STUDENT ICT ACCEPTABLE USE AND SECURITY POLICY

ITS-SIAUSPOL-00-060617

DATE: 6 June 2017

INTI International University and Colleges
Student ICT Acceptable Use and Security Policy

Policy Statement

This IT Policy has been written for INTI International University and Colleges ("INTI"). It maintains a comprehensive policy and procedure on IT general usage and security for students.

Scope

This policy applies to all students with access to the ICT resources and facilities of INTI International University & Colleges ("INTI").

This IT Policy covers the Usage and Security of IT Services Resources, which includes University / College's computers, peripheral devices, networks and application accounts. IT Services provides and maintains this policy to support the mission of the institution and this policy applies to all students of or students connected to INTI International University and Colleges.

Entities Affected By This Policy

All entities under INTI International University and Colleges.

Who Should Read This Policy

Students who uses INTI's computers, peripheral devices, networks and application accounts.

Policy Information

Responsible Executive:	Vice President
Responsible Office:	IT Services
Issued Date:	6th June 2017

Contents

Revision History

Revision Number	Document Number	Description	Effective Date
00	ITS-SIAUSPOL-00-060617	New Release	6th June 2017

Recommendation and Approvals

Prepared by:

Dennis Wong
Director
IT Services
Date: 6th June 2017

Approved by:

Stella Chua
Vice President
IT Services
Date: 6th June 2017

1. Policy Statement

1. All Information and Communications Technology (ICT) facilities and resources of the INTI International University & Colleges ("INTI Group", "University", "College" or "INTI") are valuable assets and must only be used to perform learning-related or officially authorized activities.

2. The use of these ICT facilities and resources is a privilege granted by the INTI. All users are directed to use these ICT facilities and services properly within legal and proper boundaries.

3. Access and use of INTI computers, network, e-mail, information systems, online web services, databases and use of Internet or World Wide Web through INTI's network gateway (collectively referred as "System") is governed by this policy document.

4. Students (sometimes referred as "user" or "users") are to be familiar with the University/ College procedures and policies specifically on this policy document that covers the use of INTI System and all other ICT services and facilities as may be added from time to time.

5. Students' email and browsing activities on any websites or any illicit transaction made on INTI's network is monitored, tracked and filtered.

6. It is not possible to guarantee that users will not come across Internet resources that are offensive, profane or otherwise violate our ICT acceptable use and security policy. The ultimate responsibility for compliance lies with the user.

2. Computer / Network / Application Account Usage

1. Students are NOT PERMITTED to:

   (a) Make known their user ID and password to another person.

   (b) Use INTI'scomputers, network and application accounts for any activity that :-
      i. will or might compromise eitherINTI, the network, system or the learning activities of others.
      ii. is unlawful or for illegal purposes.

   (c) Keep any personal information or data in INTI's computers.

   (d) Erase, remove or destroy any information maintained in INTI's computer hard disk drives.

   (e) Violate system security or interfere with system performance or another user's use of INTI provided networks or systems.

   (f) Access other users' computer/network/application accounts, files or password without the prior consent of the party concerned, whether intentionally or not.

   (g) Copy, modify, pilfer or tamper with any electronic files without authorization.

   (h) To make any direct connections via machines and/or unauthorized ports to the server which will enable the user to make modifications to the system.

   (i) To make any unauthorized distribution of confidential information via the ICT system.

2. INTI's IT Services Management appointed staff have the full access privileges to student accounts for maintenance, upgrading, or correcting problems in INTI's network, online services and computers.

3. Students are responsible for all the information they access to, make available or distribute using INTI's computers, online services and network. INTI cannot be held responsible for the contents of e-mails that it provides.

4. Students are not to put up or make available (whether directly or indirectly) via INTI's computers or network, any opinion, information or material that may be:

   (a) Inappropriate, threatening, intimidating, harassing, profane, obscene, indecent, defamatory, derogatory or cause the discredit of any person or body in the eyes of the general public; or
   (b) Unlawful or that violates any applicable copyright, trademark, intellectual property or privacy laws.

5. Any students who suspect that their computer/network/application accounts have been accessed without their permission are expected to change their passwords and are strongly advised to report the suspected activity to INTI's IT Services Office.

3. Privacy and Logging

1. Ownership and Right to Monitor. All INTI ICT resources are owned by the University / College or members of INTI Group. The relevant owner reserves the right to monitor and/or log all network-based activity.

2. Implied User Agreement to Terms and Conditions. By logging-in to the INTI System / ICT facilities, the user agrees to the terms and conditions of this Policy.

4. Electronic Emails

1. INTI grants electronic mailboxes/ accounts to Students. Students are responsible on the contents and the maintenance of their electronic mailboxes.

2. Students are advised to:

   (a) Ensure that their individual mailbox size is within the disk quota provided.

   (b) Delete unwanted / junk email messages immediately.

3. Students are NOT PERMITTED to:

   (a) Send or disseminate to anyone via INTI's email accounts or online services (forums/chats/instant messaging), any message or e-mail that contains or could be viewed as defamatory, threatening in nature, racially disturbing or political, or sexually harassing. Any student who is aware of or who receives such messages or email are to immediately notify the Head of the IT Services Office.

   (b) Send or propagate chain letters via INTI.s e-mail facilities.

4. Use other non-INTI email services unless the use of these mails services are consistent with the learning activities of the students.

5. It is understood that email privileges including the disk files containing the email files of the user are surrendered upon separation, termination, or other circumstances deemed legal by INTI.

5. Software Copyrights and Downloads

1. Students are advised to:

   (a) Download file(s) which exceed 100MB from the Internet only during non-peak hours i.e. before 9:00am and after 5:00pm

   (b) Check for copyrights or licensing agreements on possible infringements when downloading a program or file for the Internet via INTI's computer / network facilities.

2. Students are not allowed to download or install any illegal, pirated or unlicensed software into INTI.s computers or via INTI network.

6. Virus Prevention and Protection

1. All users are not to introduce any viruses, Trojan horses, worms or spyware into INTI Systems.

2. Students are advised to activate virus scan program or virus scanner before opening any files from their portable disk, thumb drives, online storage and any email attachment using INTI's computers or online services.

3. Students must report any virus-like activities in INTI's computers to IT Services staff or IT Services Office.

7. INTI Websites

1. The College and members of INTI Group provides certain official websites that are legally hosted and registered under its domain name for the convenience and access by students/staff/public. Other web sites with different domain name associated with the INTI Group or its campuses available in the cyberspace are beyond the control of the University, College and INTI Group.

2. INTI requires that its content not appear within the web pages frames of others, nor accompanied in any way by third-party material that may create confusion, false or mistaken impression in the mind of the viewer about the University / College's affiliation or association with or endorsement of the third party website, web pages frame, services, products or any equivalent material.

8. Students' Participation in Non-INTI Websites

1. INTI does not stop students from participating, visiting or accessing other websites.

2. Any student with grievances/complaints is to voice to/ seek clarification from the University, College or INTI Group regarding any grievances/ complaints and should follow the existing INTI procedures for such purposes.

3. As such, the University, College and members of INTI Group takes a very stern view of any students who access other websites to post/ disseminate / make available unverified information / personal statements / material that:

   (a) Refers, identify, insinuates or mentions INTI name or any of its students in negative light; or

   (b) Derogate, defame or discredit the reputation or good standing of INTI or any of its students, referred as "**Damaging Material**".

9. Tolerated Use

1. Tolerated Use. Some ICT use, though unofficial, may be tolerated. These are considered privileges that may be revoked at any time. They include:

   (a) The use of email for personal communication;

   (b) The use of instant messaging and other social media applications; and,

   (c) The use of computers to play compressed audio / video files, optical disks or online media files.

2. Update to "Tolerated Uses" of ICT Facilities. The IT Services Office may, from time to time, issue a list classifying certain types of use under the category of "Tolerated Use". This list shall form part of this Policy and will be considered binding on all users.

10. User Responsibilities

1. Reporting of Troubles or Problems / User Cooperation. Users should report suspected abuse, especially any damage to, or problems with INTI ICT facilities. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions. Users should cooperate with INTI system administrators in any investigation of system abuse.

2. Contact Person or Unit. Exception and trouble reports must be made to the INTI IT Services Office so that appropriate action can be taken to solve the problem.

11. Prohibited Acts and Uses of the ICT Resources

1. General Principles in Proper Use of ICT Resources.

   (a) A user may access only those services and parts of the ICT System that are consistent with his/her learning activities. The ICT System should be used in accordance with its authorized purpose.

   (b) The following uses and acts, discussed in the following paragraphs, are considered violations in the use of the INTI ICT facilities and network:

      i. Uses contrary to laws, customs, race and ethical behavior;
      ii. Uses for personal benefit, business, or partisan activities;
      iii. Acts that damage the integrity, reliability, confidentiality and efficiency of the ICT System;
      iv. Acts that encroach on the rights of other users; and,
      v. Acts which violate privacy.

2. Uses Contrary to Laws, Customs, Racial and Ethical Behavior

   (a) Criminal Use. Users should not use the INTI System/ ICT resources for criminal activities.

   (b) Use of Copyrighted Material. Prohibited acts include but are not limited to:

      i. Copying, reproduction, dissemination, distribution, use, importation, removal, alteration, substitution, modification, storage, unloading, downloading, communication, publication or broadcasting of copyrighted material. Users should properly attribute any material they copy from or through the ICT System.

      ii. Infringement of intellectual property rights belonging to others through the use of telecommunications networks, which is a criminal offense under the Malaysian Laws.

   (c) Cheating. Prohibited acts include but are not limited to:

      i. Copying a computer file that contains another person's work and submitting it for one's own credit, or, using it as a model for one's own work, without the permission of the owner or author of the work;

      ii. Submitting the shared file, or a modification thereof, as one's individual work, when the work is a collaborative work, or part of a larger project.

3. Uses for Personal Benefit, Business or Partisan Activities

   (a) Commercial Use. Use of the ICT System for commercial purposes, and product advertisement, for personal profit, unless permitted under other written policies or with the written approval of a competent authority.

(b) Use of the ICT System for any partisan political activities. Use of ICT resources for religious or political lobbying, for disseminating information or gathering support or contributions for social, racial, political or cause-oriented group, which are inconsistent with the activities of INTI as an educational institution.

(c) Games and Entertainment. Use of ICT resources to play games, watch video, or any activity unrelated or inappropriate to the learning and responsibilities of the user, especially during class hours.

4. Acts that Damage the Integrity, Reliability, Confidentiality and Efficiency of the ICT System.

(a) Destruction, deletion, removal, modification, or installation of any computer equipment, peripheral, operating system, disk partition, software, database, or other component of the ICT System;

(b) Connection of any computer unit or external network to the ICT System without the permission of the Head of IT Services Office.

(c) Acts that attempt to crash, tie up, or deny any service on the ICT System, such as, but not limited to: sending of repetitive requests for the same service (denial of-service); sending bulk mail; sending mail with very large attachments; sending data packets that serve to flood the network bandwidth.

(d) Concealment, deletion, or modification of data or records pertaining to access to the ICT System at the time of access, or alter system logs after such access for the purpose of concealing identity or to hide unauthorized use.

5. Acts that Encroach on the Rights of Other Users

(a) Sending Unsolicited E-mail. Sending unsolicited mail such as chain-letters, advertisements, jokes, trivia, announcements to non-official groups or activities, offers, inquiries, and the like (spamming);

(b) Morally Offensive and Obscene Use. Accessing, downloading, producing, disseminating, or displaying material that could be considered offensive, pornographic, racially abusive, culturally insensitive, or libelous in nature.

(c) Sending Fraudulent and Harassing Messages. Sending messages which are fraudulent, maliciously harassing, obscene, threatening, or in violation of laws, administrative rules and regulations, or other policies of the ICT.

(d) Interfering or disruptive acts. Acts that interfere with or disrupt other computer users such as, but not limited to: sending messages through pop-up screens; running programs that simulate crashes; running spyware to monitor activities of other users.

6. Acts which Violate Privacy

(a) Hacking, Spying or Snooping.

i. Accessing, or attempting to gain, access to archives or systems that contain, process, or transmit confidential information. Authorized users should not exceed their approved levels of access, nor should they disclose confidential information to others.

ii. Decrypting, attempting to decrypt, or enabling others to decrypt such information, which are intentionally decrypted, password-protected, or secured. Encrypted data are considered confidential, and include, but not limited to: passwords, digital keys and signatures.

iii. Re-routing or capture of data transmitted over the ICT System.

iv. Accessing, or attempting to access, restricted portions of the system, such as e-mail lists, confidential files, password-protected files, or files that the user has no authorization to open or browse.

(b) Unauthorized Disclosure.

i. Copying, modification, dissemination, or use of confidential information such as, but not limited to : mailing lists; employee / student directories of any sort; INTI operations data; research materials, in whole or in part, without the permission of the person or body entitled to give it.

ii. Searching, or providing copies of, or modifications to, files, programs, or passwords belonging to other users, without the permission of the owners of the said files, programs or passwords.

iii. Publication on mailing lists, bulletin boards, and the World Wide Web (WWW), or dissemination of prohibited materials over, or store such information on, the ICT System. Prohibited materials under this provision include but are not limited to the following:

- Any collection of passwords, personal identification numbers (PINs), private digital certificates, credit card numbers, or other secure identification information;

- Any material that enables others to gain unauthorized access to a computer system. This may include instructions for gaining such access, computer code, or other devices. This would effectively preclude displaying items such as “Hackers Guides’, etc.

- Any material that permits an unauthorized user, who has gained access to a system, to carry out any modification of the computer programs or data stored in the system; and

- Any material that incites or encourages others to carry out unauthorized access to or modification of a computer system.

12. Disciplinary Action

1. The University, College and/or members of INTI Group reserves the rights to take steps to identify students / users who :

   (a) willfully post Damaging Material (as stated in items 3(a) and (b) of Section 8); or

   (b) who violates INTI ICT Policy or who improperly accesses or use INTI System / resources;

2. Any such students/ users identified under Item 1 above is subject to appropriate / stern disciplinary action which may include:-

   (a) putting a preventive suspension to the Internet and network privileges and/or access to INTI system of the offender/suspected violator

   (b) appropriate charges will be filed in court if offenses are punishable under applicable Malaysian Laws.

   (c) Other appropriate disciplinary action (which may include fine, suspension, expulsion and / or dismissal) against any student/ user who violates INTI ICT Policy.

3. Penalties for third parties. Any third party found guilty violating INTI ICT Policy through assistance, acts or collusion of any INTI student/ user will be barred from accessing any INTI ICT facility and system. The INTI student/ user who gave assisted or gave permission or colluded with a third party to access INTI System will also be held liable for all the violations that the third party may commit.

13. Enforcement Procedures

1. Implementing Unit. INTI Management reserves the right to form the Implementing Unit on needs basis. Such unit shall be primarily comprising of personnel from the IT Services Office and possibly together with selected personnel from Management and Faculty. The Unit shall be responsible for implementation, monitoring and imposition of penalties for this policy.

2. Jurisdiction of the Implementing Unit on Investigation.

   (a) Upon receipt of a report or complaint of misuse, the Implementing Unit shall conduct an investigation on the matter.

   (b) This Unit shall have the following authority:

      i. To summon the subject of the complaint to provide information.
      ii. To call and interview potential witnesses;
      iii. To inspect the user's files, storage devices, online storage, e-mail account and/or other computer-accessible storage media, or authorize system administrators to perform this inspection under its supervision;
      iv. To retain, as evidence, copies of user files or other data that may be relevant to an on-going investigation;
      v. To extend the suspension or restriction of a user's computing privileges for the duration of the investigation, or as may be deemed necessary to preserve evidence and protect the system and its users;

   (c) The implementing Unit shall submit the results and recommendations to INTI Management for appropriate action.

3. Appropriate Action. If the Implementing Unit have persuasive evidence of misuse of ICT resources, and if that evidence points to the computing activities or the computer files of an individual, INTI management shall take appropriate disciplinary action.

4. Filing of Charges. In cases where there is evidence of serious misconduct or possible criminal activity, appropriate charges shall be filed by INTI Management to the proper authorities. This, however, does not prohibit any aggrieved party or complainant other than INTI Management from instituting the filing of charges with the appropriate authorities.

5. External Legal Processes. The INTI System / Network does not exist in isolation from other communities and jurisdictions and their laws. Under some circumstances, as a result of investigations, subpoena or lawsuits, INTI may be required by law to provide electronic or other records or other information related to those records or relating to use of information resources. Use of the INTI computer resources and network is granted subject to existing Malaysian laws and regulations.

14. Waiver and Disclaimer

1. Disclaimer. While the University, College or INTI Group member takes careful steps to provide reliable and professional services in its ICT System, the University, College or INTI Group member does not guarantee, nor does it provide any warranties, as to the operating characteristics of its ICT resources and facilities to any of its users.

2. **Waiver**. The University, College or INTI Group member shall not be responsible for any loss or damage, whether direct or indirect, implied or otherwise, that may arise from the use of the INTI ICT facilities and resources by any person or entity.