UNIMAS ICT POLICY

UNIMAS ICT Governance Policy

VERSION : **2.7**

DATE : **13 September 2023**

Version	Comments	Approved Date	Approved By
1.0	New document	16 February 2015	JPICT
2.0	Added APPENDIX G: GOVERNANCE POLICY FOR EMAIL BROADCAST	09 September 2015	JPICT
2.1	Refer to Borang Cadangan Pindaan Dokumen CITDS Bil 2/2017	4 May 2017	JPICT
2.2	Refer to Borang Cadangan Pindaan Dokumen CITDS Bil 7/2018	30 August 2018	JPICT
2.3	Refer to Minit Mesyuarat JPICT Bil. 1/2019 Ke-20 dan Borang Cadangan Pindaan Dokumen CITDS Bil 12/2019	24 Januari 2019	JPICT
2.4	Refer to Minit Mesyuarat JPICT Bil. 5/2020 Ke-29 dan Borang Cadangan Pindaan Dokumen CITDS Bil 3/2020	13 October 2020	JPICT
2.5	Borang Cadangan Pindaan Dokumen CITDS Bil 4/2021	30 November 2021	JPICT
2.6	Borang Cadangan Pindaan Dokumen CITDS Bil 2/2023	23 Mac 2023	JPICT
2.7	Borang Cadangan Pindaan Dokumen CITDS Bil 5/2023	13 September 2023	JPICT

1. PREAMBLE

This document provides ICT service providers in UNIMAS with principles, rules and guidelines pertaining to the proper governance of existing ICT resources to enhance effectiveness and efficiency in teaching, research, administration and other scholarly activities. It 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 Usage Policy; therefore it must be read together with the said policy.

b. This policy seeks to provide guidelines for lawful, efficient, economical, ethical, responsible governance 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 and services 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 Jawatankuasa Kerja Teknikal ICT, UNIMAS.

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

g. The term " website" 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 "service provider(s)" refers to F/C/I/D that provides ICT resources for the university.

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

m. The term "staff" refers to individuals who are under employment with the university or UNIMAS affiliates

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

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

p. The term "VC" refers to Vice Chancellor of UNIMAS.

4. PRINCIPLES

a. This policy ensures that proper governance of ICT resources is done in accordance to the aspirations of the university.

b. The ICT resources provided for by the university is to support work associated with the main functions of the university.

c. Service providers are responsible for their actions while in service to the university.

5. COVERAGE

a. This policy applies to all service providers of ICT services at Universiti Malaysia Sarawak.

b. ICT security is addressed in the Dasar Keselamatan ICT UNIMAS (DKICT) which must be read together with this policy.

c. ICT usage is addressed in the UNIMAS ICT Usage Policy.

6. CONDITIONS OF GOVERNANCE

The followings are subjected to the statutes contained in this policy :

a. Procurement of ICT resources using university funds;

b. ICT resources deployed within the UNIMAS ICT infrastructure or its affiliates; and

c. ICT resources that gain access to the UNIMAS ICT infrastructure.

7. MONITORING

a. The university reserves the right to track user behaviour within the ICT network.

b. The university reserves the right to generate detailed logs of user activity, behaviour or usage of ICT resources.

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. Where criminal offences are suspected or detected, appropriate actions 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(c).

c. The university reserves the right to withdraw or restrict user access to ICT resources within or outside campus and take any action under the Akta 605.

10. RESPONSIBILITIES

a. Service providers are to ensure that the services provided adhere to the policy.

b. JPICT is responsible to enforce the policies at their respective levels.

c. Third parties, who are provided access to information or data contained within the ICT resources, are to sign the compliant document to the DKICT and to sign the Non- Disclosure Agreement (NDA); where applicable.

d. The ICT Service Provider is responsible to ensure that the policy document is reviewed annually to reflect the current practices and ICT enhancements.

e. 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 : GOVERNANCE POLICY FOR ICT DISTRIBUTION

1. This policy is only applicable to ICT hardware purchased using the central budget of the university.

2. Any procurement for ICT hardware from Faculties/Centres/Institutes/Divisions is subject to the approval from JPICT.

3. The distribution of ICT hardware is guided but not limited to the following ratio (hardware:people):

I.	**Desktop Computer**	
	Desk-bound Staff	1:1
II.	**Printer/Copier 3 in 1**	
	Personal Assistant to VC/Deputy VC/Assistant VC/ Head of F/C/I/D/Office area	1:1
III.	**Copier 3 in 1**	
	General office / Academic office 1 or 1 for every 15 users	
IV.	**Notebook**	
	a. VC/DVC/Assistant VC	1:1
	b. Head of F/C/I/D	1:1
	c. Deputy Dean/Deputy Directors	1:1
V.	**Computer laboratory**	1:3

** Subject to management approval

4. Any ICT hardware distributed for a designated portfolio must be returned to respective PTj as stated in KEW.PA2 /KEW.PA3 upon the completion of his/her portfolio term.

APPENDIX B : GOVERNANCE POLICY FOR EMAIL

1. All UNIMAS staff and students are provided access to email services.

2. All email addresses are UNIMAS owned entity.

3. All UNIMAS application must relay emails through the authorised UNIMAS email gateway.

4. UNIMAS retains the right to publish and distribute email addresses as publicly available directory information.

5. UNIMAS will, subject to the requirements of this policy, use or disclose anything created, stored, sent or retrieved by users of its email systems, in (and only in) the circumstances set out below:

   a) when required by the laws of Malaysia;

   b) where UNIMAS with good reason believes violations of the laws of Malaysian or of University Regulations have occurred;

   c) where UNIMAS with good reason believes failure to act may result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or significant liability to UNIMAS or to members of UNIMAS community; and/or

   d) where critical operational circumstances exist, failure to act would seriously damage the ability of UNIMAS to function administratively or to meet its teaching, research or community services obligations.

6. Each registered user is allocated with one official email account. The same user may also be held accountable to administer another email account as instructed.

7. All email addresses will adhere to the following conventions:

   7.1. Without surnames:
   Father's name initial + user's first name initial + user's first name *@unimas.my*.

   Example for user name Abdul Ali bin Abu, internet mail address is *aaali@unimas.my*

   7.2. Using surnames:
   Initial of the user's name + surname *@unimas.my*.

   Example for user name Phua Liu Kang, internet mail address is *lkphua@unimas.my*

7.3. The administrator reserves the right to assign any appropriate username which are not covered in items 7.1 and 7.2.

7.4. Student will be issued with an email address in the following convention: Graduates, Pre-University Students, Undergraduate Students: *matric-number@siswa.unimas.my* (eg:*1234@siswa.unimas.my*).

APPENDIX C : GOVERNANCE POLICY FOR NETWORK EQUIPMENT AND NODES

1. Installation, changes or removal of any network equipment/nodes within UNIMAS is prohibited without prior approval by TAHODC.

2. The network nodes to be added, modified or terminated are only confined to those available within UNIMAS premises, excluding staff residence.

3. TAHODC reserves the right to remove, seize and block access to any installed network equipment that has not been approved by TAHODC without prior notice to the equipment owner.

4. TAHODC reserves the right to revoke approval of installed network equipment.

5. TAHODC is assigned administrator/root level account and the right to access network equipment. The users are not allowed and will not be given any administration access to the network equipment without TAHODC consent.

6. TAHODC reserves the right to approve, hold or reject requests for network equipment based on and not limited to:
    a. Technical feasibility
    b. Strength and validity of application justification
    c. Compliance to UNIMAS standard and existing infrastructure
    d. Other significant consideration

7. TAHODC has the right to remove any existing configuration in the network equipment.

8. UNIMAS will not be held responsible to damages caused by the approved or nonapproved network equipment. The liability is fully on the user of the network equipment.

APPENDIX D : GOVERNANCE POLICY FOR APPLICATION DEVELOPMENT AND MAINTENANCE

1. Any new request for application development from a process owner should be submitted to TAHODC (attn.: Secretariat, Jawatankuasa Saringan Pembangunan Aplikasi). Justifications for the request should include evidence of compliance to an existing policy and the availability of a Standard Operating Procedure (SOP) and Process Flow for the requested application.

2. For any ad-hoc application development request which requires speedy development within a stringent time-frame, the process owner must accept any possible risks of the system.

3. Each product/system development should be considered for its potential effects on the confidentiality, integrity and availability, both directly and indirectly in conjunction with other systems and assets.

4. Use of a separate test environment should, if at all possible, be used to replicate the live system to allow assessments to be conducted without risk of adverse effect.

5. The use of personal or sensitive information for test purposes is prohibited.

6. Process owners are responsible for the validity and quality of data for the respective system.

7. The criticality of a system in terms of the maximum tolerable times to restore from critical incidents needs to be established and agreeable by the process owner.

8. Appropriate backup, recovery and contingency procedures should be utilised during development or maintenance.

9. Access to development tools and system utilities will be restricted to respective development teams and will not be accessible from operational systems.

10. Access to program source code is restricted to the permitted development team.

11. If bugs are discovered in a software application or system then any solution to the bug should be tested and installed at the earliest opportunity.

12. System developers are responsible for safeguarding the confidentiality of information during the complete ICT systems development lifecycle.

13. During disposal of any system, if required, data and information may need to be archived in line with statutory requirements and internal/external audit requirements.

14. The integrity, confidentiality and availability of data from decommissioned application systems and translation to new systems needs to be assured during and after the archive process.

15. All Navigation (menu and links), labels and notices of UNIMAS Application System shall be written in English except for Student Management System (for Undergraduate).

APPENDIX E : GOVERNANCE POLICY FOR UNIVERSITY'S WEBSITE

1. Postings for event announcements/news on the portal shall be reviewed by UNIMAS Corporate

2. Banners, News and Announcement are subjected to the regulations imposed by UNIMAS Corporate.

3. The Jawatankuasa Laman Web is responsible for the design, implementation and assessment of the university's Website.

4. The Jawatankuasa Penjenamaan UNIMAS is responsible for the overall look and feel for the university main website

5. The design and writing of the published content for microsites are the responsibilities of the various F/C/I/D webmaster, which is answerable to Jawatankuasa Laman Web.

6. Microsites must reside in the official web-servers of the university.

7. Any and all other websites that represent the interest of the university; local or international sanctioned events or programs, that bear the UNIMAS emblems or logos must reside in the official university's web-servers and must adhere to the guidelines set by UNIMAS Corporate.

8. The guidelines relevant to this policy are:

    a. Guidelines for Web Site Presentation,
    b. Guidelines for Microsites Information,
    c. Guidelines for Information Quality,
    d. Governance Policy for Microsites,
    e. UNIMAS Brand Manual

9. The content placed on the portal, microsites and other related websites must adhere to rulings and decisions, but not limited to, the followings:

    a. The Malaysian Communications and Multimedia Content Code issued by the Communications and Multimedia Content Forum (CMCF);

    b. The Malaysian Government Portal and Website Assessment by Multimedia Development Corporation (MDEC); and

    c. Jawatankuasa Laman Web UNIMAS.

APPENDIX F : GOVERNANCE POLICY FOR TECHNICAL SPECIFICATION OF ICT PROCUREMENT

1. Procurement for any new ICT resources; technical specification approval shall be obtained from JKTICT and endorsed by JPICT.

2. JPICT reserves the right to advice on any potential issues or considerations pertaining to ICT procurement on recommendation made by JKTICT.

3. JKTICT reserves the right to approve, hold or reject ICT technical specification submittion based on but not limited to :

    a) Technical feasibility;

    b) Strength and validity of application justification;

    c) Compliance to UNIMAS standard and existing infrastructure; and

    d) Other significant considerations.

APPENDIX G : GOVERNANCE POLICY FOR EMAIL BROADCAST

1. The university's email broadcast service is to be used for the university's purposes and should directly support or relate to university activities.

2. The email broadcast service shall not be used for personal use, illegal activities, commercial purposes which are not associated with the university, political activism, incitation of racial or religious disharmony, dissemination of pornographic material or other uses that violate other university policies or guidelines.

3. Announcements that contain messages intended for and relevant to at least 80% of the university staff/students shall be considered for broadcast via email at purview of UNIMAS Corporate.

4. The following shall be recognised as official channels but limited to, for email broadcast in the university:
   a. UNIMAS-All
   b. UNIMAS-Students
   c. Academicians

5. The following are descriptions about the categories of messages for broadcast 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. Messages that contain official statements from the top management of the university; and

   c. Updates on general orders, policies or media coverage.

6. UNIMAS Corporate is responsible for publishing email broadcasts through the UNIMASAll channel.

7. Other departments or sections of the university are permitted to do broadcast emails with prior approval from the university's top management.

8. It is the responsibility of every message publisher to ensure that the content is factually correct and has been reviewed for appropriateness, relevance, readability, grammatical accuracy and layout before broadcasting.

9. UNIMAS Corporate reserves the right to approve the publishing of any email deemed appropriate for circulation to the staff of the university, remove, disallow, edit, and debunk any broadcast emails that are inappropriate or contain information that may be better communicated through an alternate medium.

APPENDIX H : GOVERNANCE POLICY FOR CODE OF CONDUCT – STUDENTS

1. Students shall use the UNIMAS computing facilities and information resources, including hardware, software, networks, and computer accounts, in a responsible manner.

2. The use of these facilities is a privilege granted to students to support their studies at UNIMAS.

3. Students shall not misuse their privileges including but not limited to:

   3.1 Using facilities for the purpose other than those for which they were intended or authorised;

   3.2 Illegally copying licensed software or violating any software license agreement or copyright;

   3.3 Storing or installing files on any UNIMAS equipment that are not directly related to their studies;

   3.4 Accessing any computer or information without proper authorisation;

   3.5 Disclosing their password to anyone or anybody's password other than theirs;

   3.6 Circumventing normal resource limits, procedures or security regulations;

   3.7 Taking advantage of another user's naiveté or negligence to gain access to the user's account and information or logging into another user's account or seeking to masquerade as another user;

   3.8 Sending any fraudulent electronic transmission or accessing illegal information;

   3.9 Compromising the privacy of others;

   3.10 Violating and disrupting another users' rights when using the university's facilities (example: harassing, libellous or disruptive to others, game playing, chatting unnecessarily that is not related to studies, sending excessive messages or huge multimedia files, printing excessively, modifying system facilities, attempting to crash or tie up facilities, relocating facilities, damaging or vandalising facilities).

4. Processes/programs on UNIMAS machine or equipment may be terminated, shutdown or modified without notification.

5. If, in the best judgment of the System Administrator, with the consent of the Vice Chancellor, that certain privileges or actions threatening other users or if a system or network is in imminent danger of crashing, the administrator can monitor, record, view, copy and thereby log all electronic traffic that were directly or indirectly generated and show these systems logs to associated personnel as required.

6. Access to the facilities that have been granted can be suspended or revoked at any time without notification.

7. All abuse and misuse of the ICT facilities will be reported to the Pusat Khidmat Pelajar (PKP) reserves the right to take appropriate actions, depending on the severity of the case, such as, suspension of their account for an indefinite period, paying a fine, or terminating their studies in the University.

APPENDIX I : GOVERNANCE POLICY FOR CODE OF CONDUCT – STAFF

1. Staff shall use the UNIMAS computing facilities and information resources, including hardware, software, networks, and computer accounts, in a responsible manner.

2. The use of these facilities is a privilege granted to staff to support their works at UNIMAS.

3. Staff shall not misuse their privileges including but not limited to:

   3.1 Using facilities for the purpose other than those for which they were intended or authorised;

   3.2 Illegally copying licensed software or violating any software license agreement or copyright;

   3.3 Storing or installing files on any UNIMAS equipment that are not directly related to their works;

   3.4 Accessing any computer or information without proper authorisation;

   3.5 Disclosing their password to anyone or anybody's password other than theirs;

   3.6 Circumventing normal resource limits, procedures or security regulations;

   3.7 Taking advantage of another user's naiveté or negligence to gain access to the user's account and information or logging into another user's account or seeking to masquerade as another user;

   3.8 Sending any fraudulent electronic transmission or accessing illegal information;

   3.9 Compromising the privacy of others;

   3.10 Violating and disrupting another users' rights when using the university's facilities (example: harassing, libellous or disruptive to others, game playing, chatting unnecessarily that is not related to studies, sending excessive messages or huge multimedia files, printing excessively, modifying system facilities, attempting to crash or tie up facilities, relocating facilities, damaging or vandalizing facilities).

4. Processes/programs on UNIMAS machine or equipment may be terminated, shutdown or modified without notification.

5. If, in the best judgment of the System Administrator, with the consent of the Vice Chancellor, that certain privileges or actions threatening other users or if a system or network is in imminent danger of crashing, the administrator can monitor, record,

view, copy and thereby log all electronic traffic that were directly or indirectly generated and show these systems logs to associated personnel as required.

6. Access to the facilities that have been granted can be suspended or revoked at anytime without notification

7. All abuse and misuse of the ICT facilities will be reported to the Bahagian Pengurusan Sumber Manusia (BPSM) and Bahagian Integriti (BI) for further actions. BPSM and BI reserve the right to take appropriate actions, depending on the severity of the case, such as, suspension of their account for an indefinite period, paying a fine, or terminating their service in the University.

APPENDIX J : GOVERNANCE POLICY FOR MOBILE APPLICATION

UNIMAS will not permit any external parties to access and operate UNIMAS' Google Play, Apple App Store, and Huawei Web Gallery for any app-publishing or related activities.