UNIMAS ICT POLICY
UNIMAS ICT Usage Policy

VERSION : 2.6

DATE : 13 September 2023

Version	Comments	Approved Date	Approved By
1.0	New document	16 February 2015	JPICT
2.0	Added APPENDIX D: ACCEPTABLE USE POLICY FOR EMAIL BROADCAST	09 September 2015	JPICT
2.1	Refer to Borang Cadangan Pindaan Dokumen CITDS Bil 3/2017	4 May 2017	JPICT
2.2	Refer to Borang Cadangan Pindaan Dokumen CITDS Bil 6/2018	30 August 2018	JPICT
2.3	Refer to Minit Mesyuarat JPICT Bil. 5/2020 Ke-29 dan Borang Cadangan Pindaan Dokumen CITDS Bil 3/2020	13 October 2020	JPICT
2.4	Borang Cadangan Pindaan Dokumen CITDS Bil 3/2021	30 November 2021	JPICT
2.5	Borang Cadangan Pindaan Dokumen CITDS Bil 3/2023	23 March 2023	JPICT
2.6	Borang Cadangan Pindaan Dokumen CITDS Bil 6/2023	13 September 2023	JPICT

1. PREAMBLE

   This document provides users with principles, rules and guidelines pertaining to the proper use of existing UNIMAS ICT resources for teaching, research, administration and other scholarly activities in line with best practices and the current laws governing the use of ICT in the country. Users of ICT resources are advised to read and to be familiar with this policy. This policy is to be complied with, and any violation of the rules and procedures stated in this policy may result in disciplinary and legal actions.

2. POLICY
   a. This policy is an integral part to the UNIMAS ICT Governance Policy; therefore it must be read together with the said policy.

   b. This policy provides guidelines for lawful, efficient, economical, ethical, responsible use of ICT resources in UNIMAS.

   c. In addition to this policy, all activities of the university must be conducted in accordance with current legislations or cyber laws in Malaysia and those adhered to by the university but not limited to:

      i.   Computer Crime Act 1997
      ii.   The Copyright (Amendment) Act 2022
      iii. The Communication and Multimedia Act 1998
      iv.   The Electronic Government Activities Act 2007
      v.   Digital Signature Act 1997
      vi.   Digital Signature Regulations 1998 [P.U.(A) 359/98]
      vii. Electronic Commerce Act 2006
      viii. Payment Systems Act 2003
      ix.   Personal Data Protection Act 2010
      x.   Penal Code (including Chapter on terrorism & cyber-terrorism)
      xi.   Communications and Multimedia Content Code
      xii. Surat Aku Janji UNIMAS
      xiii. Dasar Keselamatan ICT (DKICT) UNIMAS
      xiv. Akta Badan-Badan Berkanun (Tatatertib dan Surcaj) 2000 [Akta 605] dan pindaannya
      xv.   Official Secrets Act 1972

3. DEFINITIONS

   a. Where the term "UNIMAS" or "Universiti Malaysia Sarawak" or "the university" is used, they refer to Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak and shall include its lawful representative, permitted assign and associated locations.

   b. The term "ICT resources" refers to any hardware or software, electronic resources, network infrastructure, application, services and facilities owned or managed or supplied by UNIMAS or one of its partners or third party individuals associated with the university through contracts or agreement.

c. The term "user" refers to any person (who is located within or outside the campus), who accesses any ICT resources.

d. The term "TAHODC" refers to the Tun Abang Haji Openg Digital Centre, UNIMAS.

e. The term "JKTICT" refers to the Jawatankuasa Kerja Teknikal ICT, UNIMAS.

f. The term "JPICT" refers to the Jawatankuasa Pemandu ICT, UNIMAS.

g. The term "portal" refers to the official website of the university – www.unimas.my.

h. The term "F/C/I/D" refers to Faculties/Centres/Institutes/Divisions.

i. The term "microsite(s)" refers to the websites managed by F/C/I/D.

j. The term "head(s)" refers to Heads of F/C/I/D.

k. The term "student" refers to any individual who registers for any course/program offered by the university.

l. The term "staff(s)" refers to individuals who are under employment with the university.

m. The term "third parties" refers to external entities that provide ICT services to/for the university.

n. The term "visitor" refers to an individual(s) who visits the university upon invitation or by request or by walk-in.

o. The term "custodian" refers to Bahagian Integriti, UNIMAS.

p. The term "social media" refers to any websites and applications that enable users to create and share content or to participate in social networking.

4. PRINCIPLES

a The ICT resources provided for by the university is to support work associated with the main functions of the university.
b Users of the ICT resources provided for by the university are responsible for their own actions when within the confines of the UNIMAS ICT network.
c All data contained within the university computer databases are considered private and confidential.

5. COVERAGE

    a   This policy applies to all users of ICT resources at UNIMAS.
    b   ICT security is addressed in the Dasar Keselamatan ICT UNIMAS (DKICT) which must be read along-side this policy.
    c   ICT governance is addressed in the UNIMAS ICT Governance Policy.

6. CONDITIONS OF USE

The following are strictly prohibited:
a. The use of ICT resources in any way to harass or discriminate any other individual(s);
b. Unauthorised access to ICT resources or restricted data;
c. The use of ICT resources for commercial use, endorsement deals or profit making unless approved by the university's management;
d. Pornography, gambling, spam or intentional spread of viruses;
e. Deliberate transmission or use of material, which infringes copyright held by another person or UNIMAS;
f. Violation of software licensing agreements;
g. Unauthorised manipulation or downloading of ICT resources that degrades or is likely to degrade system performance, network performance or to cause system malfunction;
h. Attempt to load unauthorised software, applications and games onto the university computer systems, unless approved by UNIMAS; and
i. Systematic or excessive downloading of electronic resources from the subscribed online databases or electronic journals using 'bots' or any similar software, or any manual means, (which results in a vendor license violation on the part of UNIMAS and/or its library).

7. MONITORING

a. The university reserves the right to track user behaviours within its ICT network.
b. The university reserves the right to generate detailed logs of user activity, behaviour or usage of ICT resources for any official use.

8. EXCEPTIONS

Any request for exception to this policy must be made in writing and addressed to the custodian.

9. RESPONSES TO BREACHES

   a. Infringement or non-compliance to the policies stated here will be investigated under the appropriate disciplinary procedures under the purview of the Bahagian Pengurusan Sumber Manusia (BPSM) and Bahagian Integriti (BI) or Pusat Khidmat Pelajar (PKP).

   b. Disciplinary actions will include but not limited to:
      i. Withdrawal of UNIMAS ICT facilities
      ii. Seizure of equipment that is in violation of the policy
      iii. Expulsion from the university iv. Termination of contract
      v. Any other disciplinary actions as contains in the Akta 605

   c. Where criminal offences are suspected or detected, an appropriate decision will be made in referring the matter to external law enforcement agencies for advice, guidance or prosecution under the relevant criminal law as stated in Clause 2(b).

   d. The university reserves the right to withdraw or restrict user access to ICT resources within the campus and from any remote location, external to the campus and take any action under the Akta 605.

10. RESPONSIBILITIES

   a. Users are to abide by the rules stated in this policy.
   b. Users must abide to the respective computer labs regulations.
   c. JPICT is responsible to enforce the statutes of this policy.
   d. The Heads are responsible to ensure all users under their charge comply with the ICT policy.
   e. Users are responsible to inform TAHODC of any suspected breaches.
   f. Visitors to the university, who are provided access to information or data contained within the ICT resources, are to sign the compliant document to the DKICT or to sign the Non-Disclosure Agreement (NDA); where applicable.
   g. The custodian of this policy is responsible to ensure that the policy document is reviewed annually by JPICT to reflect current practices and ICT enhancements.
   h. JPICT is responsible to present any proposed amendments of the policy document to the custodian.

11. DISCLAIMER

UNIMAS shall not in any event be liable for any damages, costs or losses (including without limitation direct, indirect, consequential or otherwise) arising out of, or in any way connected with, the use of ICT resources, or with delayed access to, or inability to use the services and whether arising in tort, contract, negligence, under statute or otherwise. Nothing in these terms excludes or limits liability for death or personal injury caused by the negligence of institution in providing this service.

12. OTHER ASSOCIATED DOCUMENTS

APPENDIX A : ACCEPTABLE USE POLICY FOR EMAIL

1. Users are required to use the email account provided by UNIMAS for any official correspondence.

2. Users are to refer to the ICT Governance Policy document for detailed information concerning their email accounts.

3. Students are responsible to activate and use their respective assigned university email accounts.

4. Users are responsible for the security of their passwords, email accounts and contents. Users are advised to refer to the Dasar Keselamatan ICT UNIMAS for details on security matters respectively.

5. Staff are eligible to apply for email redirection for a period of one month if they retire, resign or transfer to another agency from UNIMAS.

6. Users will not be added to any mailing list without his/her consent, unless the list is set up for official university business.

7. Users sending copies of documents in violation of copyright laws or inclusion of the work of others into email communications in violation of copyright laws is strictly prohibited.

8. Users must be aware that communications in the form of email may constitute "correspondence" and, therefore, become a public record and subject to inspection.

APPENDIX B : ACCEPTABLE USE POLICY FOR SOCIAL MEDIA

1. Users are duly responsible for all content they post on social media and will be treated as a personal statement, unless stated as authorized by the university.

2. Postings of confidential or proprietary information about the university, its faculty and departments, students, affiliates, its alumni or its employees are strictly prohibited.

3. Postings of statements, photographs or video or audio materials that could affect the reputation of the university and its partners are strictly prohibited.

4. Postings of embargoed information about the university, executive decisions or information about its people are strictly prohibited.

5. Postings of offensive or derogatory remarks about students, staff or other individuals, and obscene or derogatory images are strictly prohibited.

APPENDIX C : ACCEPTABLE USE POLICY FOR UNIMAS WIKI

1. UNIMAS Wiki services are provided as an online tool in support of collaborative work efforts at UNIMAS.

2. UNIMAS Wiki spaces will not be created for individual use.

3. Use of Wiki space must be consistent with the university's educational goals, as well as comply with local laws and university policies.

4. No confidential information may be contained in a Wiki space; the university reserves the right to remove any information deemed not suitable for publication in a Wiki space.

5. Wiki space owners must keep data space usage to a reasonable level for the purpose of their Wiki.

6. It is the responsibility of the user to ensure the accuracy of the information posted on a Wiki space.

APPENDIX D : ACCEPTABLE USE POLICY FOR EMAIL BROADCAST

1. All UNIMAS staff are required to receive university broadcast emails and are automatically added to the mailing lists using their UNIMAS email address.

2. It is the responsibility of every UNIMAS email user to regularly check his/her official university email account for broadcasted email messages.

3. Email broadcasts shall use, but limited to, any of the following emailing list :

   a. UNIMAS-All,
   b. UNIMAS-Students,
   c. Academicians

4. The following content shall be broadcasted through relevant mailing groups :

   a. Announcements that are time-critical in nature, safety related, or health related such as, but not limited to; IT system downtime, scheduled or non-scheduled maintenance of services or infrastructures, and closure of building or services related to the core functions of the university.

   b. Official statements from UNIMAS Corporate

   c. Updates on general orders or policies

APPENDIX E : ACCEPTABLE USE POLICY FOR RESEARCHER'S VIRTUAL MACHINE

1. UNIMAS shall provision Virtual Machine(VM) based on requested Operating System(OS). Any other software installation, configuration and administration are the researcher's responsibility.

2. Researcher's are allowed to use virtual machines on the UNIMAS's servers which includes access to the virtual machine through a secure connection, as well as technical support and maintenance provided by UNIMAS. However, UNIMAS does not guarantee the availability of the Services or continuous, uninterrupted or secure access to the Internet.

3. It is the responsibility of the researcher for the security of the virtual machine and any content hosted on it. UNIMAS recommends appropriate security measures are implemented, such as firewalls and virus scanners, to protect the virtual machine and data.

4. UNIMAS does not provide technical support for any installed software.

5. UNIMAS shall provide monthly backups of the virtual machine for the last two (2) months. However, it is the responsibility of the researcher's to keep their own copies of any important data stored on their virtual machine. UNIMAS will not be liable for any loss of data or other damage resulting from the failure of the backup system.

6. It is the responsibility of the researcher for the content and information hosted on the virtual machines, including any data, text, software, music, sound, photographs, graphics, video, messages, or other materials (collectively, "Content"). UNIMAS is not responsible for the accuracy, integrity, or quality of any Content hosted on the virtual machine.

7. In using the virtual machine hosting services, any illegal or unauthorized purpose are strictly prohibited, including but not limited to:

   (a) Distributing spam or other unsolicited emails;

   (b) Distributing illegal or copyrighted content;

   (c) Distributing viruses or other harmful software; or

   (d) Engaging in any other activities that may harm UNIMAS or its users.

   (e) Commercialization purposes

8. The virtual machine will be shut down after 6 months of inactivity. UNIMAS reserves the right to terminate your use of the virtual machine hosting service at any time, without notice, for any reason, including but not limited to violation of these terms and conditions.

9. UNIMAS provide the virtual machine hosting service on an "as is" and "as available" basis. Therefor makes no warranties, express or implied including but not limited to any implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

10. UNIMAS will not be liable for any damages of any kind arising from the use of the virtual machine hosting service, including but not limited to direct, indirect, incidental, punitive, and consequential damages.

11. The usage of domain name for the virtual machine is allowed provided that it is properly configured to point to the virtual machine. UNIMAS is not responsible for any issues related to the domain name used or its configuration.

12. UNIMAS reserves the right to assign an IP address for the virtual machine. The IP address assigned is prohibited to be used for any illegal or unauthorized purpose, including but not limited to spamming or hacking.

13. UNIMAS encourages the use of SSL certificates to secure data transmitted between the virtual machine and users. A third-party SSL certificate or obtain a free SSL certificate from Let's Encrypt is allowed to be used. However, UNIMAS is not responsible for any issues related to the installation or maintenance of the SSL certificate used.

14. UNIMAS reserves the right to modify these terms and conditions at any time, without notice. Continued use of the virtual machine hosting service after any changes have been made will constitute to the acceptance of the revised terms and conditions.