SMU IT POLICIES & PROCEDURES

Title: **Acceptable Use Policy**	
Prepared by: IITS	Approved by: Chief Information Officer and Vice President, IITS

Contents

SMU IT POLICIES & PROCEDURES

Title: **Acceptable Use Policy**	
Prepared by: IITS	Approved by: Chief Information Officer and Vice President, IITS

1. INTRODUCTION

Singapore Management University (SMU) provides information technology (IT) resources for the shared and responsible use by members of its community who are in turn, expected to use them in an efficient, ethical, professional, and legal manner consistent with the University's objectives and values. Inappropriate use exposes the University and community members to risk of data theft/loss and unintended disclosure. The University, therefore, has a responsibility to protect itself, its IT resources, and its users from illegal or damaging actions, intentional or unintentional, on the part of individuals or computer systems.

Participation in a community of networked computers and users requires adherence to an ethical code of conduct. The fact that an activity is technologically possible does not legitimise its use. Users of the University's IT resources have a responsibility not to abuse these resources and to respect the rights of the members of the community as well as the University itself. This includes the University's wholly owned subsidiaries, namely, university staff residences, student hostels, and any overseas and satellite offices, on which SMU policies, Singapore laws, and the relevant local laws apply.

2. PURPOSE

The purpose of this Acceptable Use Policy (the "Policy" or "AUP" hereafter) is to articulate the acceptable use procedures for the appropriate use of the IT resources provided by SMU as well as for SMU's right to access information about and management of these resources on campus and in any of its overseas and satellite offices .

In effecting this Policy, the University aims to meet the following goals:

a. To ensure the integrity, reliability, availability, and superior performance of University IT resources; and

b. To ensure that University IT resources are used for their intended purposes.

3. SCOPE OF POLICY

This AUP applies to all users of University IT resources including faculty, staff, students, alumni and guests. It also applies to technology resources administered by individual departments as well as centrally, to personally owned computers and devices connected to the campus network by wired and wireless connections, and to off-campus computers that connect remotely to the University, and to IT networks of all SMU local, overseas and satellite offices.

4. DEFINITIONS

For the purposes of this document, the following definitions apply:

4.1. **Data:** a collection of information that may include alphanumeric characters, words, sounds, symbols, images or videos, etc, stored in a form suitable for a computer or other networked device (see 4.2).

4.2. **Equipment:** any information-handling technology and equipment including, but not limited to, the following: standalone or networked personal computers, digital mobile devices, printers, network devices, and all forms of telecommunication equipment.

4.3. **Personal Computer**: a general-purpose, cost-effective computer designed to be used by a single end-user. This includes desktop, laptop or any other personal device, and these typically run on Windows (Wintel), Mackintosh (Mac OS) or Linux mobile operating systems.

4.4. **Personal Information:** any and all personally identifiable information on an individual, including his/her/their name, IP address, University log-in usernames and accounts, through which he/she/they can be identified.

4.5. **Personal Data**: data whether true or not about an individual who can (a) be identified from that data; or (b) can be identified from that data and other information to which the university has or is likely to have access.

4.6. **University IT resources:** all University Licensed Software and databases; data and equipment; cloud storages (e.g., OneDrive for Business and Google drives), teleconferencing services (e.g., MS Teams, Zoom), support services and University connectivity to electronic information such as wired and wireless access to computer and telephone networks.

4.7. **University Licensed Software**: the software or licences acquired by the University for its community for purposes of teaching and research, and any other relevant activity that the University undertakes in accordance with its function as an institute of higher learning. Such software could be acquired under a single user licence or campus-wide licence. In all circumstances, the provision is ONE University Licenced Software per user (meaning ONE copy for each student, faculty, and staff member) regardless of the number of personal computers or devices owned or acquired by each person.

4.8. **Users:** persons who have been authorised to use any IT resources from any location and/or given SMU accounts to accomplish tasks related to their respective relationships and statuses with the University. Current faculty, staff, students, and other affiliates of SMU are considered to be authorised users.

5. POLICY

5.1. General Provisions

5.1.1. This AUP sets forth the general parameters of the acceptable use of University IT resources. Users should consult the respective governing policies, where available, for more detailed statements on permitted use and the extent of use that the University considers appropriate. In the event of conflict between IT policies, the respective governing policies will prevail.

5.1.2. Users have the responsibility to utilise the University IT Resources properly for purposes consonant with the mission of the SMU and in accordance with all Singapore laws, whether they are on SMU's campus or any of SMU's overseas and satellite offices.

5.1.3. Files that are used in the cause of official business are the property of SMU. The access and ability to alter another user's files does not in itself imply the permission to alter those files. Under no circumstances may a user alter a

file that does not belong to him or her without prior permission of the file's owner or of SMU.

5.1.4. **Security is the responsibility of all members of the SMU community**. The University shall conduct mandatory cybersecurity and data protection awareness programmes including mandatory cybersecurity awareness trainings and simulated phishing tests for employees, students, and contractors given access to SMU's IT resources. Additional training, where appropriate, will be conducted for users who repeatedly fail to get a passing grade for these mandatory trainings.

5.1.5. A user is not permitted to allow third parties any access to University IT Resources without prior written consent from the Chief Information Officer (CIO) of Integrated Information Technology Services (IITS) or his designee. In addition, a user is not permitted to transfer or sell/resell resources/materials sourced from University IT Resources to third parties in return for a fee or any other forms of payment-in-kind.

5.1.6. **Deleting Electronic Communications.** Users of the University IT Resources, particularly SMU's email system should be aware that electronic communications are not necessarily erased from the computer system when the user "deletes" the file or message. Electronic communication may continue to be stored on as a backup copy long after it is "deleted" by the user. As a result, deleted messages can be retrieved and recovered after they have been deleted within the retention period specified in the SMU email policy under "Backup and Retention of Email Data".

5.1.7. **Inspection of electronic Information.** Information located on University IT Resources may be subject to examination, as and when deemed necessary, to maintain or improve functioning of technology resources, investigate alleged violations of University policies and/or Singapore law and/or the relevant local laws applying to any overseas and satellite office of SMU, or to comply or verify compliance with the University policies and/or Singapore law and/or the relevant local laws for any overseas and satellite office of SMU.

5.1.8. **Disclosure.** In disciplinary proceedings, the University at its discretion may submit results of investigative actions to authorised University personnel and/or law enforcement agencies. Information and communications created with/communicated through University IT Resources may be subject to legally binding demands, such as court orders. Ultimately, it is the University that owns IT resources and all information and communications created through them, not the users who use them.

5.1.9. **Right of University Access.** The University reserves the right for authorised personnel to access a user's stored information to investigate cases of computing abuse and for systems maintenance purposes. Such access shall be approved by the University's Chief Information Officer and Vice-President, IITS, and in consultation with the President and University counsel when necessary.

5.1.10. **Right to Identity Verification.** The University has a right to request users of University IT resources to produce a valid University identification or other evidence of authorised use.

5.1.11. **Security and Privacy.** The University employs various measures to protect the security of its information technology resources and of user data and accounts. Users may have a reasonable expectation of unobstructed use of information technology resources, certain degrees of privacy, and protection from abuse and intrusion. Security precautions cannot always guarantee users security or privacy, however. Users should exercise caution in using University IT Resources to store and/or transmit confidential data.

5.1.12. **Disclaimer**. The University accepts no responsibility for any damage to or loss of data, hardware, or software arising directly or indirectly from use of the University's IT resources or for any consequential loss or damage. The University makes no warranty, express or implied, regarding the facilities offered or their fitness for any particular purpose.

5.2. **Specific Prohibitions on Use**

The following categories of use are inappropriate and prohibited:

5.2.1. **Use that attempts to damage the integrity of University or other IT Resources.**

a. University IT Resources may not be used for making unauthorised connection to, monitoring of, breaking into, or adversely affecting the system's performance, whether these system(s) belong to SMU (or its overseas and satellite offices) or not. The ability to connect to other systems via the network does not imply the right to use or connect to them unless given proper authorisation by the system owners.

b. Users must not steal or attempt to use methods of electronic or any means (e.g., software, hardware, or firmware) to eavesdrop on

passwords, content, and information that he/she/they is not authorised to access.

c. University IT Resources shall not be used to access, transmit, store, display, or request for inappropriate content such as obscene, pornographic, erotic, profane, racist, sexist, defamatory or offensive materials.

5.2.2. **Use that impedes, interferes, or otherwise causes harm to activities of others.**

a. Users must not engage in any actions that may interfere with a systems' supervisory or accounting functions, cause network congestion, or interfere with the work of others. Examples of prohibited conduct include placing unlawful information on the system, the transmitting of data or programmes likely to result in the loss of recipient's work or system downtime, sending of "chain letters" or "broadcast" messages to lists or individuals, or spamming or gaming via the SMU network.

b. Users must <u>not</u>:

i. develop and/or use programmes that may/will harass or harm other users of the system;
ii. develop and/or use programmes that may/will attempt to bypass system security mechanisms, or to steal passwords or data;
iii. develop and/or use programmes that, by design, attempt to consume all of an available system resource. Special arrangements can be made with IITS to accommodate such requests, where relevant and acceptable;
iv. develop or use programmes designed to replicate themselves or attach themselves to other programmes, commonly called "worms" or "viruses"; or
v. develop and/or use programmes designed to evade software licensing or copying restrictions.

5.2.3. **Use in Violation of the Law.**

a. **Unauthorised Access or Use.** It is a violation to use another person's account, with or without that person's permission. Users should use only the computer accounts they are individually authorised to use.

b. Users should not attempt to crack, guess, or otherwise capture another person's computer or account password.

c. **Disguised use.** Users must not conceal their identity when using the University IT resources, except when the option of anonymous access is explicitly authorised. Users are expressly prohibited from masquerading as or impersonating others or otherwise using a false identity.

d. **Use in Violation of Laws.** Users must not use their SMU account in any way that violates the laws of any country. The University expects its users to be cognisant with and to abide by the provisions stipulated in the Computer Misuse Act (Chapter 50A) and Cybersecurity Act 2018 and the Sedition Act (Chapter 290). This applies to all users on SMU's campuses, including in its overseas and satellite offices worldwide.

e. **Copyright.** Users are responsible for ensuring that no copyrighted material (including music, film, podcasts, books, games, and/or software) is downloaded using, published on, or distributed from SMU network without the copyright holder's permission. Users should be aware of the Copyright Act 2021 and the *Digital Copyright Policy* in force across the University. Users are also to note that in some instances and depending on the type of content, they may be subjected to the laws of a foreign jurisdiction.

f. **Personal Data Protection Laws**. Users are responsible for ensuring that the collection, use, and disclosure of Personal Data are in compliance with Singapore's Personal Data Protection Act 2012 (PDPA). Generally, users should obtain valid consent before they collect, use, or disclose Personal Data, unless any exception applies.

5.3. **Use in Violation of University Contracts.**

5.3.1. **Copyrighted Materials and Licensed Software, Programmes, and Data.**

Users must:

a. not transfer, duplicate, make available or obtain illegally, any copyrighted material including, but not limited to, agreements, license software, programmes, and data;
b. respect the rights of others by complying with all SMU policies and the relevant local law regarding intellectual property;
c. not install unlicensed or unauthorised software in the local (meaning desktop / laptop / computing devices) hard disk or on any University server drives.

5.3.2. **University Licenced Software.** SMU provides ONE (1) University Licensed Software license per user (meaning ONE (1) for each student, faculty, and staff member) regardless of the number of PCs, desktops, laptops and/or computing devices purchased via SMU's PC Tender. Users must:

a. uninstall all University Licenced Software from their PC when selling their PCs, upon termination of employment, or on leaving the University before graduation or upon graduation.

5.3.3. **Guidelines from Third-party or subscribed services**. When accessing other organisations' IT facilities and resources from the SMU network, users are responsible for abiding by these terms and conditions, relevant local laws, and the relevant policies of such other organisations.

5.4. **Use in Violation of University Policies.**

5.4.1. The privilege of using SMU equipment, including the network cabling, wireless access, computer and network systems and servers, broadcast media, and access to global communications and information resources is provided and granted by SMU, and may not

be transferred or extended by the campus community to people or groups outside the SMU, without prior authorisation.

5.4.2. **Account Removal**. Users must inform IITS to remove their SMU network configuration settings before they sell their PCs, upon termination of employment, or when they leave the university before graduation or upon graduation.

5.4.3. **Email and Web Policies**. Users must manage the use of email and web pages in accordance with the policies outlined in the *SMU Email Policy* and the *Web Policy.* Offenders will be held liable and sanctioned in accordance with the established University guidelines stipulated in the appropriate University policies. As a general guidance, the following conduct / actions are prohibited:

a. harassing, sending pornographic or defamatory materials / messages via e-mail or through posting to Web pages;
b. sending or posting forged e-mail ("masquerading"), web pages and/or newsgroups or chat group messages;
c. massive or unsolicited emailing without explicit approval from IITS;
d. flooding a user or a site with very large or numerous pieces of e-mail; and
e. sending or forwarding of confidential SMU information via e-mail.

5.5. **Responsible and Acceptable Use**

5.5.1. **Personal Account Responsibility**. Accounts are assigned to individuals and are not to be shared unless specifically authorised by the IITS. Users are solely responsible for all functions performed from the accounts assigned to them.

a. **Not allowing others to use personal accounts.** Users should safeguard their computer accounts and passwords. Peer pressure and/or negligence cannot be accepted as a defense of wrongdoing or misconduct.

b. Users are responsible for ensuring the absolute privacy and secrecy of their personal accounts and passwords by:
   i. changing any pre-assigned default password at the first possible opportunity; and
   ii. avoiding composing passwords based on their personal information (e.g., name, user ID, date of birth, etc).

5.6. **Responsibility for Safeguarding University IT Resources.**
Users should actively protect and defend University IT Resources against unauthorised access and use. Users should:

a. exercise appropriate data or character masking in transferring of any data of confidential and sensitive nature to minimise any data breach.

b. have the anti-virus software running on their PC and update the anti-virus signature file regularly.

c. regularly update the operating system (OS) updates or patches on their PC and other networked devices, including mobile phones.

5.7. **Use of University IT Resources by Faculty and Staff.**
The University provides IT resources and services to employees of the University for University business use. Prohibited use for employees on campus including all overseas and satellite offices of SMU includes, but is not limited to: political campaigning, solicitation, unauthorised financial gain, or conducting any business that has no official relationship with the University. Additional limits may be imposed by a supervisor, appropriate office, applicable University policies and/or Singapore laws and/or the relevant local laws.

5.8. **Use of University IT Resources by Students.**
Students' use of the University's IT resources must be for academic advancement in teaching and research and must adhere to the provisions of this AUP and other University policies such as the *Email Appropriate Use* and *Web* policies detailing specific use of the services. Uploading to or sharing of SMU Information or digital resources, (e.g., eLearn Course Materials) on non-SMU endorsed systems, social websites, or any other

public platforms (e.g. CourseHero, etc.) are strictly prohibited. Additional restrictions, where applicable, may be imposed by the Deanery of their respective schools and Dean of Students. Students may be subject to disciplinary action or legal penalties for any misuse or violation of this policy.

5.9. **Use of University IT Resources by Alumni.**
All SMU Alumni are given lifetime email and the use of this alumni email service is subject to the provisions of AUP, SMU Email Policy and Email Appropriate Use Policy. Alumni will no longer have access to SMU Intranets, their personal OneDrive for Business and Google drives and telecommunication services such as MS Teams and Zoom. Graduating students are strongly encouraged to download / backup their files in alternative media / storages before graduation.

5.10. **Use of University IT Resources by Former SMU Faculty and Staff.**
For security and cost accountability, the accounts of former employees will be deleted after 6 months and assigned storages reclaimed, unless excepted All requests for exceptions shall be duly approved by their Dean or Head of Department, who will assume the role of a sponsor and be accountable for the use and access by the ex-faculty / ex-staff throughout the period of exception. Exceptions, approved by the Chief Information Officer, shall be restricted to SMU Email service and the use subjected to this AUP, SMU Email Policy and Email Appropriate Use Policy. Former faculty and staff will not be part of SMU's distribution lists to receive University Information or have access to SMU Intranets or their personal OneDrive for Business and Google drives and telecommunication services such as MS Teams and Zoom.

5.11. **Backup.**
All data on the University computer systems is subject to backup at the sole discretion of the University. While the IITS will do its utmost efforts in ensuring the integrity of the backed-up data, IITS cannot guarantee that all backed-up data can be restored. Users therefore have the responsibility to backup their own critical files and systems.

5.12. **Policy Enforcement**

5.12.1. **Use is Revocable**. The use of software, databases, and/or computer and network resources at SMU is a revocable privilege. All faculty, staff, students, and authorised users using SMU's IT facilities are responsible for using these resources and facilities in an effective, ethical, and lawful manner. The use of University IT Resources has been made available for the purpose of supporting teaching, learning, research, professional development, and administration within SMU.

5.12.2. **Disciplinary measures** for violation are normally applied by the University office or department appropriate to the violation. Violators may be subject to additional penalties and disciplinary actions by the University and are also subject to international and Singapore laws governing interactions that occur on information technology systems and the Internet. The University may restrict or deny access to information technology resources temporarily or permanently, including prior to the initiation or completion of disciplinary procedures, when it appears necessary to protect the integrity, security, or functionality of the University's IT resources.

5.12.3. **SMU's right to Indemnity**. Failure by users to observe the policies within this AUP may also result (directly or indirectly) in SMU being involved in claims and/or suffering damages, losses and expenses. The user shall indemnify SMU and its officers from such claims, damages, losses, and expenses resulting from the user's intentional failure to observe the policies. In addition, the user must understand that SMU will cooperate in any official investigations in Singapore or any other relevant jurisdiction resulting from any breach of these policies and may, at its discretion, decide to furnish the relevant authorities/parties with the relevant information and your consent to any such disclosure shall be deemed by all users' acceptance of this policy.

5.12.4. **Waiver**. When restrictions in the policies interfere with the research, educational or service missions of the SMU, members of the SMU community may request for a written waiver from the Chief Information Officer of Integrated Information Technology Services or his designee.

6. ROLES AND RESPONSIBILITIES

6.1 All Users of University IT Resources

6.1.1 All SMU faculty, staff, students, and authorised users have an obligation to report any misuse of University IT resources or suspected breaches of conditions in this AUP to the IT Help Centre.

6.2 The University Administration and School Deanery shall:

6.2.1 Investigate and manage any and all breaches or suspected breaches of this AUP concerning Faculty members in accordance with established University guidelines and policies stated in the University Handbook.

6.3 Office of Dean of Students and Schools shall:

6.3.1 Investigate and manage of all breaches or suspected breaches of this AUP concerning students in accordance with established University guidelines and policies in the University Handbook.

6.4 Office of Human Resources shall:

6.4.1 Investigate and manage all breaches or suspected breaches of this AUP concerning SMU administrative staff and other non-faculty users in accordance with established University guidelines and HR policies.

6.5 Office of Integrated Information Technology Services shall:

6.5.1 Provide the technology support for investigating infringements or alleged breaches of this AUP; and

6.5.2 Execute the technology related sanctions, where applicable.

6.6 Office of Legal and General Affairs shall:

6.6.1 Provide legal guidance to the University.

7. POLICY REVIEW

SMU reserves the right to amend and update this AUP (and its Supplemental) and/or implement additional policies periodically. Although Integrated Information Technology Services (IITS) will inform users of policy changes, users on SMU's campuses (including all overseas and satellite offices) are presumed to be informed and must share the responsibility of staying informed about SMU policies regarding the acceptable use of the University IT Resources and complying with all other applicable policies.

SMU IT POLICIES & PROCEDURES

8. RELATED DOCUMENTATION, FORMS AND TOOLS

8.1. SUB-POLICIES AND SUPPLEMENTAL POLICIES

8.1.1. AUP Supplemental: University Licenced Software
This Supplemental provides additional guidance on removal of University licenced software due to conclusion or termination of program.

8.1.2. AUP Supplemental: Commercial Databases
This Supplemental provides further guidance on permitted access to SMU-subscribed Commercial Databases with which all SMU Authorised Users are expected to comply.

8.2. OTHER RELATED POLICIES AND APPLICABLE LAWS

- Computer Misuse Act (Chapter 50A)
- Cybersecurity Act Singapore 2018
- Copyright Act 2021
- Personal Data Protection Act 2012 (PDPA)
- Sedition Act (Chapter 290)
- Governance and Academic Policies Handbook - Home (sharepoint.com)
- Spam Control Act (Chapter 311A)
- Digital Copyright Policy
- SMU Email Policy

9. CONTACT INFORMATION

For queries regarding IT policies and security policies, please email ITpolicies@smu.edu.sg.

SMU IT POLICIES & PROCEDURES

10. DOCUMENT REVIEW / CHANGE HISTORY

Sno	Change Date	Version No	Reference	Description of Change	Effective Date
Change History records prior to 2020 are deleted for relevance and length					
10	27 Dec 2020	Version 2.5	Nil	Annual review, no change.	6 Jan 2021
11	30 Dec 2021	Version 2.6	All URL references to Copyright Act	Updated URL links for all references of Copyright Act (Chapter 63) to new Copyright Act 2021.	11 Jan 2022
12	30 Dec 2022	Version 2.7	Item 5.4	1. Removed “Users must not store personal confidential information such as credit / debit card details or passwords on University IT Resources”. 2. Added University’s rights to conduct CSAT training and phishing tests and users to take additional training if they don’t have the passing grade.	11 Jan 2023
13	8 Dec 2023	Version 3	Whole document	1. Policy updated to include SMU overseas and satellite offices. 2. Update URLs of IT policies due to IITS Intranet website revamp. 3. Expand definition of “University IT Resources” to include cloud storages (OneDrive for Business, Google Drive) and IT services (MS Teams and Zoom) 4. Include clause that Alumni have access only to lifetime email and no longer have access to SMU internal resources such as SMU Intranets, cloud storages (OneDrive for Business and	23 Jan 2024

SMU IT POLICIES & PROCEDURES

Sno	Change Date	Version No	Reference	Description of Change	Effective Date
				Google Drive), MS Teams and Zoom. 5. Include clause that former employee accounts will be deleted and storages reclaimed. Exceptions, if any, will be managed.	
14	30 Dec 2024	Version 3.1	Whole document	1. Reformat to enable AI bot search.	7 Jan 2025

SINGAPORE MANAGEMENT UNIVERSITY
ACCEPTABLE USE POLICY (AUP)
Supplemental on University Licenced Software

11. SUPPLEMENTAL ON UNIVERSITY LICENCED SOFTWARE

SMU has acquired the license for the use of a collection of software ("University Licenced Software") to facilitate and enhance the teaching and learning experience at SMU and extends to users the right to use the Software on a personally owned computer (in the case of students) or an institution-owned computer designated for the respective user's use, if the relevant user acceptance forms have been signed.

Details of the software Software Licensed by the University can be obtained at this url link: https://smu.sharepoint.com/sites/iits/SitePages/Services/Software-Apps.aspx

For avoidance of doubt, users do not own the license to the University Licenced Software; rather, a user is authorised to use the Software and associated media pursuant to the terms and conditions of the license(s) granted to SMU for the term of relevant software licence.

Whilst a user is a student, faculty, or staff (or any affiliate) at SMU and receives a copy of the University Licenced Software for use, the user must read and abide by the license(s) associated with the Software.

The licence to use the relevant University Licenced Software will terminate upon

(a) any event, with the exception of a student's graduation, which causes the user to no longer to be a student of SMU; or
(b) expiration of the relevant campus software licence ("Campus Licence") licensed period.

Upon such termination of the relevant University Licenced Software licence, the user must delete or remove the associated software immediately from his/her/their personally owned computer(s).

~~~~~~~~~~
~~~~~~~~~~

SINGAPORE MANAGEMENT UNIVERSITY
ACCEPTABLE USE POLICY (AUP)
Supplemental on Use of Commercial Databases

12. SUPPLEMENTAL ON USE OF COMMERCIAL DATABASES POLICY

Providers of commercial databases ("Commercial Databases"), who licence their databases for use in educational institutions, usually restrict the authorised user group to currently enrolled students and currently employed faculty and staff ("Authorised Users"). Additional restrictions may also apply.

To be permitted access to SMU-subscribed Commercial Databases, Authorised Users must agree to use such subscribed databases in the manner required by the respective providers. In particular, any use must be for personal and academic purposes only. "Personal use" may include preparation for job interviews, manuscript writing, and other activities strictly related to one's work at SMU. "Academic use" must be directly related to research and/or classroom activities.

Authorised Users are not allowed to use their database accounts for any other activities, including but not limited to consulting or other purposes, for which a fee is charged. The use of SMU-subscribed Commercial Databases to support internship work is strictly prohibited.

~~~~~~~~~~ ~~~~~~~~~~
~~~~~~~~~~

SMU IT POLICIES & PROCEDURES

APPENDIX A – ONLINE ACKNOWLEDGEMENT FORM

By clicking on the "I Accept" button in this webpage, I indicate that I have read, understood, and accepted the Acceptable Use Policy set out above, including any revisions to the same.

Name: _____

Faculty / Staff / Student Campus ID.: _____

School / Office: _____

Username issued: _____

Date: _____

Accept / Decline (buttons)

SMU IT POLICIES & PROCEDURES

APPENDIX B – USER ACKNOWLEDGEMENT FORM

I have read, understood, and accepted the Acceptable Use Policy set out above, including any revisions to the same.

Name: _____

Faculty / Staff / Student Campus ID.: _____

School / Office: _____

Username issued: _____

Signature: _____

Date: _____

Note:

Kindly return the signed blue copy to

Office of Integrated Information Technology Services (IITS),
c/o IT Help Centre
Singapore Management University