consent to the University’s use of scanning programs for security purposes at system and network level for computers and systems that are connected to the University’s network. This is to ensure that any computers or systems attached to the network will not become a launching pad for security attacks and jeopardise the IT Resources. System level scanning includes scanning for security vulnerabilities and virus detection on email attachments. Users’ stored files and data are excluded from the scanning.
7. Enforcement Procedures

7.1 Complaints/Reports Of Alleged Violations

Any User who believes that the security of his/her computer account, NUS Smartcard or NUS Smartcard PIN number has been compromised or is aware of a violation of this Policy must report the matter to the Director of Computer Centre, who shall investigate the allegation and, if appropriate, refer the matter to the University disciplinary and/or law enforcement authorities.

7.2 Disciplinary Procedures

Violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for students, faculty and staff.

7.3 Network Connection and Computer Account

In the event that the situation poses an immediate security threat to the IT Resources or other external systems and jeopardises the reputation, properties or other interests of the University, the University may disconnect the User’s computer or any IT equipment from the University’s network or disable his/her computer account for further pending actions and notify the User accordingly.

7.4 Legal Liability For Unlawful Use

In addition to University disciplinary actions, Users may be subject to criminal prosecution, civil liability or both for unlawful use of any of the IT Resources. Users are reminded that unauthorised access to, modification or interception of computer programmes or data can amount to serious criminal offences under the Computer Misuse and Cybersecurity Act (Cap 50A) and general law.

8. Channel of Recourse

Any User who suspects that the University or its representatives have made unwarranted access to his or her computer systems may feedback his or her concerns to the President, Provost or Deputy President, who will investigate the report.

9. Indemnity

Failure by Users to observe this Policy may result, whether directly or indirectly, in the University being involved in claims and/or suffering damages, losses and expenses. The User shall 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 provisions of this Policy.

10. Consent To Disclosure of Information

In addition, the User must understand that the University will cooperate in any official investigations resulting from any breach of this Policy and may, in its discretion, furnish the relevant authorities/parties with the relevant information and User’s consent to any such disclosure shall be deemed by acceptance of this Policy.

11. Changes To Policy

The University environment is a fast-changing environment and computer technologies and network access may be subject to change at any time. The University reserves the right to amend this Policy or implement additional policies, without the User’s consent, from time to time in the future. Although Computer Centre will inform Users of policy changes, Users must share the responsibility of staying informed about the University’s policies regarding the use of IT Resources and complying with all other applicable policies. The current version of the Policy can be found at http://www.nus.edu.sg/comcen/security/aup.
I have read, understood and accepted the Acceptable Use Policy, version 4.0 set out above, including any revisions to the policy.

Name: ______________________________________

Signature: __________________________________

Date: ______________________________________

Matriculation no/Staff no/Organization: ____________________________________________