EMAIL
UNIMAS WEB
ICT DISPOSAL
SOFTWARE LICENSING
NETWORK EQUIPMENT
CODE OF CONDUCT

# UNIMAS ICT POLICY

## 2010 REVISION

MICRO-SITE INFORMATION
MOBILE COMPUTING
ICT Network Management
INFORMATION QUALITY
DATA CENTRE MANAGEMENT
STORAGE DEVICES
ICT SECURITY
NETWORK INFRASTRUCTURE
ICT DISTRIBUTION
ACCEPTABLE ICT USE
EMAIL ATTACHMENTS
WEB SITES PRESENTATION
GOVERNANCE OF MICROSITES

# FOREWORD

This latest edition of UNIMAS ICT Policy 2010 is produced based on additions, revisions and amendments to the first edition of the policy document that was approved by the 74th Senate on 15th December 2005. This latest policy takes into consideration the new changes and developments that have occurred in the field of information and communication technologies, such as, the availability of new and improved version of hardware and software.

This policy is meant to provide users in UNIMAS with guidelines, rules and procedures pertaining to the proper use of existing ICT services and facilities to enhance effectiveness in 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 services and facilities are advised to read and to be familiar with this policy. 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.

I would like to take this opportunity to thank all members of the UNIMAS ICT Policy Committee who have spent a lot of time and effort in revisiting the old policy and giving valuable inputs that have contributed to the final version of this latest policy. I hope that this form of cooperation and team spirit will continue in the future.

**Prof Dr Peter Songan**
Deputy Vice Chancellor (Research & Innovation)
Chairman of TECIS

## SUMMARY OF ICT POLICIES

| | Policy No | Name of Policy | Summary | Applied To | Page |
|---|---|---|---|---|---|
| 1. | ICT001 | ICT Distribution Policy | This Policy details the distribution policy of computers and its peripheries to UNIMAS staff and student-based facilities. | Staff and Students | 1 |
| 2. | ICT002 | Acceptable ICT Use (Staff) Policy | Policies and procedures on acceptable use of ICT by UNIMAS staff. | Staff | 3 |
| 3. | ICT003 | Email Policy | This Policy applies to all email systems established by Universiti Malaysia Sarawak for staff and students. | Staff and Students | 7 |
| 4. | ICT004 | Email Server Policy | To reduce virus infections on campus and to stop inappropriate email relaying, all existing email servers on campus must relay external email through the central mailhubs and must also use those systems to scan incoming email. All email servers should be centralized and maintain at the Data Center. | Staff | 13 |
| 5. | ICT006 | UNIMAS Web Policy | This policy is designed to ensure that:<br>1. all Web sites operated from the University must follow the guidelines set by UNIMAS;<br>2. the presentation of all Web sites should maintain the University's identity; | Staff | 15 |
| 6. | ICT007 | Security for Mobile Computing and Storage Devices | The policy applies to anyone who utilizes mobile computing devices to access UNIMAS's information and computing environment. This is to ensure security of Protected Confidential Information that may be stored on those devices. | Staff | 17 |
| 7. | ICT008 | ICT Disposal Policy | Procedures and regulations that must be adhered to in order to have the ICT equipments disposed. | Staff | 20 |
| 8. | ICT009 | Software Licensing Policy | Governance of software licensing and copyright policy for all software used for administrative and educational purposes in UNIMAS. | Staff and Students | 22 |
| 9. | ICT010 | ICT Network Management Policy | Enforcing controls on any adding/modifying/terminating network nodes to ensure the | Staff | 24 |

**UNIMAS ICT POLICY MEMBERS 2010**

1. Assoc. Prof. Dr. Hong Kian Sam
2. Assoc. Prof. Dr. Mohd Ibrahim Safawi b. Mohd Zain
3. Assoc. Prof. Dr. Alvin Yeo
4. Assoc. Prof. Dr. Chen Chwen Jen
5. Pn. Hajjah Ratifah bt. Alias
6. Cik Azeemah bt. Ahmad
7. Pn. Laila bt. Abang Ahmad
8. En. Harun b. Maksom
9. Pn. Korina Ibrahim
10. Tn. Haji Lawrence b. Abdullah
11. En. Alhadi b. Bujang
12. En. Fadly Faizal b. Rakawi

## ICT Distribution Policy

---

**References:**

Policy Number: ICT001
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: 1
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: Centre for Information and Communication Technology Services
Access Level: All staff and students

---

**Preamble:**

Students and staff at Universiti Malaysia Sarawak are given access to UNIMAS ICT services and facilities to ensure effectiveness in teaching and learning, research and other scholarly activities.

---

**Policy:**

This Policy details the distribution policy of computers and its peripheries to UNIMAS staff and student-based facilities. The ratios of computers and its peripheries to user for the various categories of use are as follows:

| | |
|---|---|
| **Computers** | |
| Tutors & fulltime postgraduate students | 1:1 |
| Part-time postgraduate students | 1:4 |
| Administrative Officers/Head of F/C/I/D | 1:1 |
| Admin-PA | 1:1 |
| Admin-general offices- based on function | 1:1 |
| **Printers** | |
| Dean/HOD/Office area | 1 |
| General office | 1 |
| Academic office & Labs | 1 for every 15 PCs |
| **Notebooks Entitlement** | |
| VC/TNC/Directors/Head of F/C/I/D | 1:1 |
| Deputy Deans and Deputy Directors | 1:1 |
| Academic staff | 1:1 |

Policy guideline is to provide information regarding computer laboratory ratio in UNIMAS.

1. **Teaching Laboratory**

| | |
|---|---|
| a. Science & Technology | 1:5 |
| b. Social Science | 1:10 |
| c. Medical Related | 1:10 |
| d. Centre For Pre-University Studies | 1:15 |
| e. Postgraduate | 1:5 |

2. **Undergraduate Laboratory**

| | |
|---|---|
| a. General Lab | 1:15 |

---

**Procedures/ Guidelines:**

1. **ICTcode001**: Code of Conduct for Staff
2. **ICTcode002**: Code of Conduct for Students
3. **ICTguide001**: Guidelines for the Use of Email
4. **ICTguide002**: Guidelines for Email File Attachments

---

**Definitions:**

1. **UNIMAS students**: All students including undergraduates, post graduates, and students from other universities attached to UNIMAS.
2. **UNIMAS staff**: All contract and permanent staff at UNIMAS, including research assistant and visiting scholars or staff from other government agencies attached to UNIMAS.
3. **ICT**: Information and Communication Technologies

---

**Related Policies & Documents:**

---

**Notes:**

## Acceptable ICT Use (Staff) Policy

---

**References:**

Policy Number: ICT002
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: 1
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff

---

**Preamble:**

Members of staff at Universiti Malaysia Sarawak are given access to the ICT services and facilities of UNIMAS to ensure effectiveness in teaching, research and other scholarly activities.

However, UNIMAS recognises its responsibility to ensure the appropriate use of electronic information systems provided for the academic, administrative and other scholarly activities of UNIMAS. UNIMAS must be protected from damage or liability resulting from the unlawful or inappropriate use of its facilities.

Therefore, all staff members are required to abide by the policies and procedures of UNIMAS on the acceptable use of ICT and any other law of the country.

In addition, if a staff member is using his or her own computer to access the network and Internet services of UNIMAS, UNIMAS also reserves the right to check what the staff has downloaded and stored, if it has reasonable grounds for believing that the staff may have infringed copyright or done some other illegal act.

---

**Policy:**

This Policy applies to all UNIMAS staff.

ICT facilities are provided for use in the academic and administrative activities of UNIMAS. These resources are not provided for recreational or personal use.

While at UNIMAS, staff must use either his or her own computer or UNIMAS ICT services/facilities for acceptable use. The specific activities that constitute unacceptable use include but are not limited to:

- Unauthorised use of another person's identity or an authorisation code
- Unauthorised sharing of accounts/passwords (without management authorisation)

- Deliberate transmission or use of material which infringes copyright held by another person or UNIMAS
- Hacking into, meddling with or damaging any other computer or service or use any hacker tool without written permission from UNIMAS
- Harassing or obstructing any person using ICT facilities and services
- Deliberate, unauthorised corruption or destruction of ICT systems or data (including deliberate introduction or propagation of computer viruses)
- Deliberate, unauthorised access to facilities or data
- Unauthorised use of data or information obtained from information systems
- Creation, transmission, or soliciting of material which is obscene, defamatory, discriminatory in nature, or likely to cause distress to some individuals or cultures, where such material is not a legitimate part of education or research (if the material is a legitimate part of education or research, an appropriate warning should be given)
- Violation of software licensing agreements
- Transmission of unsolicited commercial or advertising material
- Unauthorised disclosure of confidential information
- Operation of an ICT system or other equipment, which presents a threat to the confidentiality, integrity or availability of ICT services of UNIMAS
- Unauthorised manipulation of ICT facilities that degrades or is likely to degrade system performance, such as manipulation of excessively large files or creation of programme (such as viruses) which replicate themselves, cause damage or corruption of data or a programme which runs in an infinite loop
- Attempting to load unauthorised software programme including server software, applications and games onto university computer systems

Additionally, participation in the following practices should be demonstrably associated with current study and research activities:

- Downloading of materials from NGO's or political parties
- Viewing and/or downloading of movie and video material, including trailers and sample clips
- Accessing and/or downloading of music, including MP3s
- Listening to music / radio through the internet
- Watching online news broadcasts
- Accessing and/or downloading adult material, including pornography
- Using social networking tools
- Accessing and/or downloading and/or disseminating of information/articles which violate Malaysian Sedition Act

Additionally, UNIMAS has a policy of zero tolerance to the accessing and downloading of pornography, unless it can be clearly demonstrated that it is required for teaching, learning or research purposes.

Users must also comply with related policies and procedures and other specific instructions of UNIMAS as released by CICTS. If any unacceptable use of UNIMAS ICT systems is detected, it must be reported to CICTS. Violations of this Policy may result in legal and disciplinary action according to Malaysian Law, Government Act, and University regulation.

Queries, complaints and concerns should be directed to the ICT Service Desk maintained by CICTS which is available through Anjung UNIMAS.

**Network Monitoring**

UNIMAS reserves the right to monitor any and all aspects of its electronic information systems to determine if a user is acting unlawfully or violating this policy, or any other policy or rule of UNIMAS. Such monitoring may include individual login sessions, the Internet sites visited by users and the content of electronic communications. Monitoring may be done with or without prior notice to the user.

**Compliance**

Users failing to comply with this policy or associated policies and guidelines may forfeit their access to ICT facilities. UNIMAS may take remedial action, suspend user access and/or disconnect or disable relevant ICT systems or other equipment, with or without prior notice in response to suspected breaches of this policy. Serious breaches by staff will be addressed by the relevant staff disciplinary procedures.

**Exceptions**

Requests for exceptions to this policy may be authorised by TECIS. Each request must be made in writing and will be evaluated based on the case presented to support it.

**Responsibilities for Implementation and Review**

Users of university IT facilities are responsible for adhering to the provisions of this policy. All head of F/C/I/D or equivalent will be responsible for the implementation of this policy in their area.

---

**Procedures/ Guidelines:**

1. **ICTcode001**: Code of Conduct for Staff
2. **ICTcode002**: Code of Conduct for Students
3. **ICTguide001**: Guidelines for the Use of Email
4. **ICTguide002**: Guidelines for Email File Attachments
5. **ICTguide003**: Guidelines of UNIMAS Websites Presentation

---

**Definitions:**

1. **CICTS**: Centre for Information and Communication Technology Services
2. **TECIS**: Technical Committee for Information and Communication Technology Services
3. **ICT**: Information and Communication Technologies
4. **UNIMAS staff**: All contract and permanent staff of UNIMAS, including research assistants and visiting scholars attached to UNIMAS for a period exceeding 6 months

---

**Related Policies & Documents:**

1. **ICT003**: Email Policy
2. **ICT004**: Email Server Policy
3. **ICT005**: Virus Protection Policy
4. **ICT006**: UNIMAS Web Policy

---

**Notes:**

## Email Policy

**References:**
Policy Number: ICT003
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: -
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce 2010
Access Level: All staff and students

**Preamble:**

The use of email services is not seen as a privilege, but as a requirement for UNIMAS community. Email use raises a number of issues such as privacy of messages, email address publication, acceptable use, harassment and storage. It is important that all email users are aware of the characteristics of email in order to make effective use of this mode of communications. All email users must be aware that communicating electronically has legal ramifications.

1. Users who do not adhere to the above email policies and guidelines will be responsible for their own actions. UNIMAS will not be liable for any consequences arising from the actions.

**Policy:**

This Policy applies to all email systems established by UNIMAS for staff and students. Persons who are given access to UNIMAS email system are expected to familiarize themselves with, and abide by, the policies in this document. Violations of this Policy may result in legal or disciplinary action in accordance to Malaysian Law, Government Act, and University's regulations.

### 1. SIZE OF MAILBOXES

Each registered user is allocated with only one mailbox. The users have to manage their own mailboxes. Users are encouraged to configure mailboxes to purge deleted messages upon exiting. Allocations of mailbox size are as follows:

- Vice Chancellor, Deputy Vice Chancellors – 1.5GB
- Deans, Directors, Registrar, Bursar, Chief Librarian – 1.2GB
- Lecturers – 1 GB
- Tutors – 75MB
- Professionals – 70 MB

- Other employees - 50 MB

Additional mailbox size required for business purposes can be considered on case-by-case basis. However approval from Head of F/C/I/D is needed.

## 2. EMAIL ADDRESSES

**Staff email addresses**:

All email addresses are UNIMAS owned entity. As such UNIMAS retains the right to publish and distribute email addresses as publicly available directory information.

All email addresses will adhere to the following conventions:

- For those who do not use surnames such as the Natives and some Indians:
  Father's name initial + user's name @ F/C/I/D initial.unimas.my.
  Example for user name Ali bin Abu, internet mail address is aali@cicts.unimas.my

- For those who use surnames such as the Chinese or English: Initial of the user's name + surname @ F/C/I/D initial.unimas.my.
  Example for user name Phua Liu Kang, internet mail address is lkphua@cicts.unimas.my

The administrator reserves the right to assign any appropriate username for other addresses which are not covered above.

**Student email addresses:**
Similarly, a student's electronic mail address is also Universiti Malaysia Sarawak entity. As such UNIMAS has the right to publish and distribute their addresses as publicly available directory information. Student will be issued with an email address in the following convention:

- Postgraduates, Pre-University Students, Undergraduate Students: student-matric-number@siswa.unimas.my (eg:1234@siswa.unimas.my)

## 3. PASSWORD

Users are responsible for safeguarding their passwords. Passwords should be obscured and should not be printed, stored online or -revealed to others. The password obtained is intended for individual use and should not be shared. It is recommended that users change their email passwords on a regular basis to maximize the protection to their accounts.

## 4. ACCESS TO UNIVERSITY EMAIL SERVICES AND DISCLOSURE OF EMAIL INFORMATION

All UNIMAS staff and students have access to - email services. All students and staff using - email services are bound by UNIMAS email policy. Other persons who have received permission under the appropriate UNIMAS authority and who have agreed to be bound by the UNIMAS email policy are eligible to use the UNIMAS email services.
UNIMAS encourages the use of email services and respects the privacy of those using them. Subject to the following provisions, UNIMAS does not inspect, monitor or disclose information held on its email services without the user's consent.

- Authorized personnel may need to inspect email when rerouting or disposing of otherwise undeliverable email, spam, or email which contains, or may contain viruses or other material capable of damaging the network. Such right of access is limited to the least invasive level of inspection required and will only be carried out by an authorized personnel of UNIMAS in the course of that person's duties where that is necessary for the purpose of maintaining email service of UNIMAS. Any information obtained through such access will be destroyed immediately -as to protect email service of UNIMAS.

- This exemption does not entitle disclosure of any personal or confidential information by the authorized personnel. However, accidental disclosure of information consequent on reasonable efforts taken in good faith to deliver mail shall not be a breach of this policy.

- UNIMAS may, subject to 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. Where UNIMAS has reasonable grounds for considering that the circumstances apply, it may, in accordance with the process established by this policy, intercept emails for the purpose of ascertaining whether the circumstances do in fact apply:

i. when required by the laws of Malaysia; and/or
ii. where UNIMAS with good reason believes violations of the laws of Malaysian or of University Regulations have occurred; and/or
iii. 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
iv. where critical operational circumstances exist, where failure to act would seriously damage the ability of UNIMAS to function administratively or to meet its teaching, research or community services obligations.

## 5. PROCEDURES TO APPROVE ACCESS TO, DISCLOSURE OF, OR USE OF EMAIL COMMUNICATIONS

University officials who need to gain access to the email communications of others, under the circumstances described in the section "Access to University email services and disclosure of email information", and who do not have the prior consent of the user, must obtain approval in writing in advance of such activity from the Chairman, UNIMAS Integrity Committee (Jawatankuasa Keutuhan Universiti). The access to the electronic communications must also be supervised by a person, designated by the Chairman, UNIMAS Integrity Committee (Jawatankuasa Keutuhan Universiti), who will be kept fully informed of the actions taken by the investigating officer.

## 6. EMAIL ADDRESS PUBLICATION

Universiti Malaysia Sarawak has the right to publish the email addresses.

## 7. ARCHIVING AND RETENTION

Those using email are reminded that it is important to keep email messages as a record, when email is used in place of other written communication. In these circumstances consideration must be given to ensure that the email record is accessible by other staff. However it must be understood that stored email messages may become subject to disclose procedures resulting from legal action. Communications of University employees in the form of email may constitute "correspondence" and, therefore, become a public record and subject to inspection.

UNIMAS does not maintain central or distributed archive for send or receive mail. Users are required to archive their mail locally. Users are required to do regular backup on both archive database and their local address book.

## 8. REDIRECTING OF MAIL

Users may apply for redirecting an email addresses for 1 month if they retire/resign/transfer from UNIMAS.

## 9. ACCEPTABLE USE OF EMAIL

Email services are made available to the staff and students intended to further the teaching, research, and community service mission of UNIMAS. . Individuals must not use email for entrepreneurial activities except in cases of University-sanctioned activities.

***Personal use:***
University staff is permitted make use of the email services for personal communications provided that such use, in the judgment of the supervisor of the user, does not generate a significant cost for UNIMAS.

***Usage of not directly related to the business of UNIMAS:***
Email and email lists used to provide communication of staff social matters are permitted. This is permissible provided the cost is insignificant to UNIMAS as judged by the Head of F/C/I/D.

***Use of email lists:***
Email lists are a powerful mechanism for distributing information. When an email list is established the ‘owner’ of the list must state clearly what the purpose of the list is, and how the list will be moderated. The use of email lists in appropriate circumstances is encouraged. Electronic mail grouping are, in the preliminary, used for communication to a specific user-group within UNIMAS for official used. These lists should only be used for messages that will affect the majority of the designated audience and not only within internal faculty.

## 10. RESTRICTIONS AND UNACCEPTABLE USE AND PRACTICE

***Use of email distribution lists:***

No one shall be added to an email mailing list without her or his consent, unless the list is set up for official University business. Mailing lists may be used only for their intended purposes.

***Commercial purposes:***
University email must not be used for personal financial gain or commercial purposes not under the auspices of UNIMAS.

***Excessive personal use:***
Personal use that creates a significant cost for UNIMAS is prohibited. Participate in mailing list; list server bulk emails services, and other similar services.

***Harassment:***
It is a violation of this policy to employ email to libel, harass or threaten other individuals or organizations.

***Copyright:***
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 prohibited.

***Representation:***
Those using University email services shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of UNIMAS or any unit of UNIMAS unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing UNIMAS. An appropriate disclaimer is: "These statements are my own, not those of Universiti Malaysia Sarawak."

***False Identity (Spoofing):***
Those using University email services shall not employ a false identity. It is a violation of this Policy to originate email in such a manner as to create the impression to the recipient that the email originated from another source or individual.

***Interference:***
University email services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with the use of email or email systems by others. Such uses include, but are not limited to, the use of email services to:

i. send or forward email chain letters;
ii. "spam," that is, to exploit list servers or similar broadcast systems for purposes beyond their intended scope to increase the distribution of unsolicited email; and
iii. "letter-bomb," that is, to resend the same email repeatedly to one or more recipients to interfere with the recipient's use of email.

***Unauthorized access:***
Attempting unauthorized access to email or attempting to breach any security measures on any email system, or attempting to intercept any email transmissions without proper authorization, is a violation of this Policy.

***File attachments:***

File attachments should also not exceed 25 MB for staff.

---

**Procedures/ Guidelines:**

1. **ICTcode001**: Code of Conduct for Staff
2. **ICTcode002**: Code of Conduct for Students
3. **ICTguide001**: Guidelines for the Use of Email
4. **ICTguide002**: Guidelines for Email File Attachments
5. **ICTguide003**: Guidelines of UNIMAS Websites Presentation

---

**Definitions:**

1. **CICTS**: Centre for Information and Communication Technology Services
2. **TECIS**: Technical Committee on Information Services
3. University's Integrity Committee (Jawatankuasa Keutuhan Universiti).
4. **UNIMAS students**: All students including undergraduate, post graduate, and students from other universities attached to UNIMAS
5. **UNIMAS staff**: All contract and permanent staff at UNIMAS, including research assistant and visiting scholars attached to UNIMAS

---

**Related Policies & Documents:**

1. **ICT002**: Acceptable ICT Use (Staff) Policy
2. **ICT004**: Email Server Policy
3. **ICT005**: Virus Protection Policy
4. **ICT006**: Web Presence Policy

---

**Notes:**

## Email Server Policy

---

**References:**

Policy Number:ICT004
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: 1
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff members

---

**Preamble:**

The number of cases of virus infection in the campus has increased steadily due to the emergence of several particularly virulent viruses that spread via email. Management of viruses on campus continues to be an important task. If the number of viruses present on systems on campus is kept at a low enough level then the task of eliminating them is significantly easier. The single most common mechanism for introducing viruses onto campus is email.

Apart from virus, our ICT environment is also exposed to security threats. They come in various forms and sources. It could lead to other possible incidents that may affect UNIMAS image.

It is a concern that in addition to the virus issue, a number of servers on campus are still operating as open email relays, thus allowing unauthorised usage of university email facilities. F/C/I/D with incorrectly configured email servers that allow the relaying of unauthorised email will be incurring considerable additional costs due to increased network traffic.

---

**Policy:**
All existing email servers on campus must relay external email through the central mailhubs and must also use those systems to scan incoming email. All email servers should be centralized and maintain at the Data Centre.

---

**Procedures/ Guidelines:**

1. **ICTguide001**: Guidelines for the use of email
2. **ICTguide002**: Guidelines for email file attachments

---

**Definitions:**

1. **Email servers**: Servers to host email facilities
2. **Virus**: Disruptive applications often executed without the users knowledge
3. **Central mailhubs**: A focal point where all outbound/inbound emails must pass through to ensure email services are secured
4. **Data Centre**: A special place to house all computer hardware, network/communication equipments and other computer peripherals

---

**Related Policies & Documents:**

1. **ICT002**: Acceptable ICT Use (Staff) Policy
2. **ICT003**: Email Policy
3. **ICT006**: Web Presence Policy
4. **ICT012**: ICT Security Policy

---

**Notes:**

UNIMAS Web Policy

**References:**
Policy Number: ICT006
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: 1
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff

**Preamble:**

The presence of Universiti Malaysia Sarawak Web is to publish relevant information about UNIMAS alongside appropriate teaching, learning, research and administrative resources. UNIMAS Website is also a major communication tool for UNIMAS, providing information and services for staff, students, prospective students and the public, as well as supporting teaching and learning, research activities, and administrative processes.

UNIMAS strives to provide a usable, informative and up-to-date website that represents and promotes the teaching, research, values and culture of Universiti Malaysia Sarawak. These websites are also referred to as Universiti Malaysia Sarawak websites.

UNIMAS Web domain is made up of many separate sites located throughout UNIMAS.

For the purposes of this document two separate types of sites are identified:

1. **Homepage** – This is the central site of UNIMAS, incorporating UNIMAS homepage. The Webmaster is responsible for the site. The site provides information on matters common to UNIMAS, and links to F/C/I/D micro-sites and other relevant external links.

2. **Micro-sites** – Refer to the sites managed by F/C/I/D.

This document is intended to facilitate the clarity and coherence of UNIMAS Web presentation by giving guidance to members of UNIMAS who are involved in setting up, amending or updating Websites operated from UNIMAS. It is essential that the principles and guidelines set out in this document are understood and complied with by anyone setting up or operating a Universiti Malaysia Sarawak Website.

**Policy:**
This policy requires:

1. All Websites operated from UNIMAS must follow the guidelines set by UNIMAS.
2. The presentation of all Websites should maintain UNIMAS identity and UNIMAS good name.
3. The guidelines relevant to this policy are *ICTguide003*, *ICTguide005*, *ICTguide006, and ICTguide007*.
4. The content placed on the UNIMAS website must adhere to *The Malaysian Communications and Multimedia Content Code* issued by CMCF.

---

**Procedures/ Guidelines:**
1. **ICTguide003** – Guidelines of UNIMAS Websites Presentation
2. **ICTguide005** – Micro-site Information
3. **ICTguide006** – Information Quality Guidelines
4. **ICTguide007** – Governance of Micro-Sites
5. *The Malaysian Communications and Multimedia Content Code* by CMCF.

---

**Definitions:**
1. **CMCF** – Communication and Multimedia Content Forum
2. **Other Sites** – These are sites which are jointly administered with, or separately administered by outside organisations and are not covered by this policy document. However if these sites are being hosted on a University server, then the technical requirements (for ease of access etc.) need to be complied with.
3. **Websites** – Refers to any UNIMAS websites including micro-sites that are accessible to the general public.
4. **TECIS** – Technical Committee on Information Services
5. **F/C/I/D** – Faculty/Centre/Institute/Division

---

**Related Policies & Documents:**

---

**Notes:**

## Security for Mobile Computing and Storage Devices

---

**References:**

Policy Number: ICT007
Original Approved By: TECIS
Date: 17 April 2009
Revision No: 1
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff members

---

**Preamble:**

Mobile storage and computing devices are becoming increasingly powerful and affordable. With the growing need for data access, the use of mobile devices is becoming more desirable to replace traditional desktop devices in a wide number of applications because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognized and addressed to protect both the physical devices and the information they contain.

Mobile computing, communication, and storage devices are subject to risk areas as follows:

1. Physical Risk. Theft or Loss
2. Unauthorized Access Risk. Login or network access
3. Operating System or Application Risk. Vulnerabilities that can be exploited to gain control of the device
4. Network Risk. Viruses, worms, and other malware can enter a computer or other electronic device through networks, Websites, e-mail attachments, attachments and mobile storage media.
5. Mobile data storage device risk.

This policy applies to anyone who utilizes mobile computing devices to access UNIMAS' information and computing environment. This is to ensure security of **Protected Confidential Information (PCI)** that may be stored on those devices.

---

**Policy:**

This Policy applies to all staff of UNIMAS. ICT facilities are provided for use in the academic and administrative activities of UNIMAS.

***Physical Security***

Users must protect mobile computing devices, removable storage components, and removable computer media from unauthorized access. Physical security measures shall, at minimum, include the following:

- Mobile computing devices, computer media, and removable components, such as disk drives and network cards must be stored in a secure environment. Devices must not be left unattended without employing adequate safeguards such as cable locks, restricted access environments, or lockable cabinets.
- When possible, mobile devices, computer media, and removable components must remain under visual control while travelling. If visual control cannot be maintained, then necessary safeguards shall be employed to protect the physical device, computer media, and removable components.
- Safeguards shall be taken to avoid unauthorized viewing of sensitive or confidential data in public or common areas.

***Operations and Maintenance***

Configuration guidelines address the following:

- **Anti-virus software:** Where applicable, mobile computing devices must be equipped with anti-virus software in accordance with UNIMAS policy
- **System configuration:** Mobile computing device operating system s must be maintained with appropriate security patches and updates.

***Data Protections***

Given their small size and mobile nature, it is more likely that these mobile computing devices will fall into the wrong hands than a desktop system. The following guidelines are used to govern the management and maintenance of data on mobile devices:

- Sensitive data should not be stored on mobile devices. However in the event that there is no alternative to local storage, all sensitive data stored on mobile devices must be secured. Methods for securing information maintained on mobile computing devices include, but not limited to:
  - Data /Application encryption using approved encryption techniques
  - Personal Firewalls – enabled by policy

- When a device is removed from service, the IT equipment must be sanitized to remove all information
- Secured backup storage data is required to ensure data retention or continuity of operations in the event of data loss
- Sensitive data stored on laptops and other mobile devices should be kept to a minimum to reduce risk and impact should breach of security occur.
- Loss of any mobile device containing sensitive data, or any other security breach, should be reported to UNIMAS Security immediately.

---

**Procedures/ Guidelines:**

Securing USB Drive Thru Crypt (downloadable through Anjung UNIMAS)

---

***Definitions:***

1. **Mobile Computing Devices:** These include, but not limited to, Mobile Digital Assistants (PDAs), notebooks, Tablet PCs, Palm Pilots, Microsoft Pocket PCs, Blackberry, MP3 Players, text pagers, smart phones and other similar devices.
2. **Mobile Media/Storage Devices:** This includes but not limited to, compact disks, DVD disks, memory sticks, flash drives, external/removable hard drives, magnetic tapes/cartridges etc. The portability offered by these devices may increase the risk of exposure to groups using the devices.
3. **Protected Confidential Information:** Data which if exposed to any security risk or otherwise disclosed, would violate Malaysian Law or contract or policy. PCI data includes:
    1. Academic Data
    2. Non-Public Directory Information
    3. Other confidential data which is defined by UNIMAS as confidential
4. **User**
   Anyone with authorized access to UNIMAS Information Systems and service
5. **Secured Mobile Device**
   A mobile device that has a sufficient level of access control and protection from malware, strong encryption capabilities to ensure the protection of data that may stored on that mobile device.

---

**Related Policies & Documents:**

1. **ICT012:** ICT Security Policy

---

**Notes:**

## ICT Disposal Policy

---

**References:**

Policy Number: ICT008
Original Approved By:
Date:
Revision No: -
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce 2010
Access Level: All staff and students

---

**Preamble:**

With the extensive use of computer and electronics and rapid advancement of technology, our computers and peripherals become obsolete over time. There are certain procedures and regulations that must be strictly adhered to in order to have the equipments/devices disposed.

---

**Policy:**

This Policy details the guidelines of ICT resources disposal.

The disposal of ICT equipments/devices will be classified according to these categories with the following conditions:

1. Become malfunctioned.
2. Not cost-effective to repair i.e. will cost more than 50% of its original price.
3. Discontinued technical support by the manufacturer due to end of life.
4. Discontinued usage by UNIMAS.
5. Has exceeded 5 years of use.

All records of ICT equipments/devices disposed should be reflected in UNIMAS *Integrated Financial Accounting System* (IFAS).

**Procedures/ Guidelines:**

1. **PKPU** – Tatacara Pengurusan Aset Alih ICT UNIMAS.

**Definitions:**

Definitions for ICT equipment/devices are as follows:

1. Personal Computers / Laptops and accessories
2. Printers
3. Scanners
4. File servers
5. Servers
6. Networking equipments ( Switches, Access Points )
7. UPSs
8. ICT Storage

**Related Policies & Documents:**

1. **UNIMAS Disposal Procedures and Process Flow**

**Notes:**

## ICT Software Licensing Policy

---

**References:**

Policy Number: ICT009
Original Approved By:
Date:
Revision No: -
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce 2010
Access Level: All staff and students

---

**Preamble:**

With the increasing number of software used in UNIMAS, the issues of software licensing and copyrights have become one of the major areas of concern that must be addressed rightfully. Any mishandling of the licensing matters could lead UNIMAS liable to legal implication.

---

**Policy:**

This Policy details the use of commercial software in UNIMAS.

1. Any usage of unlicensed commercial software is strictly prohibited.
2. Auditing will be conducted as and when necessary to ensure that no illegal software is in use.
3. All users are required to ensure that the software to be installed is licensed for UNIMAS.
4. The installed software must comply with UNIMAS security standards.
5. Installations of computer games, peer-to-peer applications, file-sharing or hosting software and contents are prohibited..
6. Approval from TECIS is required prior to procuring any new software. TECIS may advise on any potential issues or considerations pertaining to the software-based on recommendation made by CICTS.
7. UNIMAS has the right to remove or uninstall any illegal commercial software from the computers owned by UNIMAS.

8. For MUSE program only those listed as below are allowed :

    - Microsoft Office Professional
    - Microsoft Windows Desktop Operating System upgrade.
    - Microsoft Visual Studio and .net Professional Academic
    - Core Client Access License (CAL) Suite Windows Server
    - Microsoft Exchange Server 2007 Client Access License (CAL)
    - Microsoft Office SharePoint Server 2007 Standard Client Access License (CAL)
    - System Center Configuration Manager Management ( SCCM ) License

    Note: Applicable only while the contract with MOHE is still valid

---

**Procedures/ Guidelines:**

---

**Definitions:**

1. **TECIS**: Technical Committee for Information Services
2. **F/C/I/D**: Faculty/Centre/Institute/Division
3. **MUSE**: Malaysian University as Enterprise
4. **Software categories**
    a. **Common/Standard Software**
        - Software that are most commonly used and are installed in all computers in UNIMAS.
        - Licenses are managed by CICTS
        - Example: *Microsoft Application and Server, Antivirus Software, AutoDesk*

    b. **Software for Teaching and Learning**
        - Software that are used for teaching and learning purposes and resides in the various faculties.
        - Licenses are managed by CALM
        - Example: *Adobe Software, Macromedia Software, SPSS*.

    c. **Specialized Software**
        - Software that bear specific purposes in UNIMAS.
        - Licenses are to be managed by the respective PTJ
        - Example: *Lightwave 3D, 3D Studio Max, Audit Software*.

---

**Related Policies & Documents:**

NONE

---

**Notes:**

## ICT Network Management Policy

**References:**

Policy Number: ICT010
Original Approved By :
Date :
Revision No :
Approved By :
Date :
Reference Authority : Technical Committee for Information Services
Authors : ICT Policy Taskforce 2010
Access Level : All staff members

**Preamble:**

Network nodes serve as gateways for user computing. The demand for network nodes increases with the growing usage of ICT services. Therefore, management of network nodes is critical to ensure the manageability and sustainability of the network services itself.

**Policy:**

This Policy addresses the addition, modification and termination of any wired ICT network nodes in UNIMAS.

i. No addition, modification or termination of network nodes within UNIMAS premises are allowed without prior approval from CICTS.
ii. All applications must be submitted online through the ICT Service Desk.
iii. TECIS reserves the rights to approve, hold or reject the application based on:
    a. Technical feasibility
    b. Justification
    c. Financial constraint
    d. CICTS recommendations
iv. The network nodes to be added, modified or terminated are only confined to those available within UNIMAS premises, excluding staff residence.
v. The technical specification for the acquisition exercise must be attached with the *Borang Pengesahan Spesifikasi* (**PKTMK-01**) provided by TECIS.

**Procedures/Guidelines**

NONE

**Definitions:**

1. **Users**: All undergraduates, postgraduate students and students from other universities attached to UNIMAS for a period exceeding 6 months, all contract and permanent staff of UNIMAS, including research assistants and visiting scholars attached to UNIMAS for a period exceeding 6 months.
2. **CICTS**: Centre For Information & Communication Technology Services
3. **TECIS**: Technical Committee for Information Services
4. **UNIMAS Premise**: UNIMAS owned/rented premises
5. **ICT**: Information and Communication Technologies

---

**Related Policies & Documents:**
NONE

---

**Notes:**

## Access to Data Centre

### References

Policy Number: ICT011
Original Approved By:
Date:
Revision No: -
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff and students

### Preamble:

This policy governs the security and viability of servers, ICT peripherals and equipments. Access to the Data Center must also be restricted in order to prevent:-

- Unauthorized access
- Manipulation of the configuration of servers' hardware and/or software and any other equipment.
- Theft
- Sabotage
- Espionage
- Misappropriation
- Misuse

### Policy:

#### 1. Access

This Policy applies to all personnel requiring access the Data Center.

In order to secure the systems housed within the data center; the following policies apply:

- Only authorized personnel are allowed.
- Visitors are required to obtain permission from the Head of CICTS.
- Visitors must be accompanied by the CICTS Technical Staff.
- Visitors to the Data Center must adhere to the visitors' guidelines (see Standard Operating Procedure 1.5).
- Visitors must sign in/out when entering/leaving the Data Center to record the time and purpose of their visit.

**2. Equipment**

- All work carried out in the Data Centre such as equipment installations, removals, dismantling or troubleshooting changes must be recorded.
- Data Center employees reserve the rights to deny entry to anyone without written permission from Head of CICTS.
- Only rack-mountable equipments are allowed. Otherwise special permission must be granted through TECIS.

**Procedures/ Guidelines:**

DC - Standard Operating Procedure 1.5

DC – Standard Operating Procedure 1.6

**Definitions:**

1. **Data Center Employee:** Employees of Data Center Unit, Network Unit, ICT Security Unit and ICT Communication Unit who work at the Data Center.
2. **Authorized Staff:** UNIMAS employees who are authorized to gain access to the Data Center but who do not work at the Data Center.
3. **Authorized Vendor:** All non-University employees who, through contractual arrangement and appropriate approvals, have access to the Data Center.
4. **Visitors:** All other personnel who may occasionally visit the Data Center but are not authorized to be in the Data Center without escort.

## ICT Security Policy

---

**References:**
Policy Number: ICT012
Original Approved By:
Date:
Revision No: -
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce 2010
Access Level: All staff members and students

---

### Preamble

This policy covers several aspects of ICT security.

1. **Physical and Environmental Security**
   The enforcement of security on the physical locations, media, equipment, and perimeter control to avoid any unauthorised access that could be harmful to ICT facilities and services.

2. **Virus Protection**
   Computer viruses have been infecting computer systems for many years and today are increasingly virile and destructive. Active viruses appear almost daily with some of these spreading across the Internet in hours. Anti-virus (AV) products are capable of detecting and isolating viruses as they arrive on a computer, usually before they are activated. In addition to viruses, many AV products also detect Trojans and other malwares.

3. **User Access Management**
   UNIMAS staff and students are given access to ICT facilities. They are responsible to ensure that the facilities are utilised accordingly in a lawful and ethical manner. This policy governs the controls and restrictions on user access to any ICT facilities of UNIMAS.

4. **Network Access Control**
   This policy addresses methods and procedures to avoid unauthorised access to UNIMAS network and internet services. This policy also covers all users who access UNIMAS wireless network services.

5. **Information Security**
   This policy provides details on the characteristics of information security such as confidentiality, integrity, availability, authenticity and non-repudiation.

**Policy**

**1. Physical and Environmental Security**

a. This paragraph should be read together with "*Arahan Keselamatan*" issued by the Chief Government Security Office.
b. To prevent unauthorised access, damage and interference, physical protection should commensurate with the identified risk and be based on the principle of defence-in-depth.
c. Critical or sensitive ICT facilities should be housed in a secured area, away from public view, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference.
d. Secured areas should be protected by appropriate entry controls to ensure only authorised personnel are allowed to access.
e. Limit physical access to personnel and/or maintenance crews who are responsible for the operation of the ICT system.
f. Access points such as delivery and loading areas and other points where unauthorized persons may enter the premise, should be controlled and if possible, isolated from ICT processing facilities to avoid unauthorised access.
g. Physical protection should be in placed to protect against damage from fire, flood, pests, explosion, civil unrest and other forms of natural or man-made disaster.
h. Supporting utilities equipment should be protected against power failures and other disruptions.
i. Multiple power feeds must be considered to avoid a single point of failure.
j. Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.
k. All equipment must be maintained to ensure continued availability and integrity.
l. Prior authorisation for all equipment, information or software should be obtained before taken off-site.
m. All equipment containing storage media should be checked to ensure that all sensitive data or licensed software have been transferred and/or securely deleted prior to disposal of the equipment.

**2. Virus Protection**

a. Since UNIMAS is managing campus-wide AV software, all computers used as desktops connected to UNIMAS ICT network infrastructure system must have the AV product installed.
b. All computers used solely as Windows-based servers must have an AV product installed. Only servers where a significant negative impact would result from operating AV software, or servers running an OS with low likelihood of virus infection, may be considered for exemption from this policy.
c. The AV product installed on desktops and servers must be configured to allow update on a daily or more frequent basis.
d. Any computers infected with viruses, spyware, malware, Trojan and/or other related programmes will be barred from accessing the Internet.

e. Any computers causing disruption to networks services provided by UNIMAS shall be removed immediately/barred remotely from the network.

**3. User Access Management**

Every user is responsible for any ICT systems/applications/hardware that he/she has accessed to. The following steps and procedures must be adhered to ensure that security traces are possible to track user activities.

a. A user is only allowed to use account that is assigned by UNIMAS.

b. A user account must be unique and reflects the user's identity (ID). Every user's ID is an owned entity of UNIMAS. As such, UNIMAS reserves the right to grant, revoke or disable the user's account at any time without notification.
   i. Authorised staff will be granted user's ID based on staff email address conventions.
   ii. Authorised student will be granted user's ID based on their matric number.
   iii. Exception to policy item (i) and (ii) is applied to E-Claim Module of IFAS.

c. For a user to have the privilege to create/update/delete data, authorization from the system owner is necessary.

d. The use of another person's account or account sharing is strongly prohibited.

e. The System Administrator has the rights to suspend or terminate a user account due to the following reasons:
   i. A user is on leave for a period of more than two (2) weeks.
   ii. Change in job roles.
   iii. A user is transferred to other PTJ.
   iv. Retirement
   v. Termination of service.

**4. Network Access Control**

a. UNIMAS reserves the right to monitor any and all aspects of its electronic information systems to determine if a user is acting unlawfully or violating this policy or other policies or rules of UNIMAS. Such monitoring may include individual login sessions, the Internet sites visited and the content of electronic communications. Monitoring may be done with or without prior notice to the user.

b. All internet usage in UNIMAS must be continuously monitored to ensure that no violation to the regulations and law of Malaysia.

c. Web content filtering method must be deployed to control the internet access accordingly. All filtering policies/rules must be approved by TECIS before being implemented.

d. To enhance the performance of accessing the internet, all Quality of Service (QoS) standards must be deployed. These standards must be approved by TECIS before being implemented.

e. The internet and network services provided are intended for official use only. No personal, profit-gaining or similar activities are allowed.

f. Approval by Head of F/C/I/D is required prior to any uploading of university-related materials on any system that is not authorised by UNIMAS.

g. Users are not allowed to perform any of these activities:
   i. To upload, download, store, and use any pirated and unlicensed software, games, video, audio or other materials.
   ii. To supply, upload, download, store pornographic materials.
   iii. To supply, upload, download, store any information that are slanderous and could affect the image of UNIMAS and Malaysian Government.

h. Authentication

Authentication is required to access network facilities to prevent unauthorised network usage. The authentication method is using *User ID* and *Password*.

**5. Information**

a. Access to University Application and Disclosure of Application Information

   i. UNIMAS proprietary applications and all information, documents and samples output (screenshot, reports etc) identified as confidential and cannot be **disclosed** in whatever nature and forms whether written, oral, visual, recorded, graphical, electronic, documents, files, prints, reproductions, designs, drawings, material, specifications or programmes and data residing in UNIMAS proprietary databases or any of these said documents, and authentication or other such material or samples.

   This shall also include all documents, computer and other data storage media such as disks and tapes, database structures, table formats, records, files, source codes, designs and drawings and other material whatsoever (and any copies of the same whether in hard copy, handwritten, photographic or electronic form) containing any information, analyses, compilations, notes or other documents.

   ii. Request for confidential information may be authorised by Vice Chancellor (VC) or any other parties appointed by the VC.

b. Confidentiality
    i. All classified information should be encrypted during storage and transmission using recommended industry standard encryption algorithms that comply with the "Digital Signature Act 1997 (Act 562)".
    ii. All private keys should be secured and kept confidential. A report is to be made immediately when private keys are lost or destroyed.
    iii. All cryptographic keys should be stored in a secure and tamper proof Hardware Security Module (HSM).
    iv. Secured transmissions from end–to–end and to protect traffic from eavesdropping, connection hijacking, and other network-level attack by making use of Secure Sockets Layer (SSL), Secure Shell (SSH) and HSM protocols of current versions.

c. Integrity
    i. Comprehensive built-in checks should be incorporated within the security sub-system to ensure integrity and completeness of all data sent to/received from external systems/applications.
    ii. Application systems and security infrastructure implemented should be protected against external and internal network attacks.

d. Availability
    i. Protection mechanisms should be in place to protect against threats that could affect the availability of network systems and information.
    ii. Single point of failure should be avoided.
    iii. Backup measures should be taken and redundancy mechanisms in place when necessary. Backup devices must be made available to quickly replace critical systems when there is a disruption.
    iv. Skilled personnel should be made available to bring the system back online immediately.
    v. Only necessary services and ports should be made available.
    vi. Intrusion Detection Systems (IDS) should be in place to monitor network traffic and host activities.

e. Authenticity
    i. For a subject to be able to access a resource, it has first to prove who it claims to be, has the required credentials, and has been given the authority to perform the requested actions.
    ii. All activities performed on UNIMAS ICT system resources should be recorded for the purpose of detection and accountability.
    iii. CICTS should properly evaluate the technique used for identification and authentication to determine the right mechanism to suit the environment.
    iv. UNIMAS should implement two-factor authentication.

f. Non-repudiation
    i. Non-repudiation means the provision for proof of the integrity and origin of data in such a way that the integrity and origin can be

verified from successfully denying involvement in a previous action. Non-repudiation is achieved cryptographically by the use of a digital signature.

ii. Digital signature should be used to achieve non-repudiation. Digital signature should comply with the requirements of the "Digital Signature Act 1997 (Act 562)".

---

**Procedures/ Guidelines:**

1. **ICTcode001**: Code of conduct for staff
2. **ICTcode002**: Code of conduct for students
3. **ICTguide001**: Guidelines for the use of email
4. **ICTguide002**: Guidelines for email file attachments
5. *Arahan Keselamatan ICT* issued by MAMPU

---

**Definitions:**

1. **CICTS**: Centre for Information and Communication Technology Services
2. **UNIMAS students**: All students including undergraduates, post graduates, pre-university, and students from other universities attached to
3. **UNIMAS staff**: All contract and permanent staff of UNIMAS, including research assistants and visiting scholars attached to UNIMAS
4. **TECIS**: Technical Committee for Information Services
5. **ICT**: Information and Communication Technologies
6. **Two-factor authentication**: Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code.
7. **AV:** Anti-virus
8. **OS:** Operating System
9. **QoS:** Quality of Service is the method that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance.
10. **F/C/I/D :** Faculty/Centre/Institute/Division

---

**Related Policies & Documents:**

NONE

---

**Notes:**

**Related Policies & Documents:**

1. **ICT002**: Acceptable ICT Use (Staff) Policy
2. **ICT003** : Email Policy
3. **ICT004**: Email Server Policy
4. **ICT011**: Data Centre Management Policy

---

**Notes:**

**Network Infrastructure in UNIMAS New Premises Policy**

**References:**

Policy Number: ICT013
Original Approved By:
Date:
Revision No:
Approved By:
Date:
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff

**Preamble:**

ICT now has been recognized as a critical element for university operation. Network infrastructure is the foundation of ICT services, therefore it is important to ensure all new premises incorporate a network infrastructure that compatible, suitable and fully works with existing universities network infrastructure.

**Policy:**

This Policy applies to all UNIMAS New Premises.

i. The owner of new premise is responsible to initiate a discussion with CICTS to deliberate on the intention of getting new network infrastructure before project started. CICTS will advise the owner based on technical and financial feasibility of the project.
ii. Once the project is kicked-off, the owner is responsible to initiate a consult with CICTS for network infrastructure requirement within that premise before civil works start.
iii. The owner is responsible to coordinate communication between parties involved in the project such as BPA and CICTS to ensure works are synchronized and coordinated well.
iv. ICT Consultant or ICT Contractor of the project must consult CICTS for the project requirements and understand existing university network infrastructure standard and then table their proposal accordingly to CICTS before ICT works start.
v. CICTS has the right to approve or reject the proposal based on :
    a. Technical feasibility
    b. Compliance to UNIMAS standard and existing infrastructure

c. Performance merit

vi. ICT Contractor must submit final test result and complete documentation of network infrastructure at the end of project.

---

**Procedures/Guidelines**

NONE

---

**Definitions:**

1. **New Premise** : UNIMAS-owned new building or room that exist after renovation or development
2. **F/C/I/D** : Faculty/Centre/Institute/Division
3. **Owner**: PTJ who initiate the premise development/renovation
4. **CICTS** : Centre for Information and Communication Technology Services
5. **BPA** : *Bahagian Penyelenggaraan dan Aset*
6. **UNIMAS Premise** : UNIMAS owned/rented premises
7. **ICT**: Information and Communication Technologies

---

**Procedures/Guidelines**

NONE

---

**Related Policies & Documents:**

1. **ICT012:** ICT Security Policy

---

**Notes:**

## Network Equipment Policy

---

**References:**

Policy Number: ICT014
Original Approved By:
Date:
Revision No:
Approved By:
Date:
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce 2010
Access Level: All staff members

---

**Preamble:**

Network service is provided to UNIMAS users to enable them to gain access to the network and other ICT services. With increasing usage and needs of network services among users and the low costs of network equipment in the market, some users take their own initiative by installing network equipment which may not be compatible with UNIMAS network infrastructure may eventually disrupt the network.

---

**Policy:**

This policy is to address details of the installation, change or removal of network equipment owned by parties other than CICTS in UNIMAS.

1. Installation, changes or removal of any network equipment within UNIMAS premises is not allowed without prior approval by CICTS.
2. Users or PTJ must submit written application to CICTS via office memo or ICT Service Desk to install, change or remove network equipment.
3. CICTS reserves the right to approve, hold or reject the application based on:
    a. Technical feasibility
    b. Strength and validity of application justification
    c. Compliance to UNIMAS standard and existing infrastructure
    d. Other significant consideration
4. CICTS reserves the right to remove, seize and block access to any installed network equipment that has not been approved by CICTS without prior notice to the equipment owner.
5. CICTS reserves the right to revoke approval of installed network equipment.
6. CICTS must be given administrator/root level account and the right to access to the approved network equipment. Owner is not allowed and will not be given any administration access to the network equipment except with CICTS consent. CICTS has the right to remove any existing configuration in the network equipment.
7. UNIMAS will not be held responsible if damages occurred to the approved network equipment.

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

---

**Procedures/Guidelines**
NONE

---

**Definitions:**

1. **Users** : All students including undergraduate, post graduate, and students from other universities attached to UNIMAS for a period exceeding 6 months , all contract and permanent staff at UNIMAS, including research assistant and visiting scholars attached to UNIMAS for a period exceeding 6 months
2. **F/C/I/D** : Faculty/Centre/Institute/Division
3. **CICTS** : Centre for Information and Communication Technology Services
4. **UNIMAS Premise** : UNIMAS owned premises
5. **Network Equipment** : Access Points, Network Switches, Modem Router, Wireless Bridge, Network Bridge, DHCP Servers, DNS Servers, Network controllers, Network Proxy
6. **ICT**: Information and Communication Technologies

---

**Related Policies & Documents:**
1. **ICT012:** ICT Security Policy

---

**Notes:**

**UNIMAS Portal Policy**

**References:**

Policy Number: ICT015
Original Approval By:
Date:
Revision No:
Approved By:
Date:
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce 2010
Access Level: All staff and students

**Preamble: The** UNIMAS Portal aka 'Anjung UNIMAS', is an official portal for students and staff of the university. It functions as the gateway to the various ICT services in UNIMAS and is intended to simplify access and customises personal information respective to the user's role in the organization.

This policy emphasises that Anjung UNIMAS as the main channel to disseminate information to UNIMAS internal community. It is a strategic resource that is owned by the University as a whole. CICTS supports, executes the implementation and ongoing development efforts, identifies and prioritise new functionalities of the portal. The community contributes to the services by providing contents and information which are relevant to UNIMAS.

Thus it is important that the contributors abide by this policy.

**Policy**

**1. User account policy**

a. Accounts are created only for the staff and students of Universiti Malaysia Sarawak.
b. Account ID will be the same as the email ID.
c. Users are categorised into the following groups:
    - Staff
    - Pre-University students
    - Under graduate students
    - Graduate students
d. Students' accounts are usually generated during registration period. New staff accounts will be created when Portal Team receives acknowledgement of the new recruit. Otherwise, in both cases, users have to submit their application via ICT Service Desk.
e. Any de-provisioning of staff account will be as instructed by the management of CICTS, Registrar's Office or any parties deemed relevant. The de-provisioning is mainly caused by the following cases:
    - Termination
    - Resignation
    - Retirement
    - Death

f. Graduating students will have their account de-provisioned after the Convocation Week. Otherwise, the de-provisioning could also be caused by the following circumstances:
   - Termination
   - Suspension
   - Death
   - As instructed by *Jawatankuasa Keutuhan*

g. Password reset can be performed by the users themselves (via the Password Reset facility), the Portal Admin or any trained staff. Please refer to ICTcode001 (staff) and ICTcode002 (students) for ruling on password creation.

h.

**2. Content Policy**

a. Banner
   i. The image to be displayed must be 490 x 130 pixels.
   ii. Request for the banner shall be done via the *ICT Service Desk*.
   iii. The request shall be endorsed by the Portal Project Leader.
   iv. Request must be submitted at least 3 working days prior to the targeted date of display.
   v. Banner will be taken off from display 3 days after the respective event or otherwise stated by the applicant.

b. News and Announcement
   i. Announcements on events and news will be propagated via *News & Event*, *ICT Info* and *Local Info* portlets.
   ii. *News & Event* and *Local Info* postings are moderated by the Publication Unit.
   iii. Postings should be submitted at least 3 days prior to the display date and will be reviewed
   iv. *News & Event* postings can only be done by UNIMAS staff and members of the Student Council (MPP). *Local Info* entries are posted by the Corporate Communication Unit and *ICT info* entries are posted by CICTS.
   v. Users must furnish all mandatory fields in the page before posting.
   vi. The page is best viewed using Internet Explorer version 6 and above.
   vii. News and announcement must not have provocative, libelous and racial sentiments content. Refer to ICTcode001 for staff and ICTcode002 (students).
   viii. Postings must be in Bahasa Melayu and English.
   ix. Postings will be displayed for the duration of the event and a week after or otherwise stated by the author.

c. General content policy
   i. Users are responsible for the use of Anjung UNIMAS, for any content posted to Anjung UNIMAS, and for any consequences thereof.
   ii. UNIMAS will not be responsible or liable for any harm to your computer system, loss of data, or other harm that results from your access to or use of the Services, or any Content.
   iii. The responsible Unit for displaying the information posted to Anjung UNIMAS will be reviewed and referred to the Corporate Communication Unit.

d. Collaborating ICT Services

i. Types of access provided :
- Hyperlink
- Single Sign-On (SSO) link
- Portlet

ii. Request for hyperlinks to applications must be submitted at least 3 (THREE) working days prior to display date.

iii. Request for SSO links must be submitted at least 2 (TWO) weeks prior to display date and will be subjected to the compatibility of the target application.

iv. Development for portlets will take up at least 2 months, depending on the complexity of the requirement.

v. Portal Team shall not be accessing raw data.

vi. Portal Team shall only maintain the interface created in Anjung UNIMAS for the adjoining application.

---

**Procedures/ Guidelines:**

1. **ICTcode001**: Code of Conduct for Staff
2. **ICTcode002**: Code of Conduct for Students

---

**Definitions:**

1. **CICTS**: Centre for Information and Communication Technology Services
2. **TECIS**: Technical Committee for Information Services
3. **Students**: All students including undergraduate, graduates, and students from other universities visiting scholarson attachment to UNIMAS
4. **Staff**: All contract and permanent staff of UNIMAS, including research assistant and visiting scholars attached to UNIMAS
5. **Portlet** : pluggable user interface software components that are managed and displayed in a web portal

---

**Related Policies & Documents:**

1. **ICT002**: Acceptable ICT Use (Staff) Policy
2. **ICT003**: Email Policy
3. **ICT012**: ICT Security Policy

---

**Notes**

## Acceptable Use of CAIS Electronic Resources

---

**References:**

Policy Number: ICTcais001
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: 1
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff and students

---

**Preamble:**

The Centre for Academic Information Services (CAIS) provides access to electronic data services and does not guarantee the authority or accuracy of any information found on it. Users will not hold CAIS responsible for:

- any loss of data resulting from delays, non-deliveries or service interruptions
- technical difficulties
- transmission of viruses
- offensive materials retrieved through use of electronic services.

Access to online and Internet resources through the electronic data services is provided to support the research, educational and administrative purposes of UNIMAS.

Use of the electronic data services at CAIS is restricted to students and staff of Universiti Malaysia Sarawak, and to any other persons who may be authorised from time to time by UNIMAS.

CAIS will not be held responsible for the actions of its users and also any 3rd party content accessed by the users.

---

**Policy:**

**Electronic Collections**
Access to these collections is available according to the relevant licence agreements. CAIS will acquire access for walk-in users, and the ability to use full text collections for document delivery purposes. CAIS reserves the right to restrict access of certain electronic resources only to Universiti Malaysia Sarawak's staff and students, in accord with the copyright regulations.

**Technical Infrastructure**

In order to ensure adequate access to electronic collections, CAIS will ensure regular updating or replacement of computer workstations, servers, printing and copying facilities etc. The adequacy of computer workstations available to in-house users is continuously monitored. In addition:

- The use of CAIS electronic resources takes priority on all CAIS ICT equipments and facilities. Among others, CAIS ICT equipments and facilities are for:
  - information searching on the Internet
  - completion of student's work such as assignments
  - accessing online course materials provided through the universities online learning system
- Time limits apply on CAIS computers. During peak periods these will be enforced.
- Most of the electronic resources provided by CAIS are subject to license agreements and copyright restrictions. Individual users are personally responsible for ensuring that their use of these resources complies with all relevant legislation and agreements.
- Users must not create, access, store, display or transmit racist, pornographic or other offensive or any other material deemed as inappropriate by UNIMAS or the general public.
- Deliberately or negligently interfering with the operation or performance of computers in any manner such as the equipments is prohibited.
- The deletion, addition or modification of files relevant to the system's operation, including the introduction of viruses or other software components, is also prohibited.
- CAIS reserves the right to refuse access to computers and other electronic resources located within CAIS.
- CAIS electronic resources should not be used for any fraudulent or unlawful purposes, including any activities prohibited under any applicable Malaysian law and appropriate international laws.
- CAIS computers shall not be used for any commercial purposes.

Users of CAIS electronic services must comply with the following University-wide policies and conditions of use:

a. ICT002 – *Acceptable ICT Use (Staff) Policy*
b. ICT003 – *Email Policy*
c. ICT012 – *Security Policy*
d. ICTcode001 – *Code of Conduct for Staff*
e. ICTcode002 – *Code of Conduct for Student*
f. ICTguide001 – *Guidelines for the Use of Email*
g. ICTguide002 – *Guidelines for Email File Attachments*

Legal and disciplinary action can be taken according to Malaysian Law, Government Act, and University regulation for any violation of the rules and regulations pertinent to CAIS electronic services.

Disciplinary action shall also be taken on users who abuse the electronic resources provided by CAIS. Systematic or excessive downloading of electronic content from the subscribed online databases or electronic journals using 'robots' or any such software, or any manual means, (which results in a vendor license violation on the part of UNIMAS and/or its Library) is expressly forbidden.

Furthermore, UNIMAS is not to be held responsible if the resource providers undertake legal action against the offender.

---

**Procedures/ Guidelines:**

1. **ICTguide001**: Code of Conduct for Staff
2. **ICTguide002**: Code of Conduct for Student
3. **ICTcode001**: Guidelines for the Use of Email
4. **ICTcode002**: Guidelines for Email File Attachments

---

**Definitions:**

1. **UNIMAS students**: All students including undergraduates, post graduates, and students from other universities attached to UNIMAS.
2. **UNIMAS staff**: All contract and permanent staff at UNIMAS, including research assistants and visiting scholars attached to UNIMAS.
3. Electronic services cover ICT hardware (such as computers and peripherals), software (such as electronic databases and journals) and communication facilities (such as routers).

---

**Related Policies & Documents:**

1. **ICT002**: Acceptable ICT Use (Staff) Policy
2. **ICT003**: Email Policy
3. **ICT012**: ICT Security Policy

---

**Notes:**

**Computer and Network Facilities**
**Code of Conduct for Staff**

---

**References:**

Code of Conduct Number: ICTcode001
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: -
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff and students

---

**COMPUTER AND NETWORKING FACILITIES**
**CODE OF CONDUCT**
For UNIMAS Staff

**I understand that:**

1. I 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 to support my work and services in UNIMAS.

3. I shall not abused the facilities and these include amongst others but not limited to:

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

   3.2 Illegally copying licensed software

   3.3 Storing or installing files on any UNIMAS computer system that are not directly related to my work;

   3.4 Accessing any computer or information without proper authorization;

   3.5 Disclosing my password to anyone

   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

3.9 Compromising the privacy of others;

3.10 Violating and disrupting other users' rights (example: harassing, libelous or disruptive to others, game playing, chatting unnecessarily that is not related to work, 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. I shall:

4.1 Choose a secure password comprising mixed-case alphabetic, numbers and punctuation, and not using any password bearing my name or my family or any word from any dictionary. Refer to security policy

4.2 Take all reasonable precautions against introducing viruses, worms, or Trojan horses in any system.

4.3 Report any problem relating to computer networking facilities to the System Administrator as soon as possible.

5. Processes/programs on UNIMAS system may be terminated or modified without notification.

6. If, in the best judgment of the System Administrator, with the consent of the Vice Chancellor, that certain privileges or actions threaten 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 I directly or indirectly generate and show these systems logs to associated personnel as required.

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

9. Whenever my service has been terminated, my account shall be disabled and my files shall be removed without notification.

10. I shall be subjected to the UNIMAS Integrity Committee's (Jawatankuasa Keutuhan) investigation for any abuse of computer and network facilities. The Committee reserves the right to take or recommend appropriate actions, depending on the severity of the case.

11. I have read and understood the UNIMAS ICT policies and services guideline and agree to adhere to them.

**COMPUTER AND NETWORKING FACILITIES**
**CODE OF CONDUCT**
For UNIMAS Staff

(Please sign this duplicate copy and return it to the Registrar's Office, UNIMAS)

**I understand that:**

1. I 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 me to support my work and services at UNIMAS.

3. I shall not misuse my privileges and these include amongst others, not:

   3.1 Using facilities for purposes other than those for which they were intended or authorized;

   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 my work;

   3.4 Accessing any computer or information without proper authorization;

   3.5 Disclosing my password to anyone or anybody's password other than mine;

   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 UNIMAS facilities (example: harassing, libelous or disruptive to others, game playing, chatting unnecessarily that is not related to work, 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. I shall:

   4.1 Choose a secure password comprising mixed-case alphabetic, numbers and punctuation, and not using any password bearing my name or my family or any word from any dictionary.

   4.2 Take all reasonable precautions against introducing viruses, worms, or Trojan horses in any system.

   4.3 Report any problem relating to computer networking facilities to the System Administrator as soon as possible.

   4.4 Use UNIMAS IT resources with caution to avoid plagiarism

5. Processes/programs on UNIMAS machines may be signalled or terminated without notification or that UNIMAS equipment may be shutdown or modified without notification.

6. If, in the best judgement of the System Administrator, with the consent of the Vice Chancellor, that certain privileges or actions threaten 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 I directly or indirectly generate and show these systems logs to associated personnel as required.

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

8. I will not do anything to misrepresent or embarrass UNIMAS.

9. When UNIMAS is advised that my service in UNIMAS has terminated, my account will be disabled and my files will be removed without notification.

10. If I abuse and misuse the Computer and Networking facilities, I will be reported to the UNIMAS Integrity Committee (*Jawatankuasa Keutuhan*) for investigation and scrutiny. The Committee reserves the right to take or recommend appropriate actions, depending on the severity of the case. These actions may include suspension of my account for an indefinite period, paying a fine if I illegally copied licensed software that is subjected to the Software Copyright Act, and/or referring my case to UNIMAS Disciplinary Committee for disciplinary investigation and/or action(s).

11. I have read and understood the UNIMAS ICT policies and service guideline and agree to adhere to them.

Name : _____

Student ID : _____ I/C or Passport No.: _____

Signature : _____Date : _____

**Computer and Network Facilities**
**Code of Conduct for Students**

---

**References:**

Code of Conduct Number: ICTcode002
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: -
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff and students

---

UNIVERSITI MALAYSIA SARAWAK

KEMUDAHAN KOMPUTER DAN RANGKAIAN
KOD PERLAKUAN
*untuk pelajar*

Saya mengerti bahawa :

1. Saya akan menggunakan kemudahan komputer dan sumber maklumat UNIMAS, termasuk perkakasan, perisian, rangkaian, dan akaun komputer, secara bertanggungjawab.

2. Penggunaan kemudahan ini merupakan satu keutamaan yang diberikan kepada saya bagi menyokong pengajian saya di UNIMAS.

3. Saya tidak akan menyalahgunakan keutamaan saya ini, dan termasuklah antara lain, tidak:

    3.1 Menggunakan kemudahan untuk tujuan selain daripada yang dimaksudkan atau dibenarkan
    3.2 Menyalin perisian berlesen tanpa kebenaran atau melanggar perjanjian atau hakcipta lesen perisian.
    3.3 Menyimpan atau memasukkan fail pada sebarang peralatan UNIMAS yang tidak berkaitan langsung dengan tugasan saya atau keperluan kursus yang berkaitan
    3.4 Mencapai/mengakses sebarang komputer atau maklumat tanpa izin
    3.5 Mendedahkan katalulus saya atau sebarang katalulus kepada sesiapa jua
    3.6 Memintas had-had normal sumber, prosedur atau peraturan keselamatan

3.7 Mengambil kesempatan di atas kelurusan atau kelalaian pengguna lain untuk memperolehi akses kepada akaun dan maklumat pengguna berkenaan atau mencapai akaun pengguna lain atau cuba menyamar sebagai pengguna lain.

3.8 Menghantar sebarang pancaran elektronik palsu atau mencapai maklumat yang salah di sisi undang-undang.

3.9 Mengancam kerahsiaan orang lain.

3.10 Melanggar hak pengguna yang lain semasa menggunakan kemudahan UNIMAS (contohnya, mengganggu atau menghina mereka, memainkannya, menghantar terlalu banyak mesej atau fail multimedia yang besar, mencetak secara berlebihan, mengubah kemudahan sistem, mencuba untuk merempuh masuk atau memberhentikan kemudahan, menukar lokasi kemudahan, merosak atau membinasakan kemudahan)

4. Saya akan:

4.1 Memilih satu katatulus selamat yang mengandungi huruf-huruf besar dan kecil, angka dan tanda bacaan, tidak menggunakan katalulus yang mengandungi nama saya atau sebarang perkataan dari sebarang kamus

4.2 Mengambil langkah berjaga-jaga yang sewajarnya untuk mengelakkan kewujudan virus di dalam sebarang sistem

4.3 Melaporkan dengan segera masalah yang berkaitan dengan sistem kepada pentadbir sistem dengan kadar segera

5. Perkara-perkara berikut dianggap tindakan menciplak yang bertentangan dengan kejujuran akademik:

5.1 Menyalin sesuatu fail komputer yang mengandungi tugasan pelajar lain, sama ada secara sebahagian atau keseluruhan, dan menghantarnya sebagai tugasan sendiri

5.2 Membenarkan pelajar lain, atas kesedaran saya untuk menyalin atau mengguna fail komputer saya, dan menghantar fail berkenaan, atau melakukan pengubahsuaian luaran ke atasnya, seolah-olah hasil kerja pelajar berkenaan.

6. Proses-proses/program-program pada mesin-mesin universiti boleh diarahkan atau diberhentikan tanpa notis atau peralatan university boleh ditutup atau diubahsuai tanpa notis.

7. Sekiranya, di bawah pertimbangan pentadbir sistem, sesetengah keutamaan atas tindakan itu mengancam pengguna-pengguna lain atau jika sesuatu sistem atau rangkaian

berkemungkinan menjadi rosak, pentadbir berkenaan boleh memeriksa, merekod, meninjau, menyalin dan justeru itu mencatat kesemua trafik elektronik yang saya janakan secara langsung atau tidak langsung dan menunjukkan catatan sistem tersebut kepada pihak lain sebagaimana yang diperlukan.

8. Capaian kepada kemudahan yang diberikan ini boleh digantung atau dibatalkan bila-bila masa tanpa notis

9. Saya tidak akan melakukan apa-apa yang boleh mencemarkan atau memalukan UNIMAS

10. Apabila Universiti dinasihatkan bahawa pendaftaran saya di UNIMAS telah diberhentikan, akaun saya akan ditutup dan fail-fail saya akan dikeluarkan tanpa notis

11. Saya telah membaca dan memahami polisi-polisi, dan panduan perkhidmatan ICT UNIMAS serta bersetuju untuk mematuhinya.

UNIVERSITI MALAYSIA SARAWAK
KEMUDAHAN KOMPUTER DAN RANGKAIAN
KOD PERLAKUAN

Untuk Pelajar

( *Sila tandatangani dan pulangkan salinan ini ke Pejabat Pendaftar, UNIMAS )*

Saya mengerti bahawa :

1. Saya akan menggunakan kemudahan komputer dan sumber maklumat UNIMAS, termasuk perkakasan, perisian, rangkaian, dan akaun komputer, secara bertanggungjawab.

2. Penggunaan kemudahan ini merupakan satu keutamaan yang diberikan kepada saya bagi menyokong pengajian saya di UNIMAS.

3. Saya tidak akan menyalahgunakan keutamaan saya ini, dan termasuklah antara lain, tidak:
   3.1. Menggunakan kemudahan untuk tujuan selain daripada yang dimaksudkan atau dibenarkan.
   3.2. Menyalin perisian berlesen tanpa kebenaran atau melanggar perjanjian atau hakcipta lesen perisian.
   3.3. Menyimpan atau memasukkan fail pada sebarang peralatan UNIMAS yang tidak berkaitan langsung dengan tugasan saya atau keperluan kursus yang berkaitan.
   3.4. Mencapai/mengakses sebarang komputer atau maklumat tanpa izin.
   3.5. Mendedahkan katalulus saya atau sebarang katalulus kepada sesiapa jua.
   3.6. Memintas had-had normal sumber, prosedur atau peraturan keselamatan.
   3.7. Mengambil kesempatan di atas kelurusan atau kelalaian pengguna lain untuk memperolehi akses kepada akaun dan maklumat pengguna berkenaan atau mencapai akaun pengguna lain atau cuba menyamar sebagai pengguna lain.
   3.8. Menghantar sebarang pancaran elektronik palsu atau mencapai maklumat yang salah di sisi undang-undang.
   3.9. Mengancam kerahsiaan orang lain.
   3.10. Melanggar hak pengguna yang lain semasa menggunakan kemudahan UNIMAS (contohnya, mengganggu atau menghina mereka, memainkannya, menghantar terlalu banyak mesej atau fail multimedia yang besar, mencetak secara berlebihan, mengubah kemudahan sistem, mencuba untuk merempuh masuk atau memberhentikan kemudahan, menukar lokasi kemudahan, merosak atau membinasakan kemudahan).

4. Saya akan:

4.1 Memilih satu katatulus selamat yang mengandungi huruf-huruf besar dan kecil, angka dan tanda bacaan, tidak menggunakan katalulus yang mengandungi nama saya atau sebarang perkataan dari sebarang kamus.

4.2 Mengambil langkah berjaga-jaga yang sewajarnya untuk mengelakkan kewujudan virus di dalam sebarang system.

4.3 Melaporkan dengan segera masalah yang berkaitan dengan sistem kepada pentadbir sistem dengan kadar segera.

5. Perkara-perkara berikut dianggap tindakan menciplak yang bertentangan dengan kejujuran akademik:

5.1 Menyalin sesuatu fail komputer yang mengandungi tugasan pelajar lain, sama ada secara sebahagian atau keseluruhan, dan menghantarnya sebagai tugasan sendiri.

5.2 Membenarkan pelajar lain, atas kesedaran saya untuk menyalin atau mengguna fail komputer saya, dan menghantar fail berkenaan, atau melakukan pengubahsuaian luaran ke atasnya, seolah-olah hasil kerja pelajar berkenaan.

6. Proses-proses/program-program pada mesin-mesin universiti boleh diarahkan atau diberhentikan tanpa notis atau peralatan university boleh ditutup atau diubahsuai tanpa notis.

7. Sekiranya, di bawah pertimbangan pentadbir sistem, sesetengah keutamaan atas tindakan itu mengancam pengguna-pengguna lain atau jika sesuatu sistem atau rangkaian berkemungkinan menjadi rosak, pentadbir berkenaan boleh memeriksa, merekod, meninjau, menyalin dan justeru itu mencatat kesemua trafik elektronik yang saya janakan secara langsung atau tidak langsung dan menunjukkan catatan sistem tersebut kepada pihak lain sebagaimana yang diperlukan.

8. Capaian kepada kemudahan yang diberikan ini boleh digantung atau dibatalkan bila-bila masa tanpa notis.

9. Saya tidak akan melakukan apa-apa yang boleh mencemarkan atau memalukan UNIMAS.

10. Apabila Universiti dinasihatkan bahawa pendaftaran saya di UNIMAS telah diberhentikan, akaun saya akan ditutup dan fail-fail saya akan dikeluarkan tanpa notis.

11. Saya telah membaca dan memahami polisi-polisi, dan panduan perkhidmatan ICT UNIMAS serta bersetuju untuk mematuhinya.

Saya telah membaca, memahami dan bersetuju untuk mematuhi Kod Perlakuan dalam dokumen ini.

Dalam keadaan saya gagal untuk mematuhi Kod perlakuan ini, tindakan tatatertib boleh dikenakan terhadap saya.

Nama : _____ No. Daftar Pelajar : _____

Fakulti : _____ No. KP : _____

Tandatangan : _____ Tarikh : _____

**Computer and Network Facilities**
**Code of Conduct for Student**

---

**References:**

Code of Conduct Number: ICTcode002
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: -
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All students

---

**COMPUTER AND NETWORKING FACILITIES**
**CODE OF CONDUCT**
For UNIMAS Student

**I understand that:**

1. I 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 me to support my studies in UNIMAS.

3. I shall not misuse my privileges and these include amongst others, not:

3.1 Using facilities for purposes 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 my studies

3.4 Accessing any computer or information without proper authorisation;

3.5 Disclosing my password to anyone or anybody's password other than mine;

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 UNIMAS facilities (example: harassing, libellous or disruptive to others, game playing, chatting unnecessarily that is not related to work, 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. I shall:

4.1 Choose a secure password comprising mixed-case alphabetic, numbers and punctuation, and not using any password bearing my name or my family or any word from any dictionary.

4.2 Take all reasonable precautions against introducing viruses, worms, or Trojan horses in any system.

4.3 Report any problem relating to computer networking facilities to the System Administrator as soon as possible.

4.4 Use UNIMAS ICT resources with caution to avoid plagiarism.

5. Processes/programs on UNIMAS machines may be signaled or terminated without notification or that UNIMAS equipment may be shutdown or modified without notification.

6. If, in the best judgment of the System Administrator, with the consent of the Vice Chancellor, that certain privileges or actions threaten 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 I directly or indirectly generate and show these systems logs to associated personnel as required.

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

8. I will not do anything to misrepresent or embarrass UNIMAS.

9. When UNIMAS is advised that my studies in UNIMAS has terminated, my account will be disabled and my files will be removed without notification.

10. If I abuse and misuse the Computer and Networking facilities, I will be reported to the UNIMAS Disciplinary Committee for investigation and scrutiny. The Committee reserves the right to take or recommend appropriate actions, depending on the severity of the case.

11. I have read and understood the UNIMAS ICT policies and services guideline and agree to adhere to them.

**COMPUTER AND NETWORKING FACILITIES**
**CODE OF CONDUCT**
For UNIMAS Student

(Please sign this duplicate copy and return it to the Registrar's Office, UNIMAS)

**I understand that:**

1. I 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 me to support my studies in UNIMAS.

3. I shall not misuse my privileges and these include amongst others, not:

   3.1 Using facilities for purposes 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 my studies

   3.4 Accessing any computer or information without proper authorisation;

   3.5 Disclosing my password to anyone or anybody's password other than mine;

   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 UNIMAS facilities (example: harassing, libelous or disruptive to others, game playing, chatting unnecessarily that is not related to work, 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. I shall:

   4.1 Choose a secure password comprising mixed-case alphabetic, numbers and punctuation, and not using any password bearing my name or my family or any word from any dictionary.

   4.2 Take all reasonable precautions against introducing viruses, worms, or Trojan horses in any system.

   4.3 Report any problem relating to computer networking facilities to the System Administrator as soon as possible.

   4.4 Use UNIMAS ICT resources with caution to avoid plagiarism.

5. Processes/programs on UNIMAS machines may be signaled or terminated without notification or that UNIMAS equipment may be shutdown or modified without notification.

6. If, in the best judgment of the System Administrator, with the consent of the Vice Chancellor, that certain privileges or actions threaten 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 I directly or indirectly generate and show these systems logs to associated personnel as required.

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

8. I will not do anything to misrepresent or embarrass UNIMAS.

9. When UNIMAS is advised that my studies in UNIMAS has terminated, my account will be disabled and my files will be removed without notification.

10. If I abuse and misuse the Computer and Networking facilities, I will be reported to the UNIMAS Disciplinary Committee for investigation and scrutiny. The Committee reserves the right to take or recommend appropriate actions, depending on the severity of the case.

11. I have read and understood the UNIMAS ICT policies and services guideline and agree to adhere to them.

Name : _____

Student ID. : _____ I/C or Passport No.: _____

Signature : _____Date : _____

## Guidelines for the Use of Email

---

**References:**

Guidelines Number: ICTguide001
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: -
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff and students

---

**Preamble:**

Electronic communication using email does have some characteristics, which set it apart from the other forms of communication we use. It has characteristics of both telephone communication and the written letter. Like the telephone it is used for informal communication but it also leaves a record, just as a paper communication does. The speed of email communication is between the immediacy of the telephone, and the day or two of paper mail.

Perhaps, because of the almost immediate nature of email, we tend to accept errors (spelling, typos, etc.) in email that we would not in a letter. Another common characteristic of email is a level of incivility that we would not find acceptable in written or verbal communication. In general, rules of common courtesy for interaction among people should be followed in communicating via email, where body-language and the tone of voice must be inferred.

This document gives some simple guidelines aimed to help make email communication easier and more effective.

---

**Guidelines:**

### 1. OFFICIAL EMAIL APPLICATION

Staff and student of UNIMAS are encouraged to use the email application supported by UNIMAS to enable CICTS to provide support when required.

**2. LANGUAGE FOR FORMAL EMAIL CORRESPONDENCE**

Official language (Bahasa Melayu and English) should be used for email correspondence which is formal in nature. Avoid using local dialects and short messaging system (sms) forms of communication. Use memo style if applicable for formal email correspondence.

**3. BE CAREFUL WITH ADDRESSES**

Be careful when addressing mail. There are addresses which may go to a group but the address looks like it is just one person. Know to whom you are sending. In particular verify all addresses before initiating long or personal discourse.

**4. HAVE A MEANINGFUL SUBJECT LINE**

Focus on one subject per message and always include a pertinent subject line for the message.

**5. NAME THE RECIPIENTS**

While some mailers will display a recipients' name (as opposed to just their email address) this does not always happen. In consequence it is helpful, particularly if you are sending to a group of people, to name them at the start of the email.

**6. USE A SIGNATURE**

Most mailers support the creation of a 'signature' which can be attached to the end of your messages. Your signature footer should include your name, position, affiliation and contact information. Your 'signature' takes the place of your business card. Some mailers allow you to have more than one 'signature' so you can apply the 'signature' appropriate to the recipient. It is appropriate to include UNIMAS Home Page address in the signature on messages going outside UNIMAS. Always include your signature at the bottom of email messages when communicating with people who may not know you personally.

**7. USE OF CAPITALISATION AND EMPHASIS**

Capitalize words only to highlight an important point or to distinguish a title or heading. Capitalizing whole sections of text is generally termed as SHOUTING! Remember that capitalized text is more difficult to read than mixed mode text. *Asterisks* surrounding a word can be used to make a stronger point. That *is* what I meant.

**8. ENRICHING MESSAGES**

Be careful when using sarcasm and humor. Without face-to-face communications your joke may be viewed as criticism. When being humorous, use 'emoticons' to express humor. For example you can use a :-) [look sideways] happy face for humor.

**9. LANGUAGE, AND INTERNATIONAL AND CULTURAL CONSIDERATIONS**

Remember that the recipient is a human being whose culture, language, and humor have different points of reference from your own. Remember that date formats, measurements, and idioms may not travel well. To avoid misinterpretation of dates spell out the month name: eg. 24 September 1999. "Reasonable" expectations for conduct via email depend on your relationship to a person and the context of the communication. Norms learned in a particular email environment may not apply in general to your email communication with people across the Internet. Be careful with slang or local acronyms.

## 10. FORMATTED MAIL MESSAGES AND THE USE OF FONT CHARACTERISTICS

Proprietary mail systems may allow the use of facilities such as bolding or including colored text. If you use these facilities consider whom you are sending the message to. The mail software they are using may not appropriately interpret such formatting, and may actually make your mail message very difficult to read (particularly if their mail program displays the control characters used for the formatting. If you send tabular information in the text of an email message using a monospaced font informed the recipient to view it with a monospaced font.

## 11. THE USE OF ACRONYMS

Acronyms can be used to abbreviate when appropriate, although messages that are filled with acronyms can be confusing and annoying to the reader. The following are in common use in emails

IMHO= in my humble/honest opinion, FYI = for your information, BTW = by the way, Flame = antagonistic criticism

## 12. FLAMING

A good rule of thumb: Be conservative in what you send and liberal in what you receive. Wait overnight to send emotional responses to messages. If you have really strong feelings about a subject, indicate it via FLAME ON/OFF enclosures. For example: FLAME ON: This type of argument is not worth the bandwidth it takes to send it. It's illogical and poorly reasoned. The rest of the world agrees with me. FLAME OFF. On the other hand, you shouldn't be surprised if you get flamed and it's prudent not to respond to flames.

## 13. ACKNOWLEDGEMENT

We usually expect email to be delivered very quickly, even across the world. However, there is a possibility of delays at all stages of the transmission via the different Internet hosts on the way. If you think the importance of a message justifies it, or the sender has explicitly requested a response, immediately reply briefly to an email message to let the sender know you got it, even if you will send a longer reply later. A long delay before reply can leave the sender thinking that you have not yet received the message.

## 14. REPLYING TO OR FORWARDING MESSAGES

When quoting another person, edit out whatever isn't directly applicable to your reply.
Don't let your mailing software automatically quote the entire body of messages you are replying to when it's not necessary. It is bad practice to simply reply to a message by including the entire previous message. Take the time to edit any quotations down to the minimum necessary to provide context for your reply. Nobody likes reading a long message in quotes for the third or fourth time, only to be followed by a one-line response: "Yes I agree." Check the reply address when you reply to messages. Frequently replies are sent back to the address which originated the post - which in many cases is the address of a list or group! You may accidentally send a personal response to a great many people.

In general, it's a good idea to at least check all your new mail subjects before responding to a message. Sometimes a person who asks you for help (or clarification) will send another message which effectively says "Never Mind". Also make sure that any message you respond to was directed to you. You might be cc:ed rather than the primary recipient.

Watch cc's when replying. Don't continue to include people if the messages have become a 2-way conversation.

If you are forwarding a message you've received, do not change the wording. If the message was a personal message to you and you are re-posting to a group, you should ask permission first. You may shorten the message and quote only relevant parts, but be sure you give proper attribution.

The auto-reply feature found in some mailers may be useful in some situations, but quite annoying when sent to entire mailing lists. Use auto-reply with care.

**15. USING MAILING LISTS**

Be careful to send subscribe and unsubscribe messages to the appropriate address. It is your responsibility to learn how the lists work, and to send the correct mail to the correct place. Save the subscription messages for any lists you join. These usually tell you how to unsubscribe as well.

In general, it's not possible to retrieve messages once you have sent them. Even your system administrator will not be able to get a message back once you have sent it. This means you must make sure you really want the message to go as you have written it. If you are using a mailer with the option to send mail immediately set on, consider turning the option off. This will then give you a second chance to retrieve and modify mail for a limited time.

Some mailing lists are left open to allow anyone to mail to them, even if you are not a member of the list. Don't assume this openness is an invitation to send to the mail list. If the right to mail to the list is not obvious contact the list owner to seek permission to mail before proceeding.

When sending a message to more than one mailing list, especially if the lists are closely related, apologize for cross-posting - this ensures the recipients of multiple copies understand what has happened. If you ask a question on a list, it is usual to post a summary. When doing so, truly summarize rather than send an accumulation of the messages you receive.

If you find yourself in a disagreement with one person, make your responses to each other rather than continue to send messages to the list. If you are debating a point on which the group might have some interest, you may summarize for them later.

**16. PRIVACY AND SECURITY**

Whether the sender or receiver of an email message has a right to privacy is irrelevant-email can be intercepted and does record in places other than the receiver's and sender's computers. Email on Internet is not secure unless encryption is used. Never include in an email message anything that you want to keep private and confidential. Never send something that you would mind seeing on the evening news.

**17. PASSWORDS**

DO use a password with mixed-case letters. Do not just capitalize the first letter, but add uppercase letters in the middle.

DO use a password that can be typed quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by looking at your keyboard.

DO use a minimum of 8 characters for your password. This makes it harder for someone to guess your password.
DO change your password regularly.
DO NOT use your userid in any form (as-is, reversed, capitalized, doubled, etc) as the password.
DO NOT use your first, middle or last name in any form. Do not use your initials or any nicknames you may have.
DO NOT use your partner's or child's name.
DO NOT use a word contained in English or foreign dictionaries, spelling lists, or other word lists.
DO NOT use other information easily obtained about you. This includes license plate numbers, telephone numbers, identification numbers, the brand of your automobile, the name of the street you live on, etc.
DO NOT write your password down, or store it on-line.
DO NOT reveal your password to anyone – including the ICT ServiceDesk personnel.

**18. COPYRIGHT**
Respect the copyright on material that you reproduce. Almost every country has copyright laws. Obey copyright laws and cite all quotations, references and sources.

**19. THE LEGAL STATUS OF EMAIL**
Remember that while email is often used as a casual form of communication it has the same status as any written communication. The laws of copyright, misrepresentation, defamation, obscenity etc., do pertain to email communication.

**20. CHAIN LETTERS**
Never send or forward chain letters. Chain letters are considered a form of "spamming". These messages can quickly clog an email system.

**21. THE SIZE OF YOUR EMAIL, AND EMAIL ATTACHMENTS**
Know how large a message you are sending, especially if you are sending to a list. Attaching graphics or video clip files, for example, may make your message so large that it cannot be delivered by some mail systems. Large files can be sent in more appropriate ways, including transfer between 'folders' in Macintosh or Windows computers. If the material is already on a Web page just quote the URL. Before attaching a Word Processor file consider whether your recipient will have appropriate software to read it. Don't attach a Word Processor file when its only content is a few lines of (unformatted) text. Include the text in your email message instead.

**22. UNACCEPTABLE USE OF EMAIL**
Don't send large amounts of unsolicited information to people. Email makes people very accessible. Remember to follow chain of command procedures for corresponding with superiors. For example, don't send a complaint via email directly to the "top" just because you can.

**23. ASPECTS TO CONSIDER WHEN YOU ARE UNABLE TO CHECK YOUR MAIL FOR AN EXTENDED PERIOD**
Consider unsubscribing from mailing lists or setting a "no mail" option (when it's available) when you cannot check your mail for an extended period. Delivery receipts, non-delivery notices, and vacation programs are neither totally standardized nor totally reliable across the

range of systems connected to Internet mail. They are invasive when sent to mailing lists, and some people consider delivery receipts an invasion of privacy.

**24. HOUSEKEEPING OF MAIL BOX**

Users should periodically do housekeeping to their mail box (e.g., archiving their mails and compacting their mail box). This is to avoid that problem of "Mailbox exceed quota" occurring and causing the users to be unable to have access to email services.

**25. CONFIDENTIAL INFORMATION**

Avoid sending confidential information by e-mail. If you do, you must secure the information by including it in a Microsoft Word or Excel file and protecting it with a password. Then provide the recipient with the password by means of other communication, for instance by telephone.

**26. PERSONAL USE**

Although the UNIMAS email system is meant for business use, UNIMAS allows the reasonable use of email for personal use according to the following guidelines:

a. Personal use of email should not interfere with work.
b. Personal emails must also adhere to the guidelines in this policy.
c. Personal emails are kept in a separate folder, named Private. The emails in this folder must be deleted weekly so as not to clog up the system.
d. The forwarding of chain letters, junk mail, jokes and executables is forbidden.
e. All messages distributed via the UNIMAS email system, including personal ones, become property of UNIMAS

---

**Definitions:**

---

**Notes:**

## Guidelines for Email File Attachments

---

**References:**
Policy Number: ICTguide002
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: -
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce 2005
Access Level: All staff members and students

---

**Preamble:**

When a virus is hidden in an executable file attached to an email it only requires the recipient to open the file to activate the virus. If the virus is a very new one, the virus detection on the mailhubs may not be able to recognise it and thus allow the infected email reaches the recipient's mailbox. In addition, email attachments should not be too large to avoid clogging up the email system.

---

**Guidelines:**

In order to help protect the campus from email borne viruses, caution is needed to avoid sending or opening emails with executable file attached. Other types of file attachments that are prone to be infected by viruses are exe, .com, .vbs, .scr, .pif, .bat, .inf and .cmd files. Additional file types may be updated by the CICTS IT Officer via the Anjung UNIMAS news and events or technical update in the event of new exploits being used.

---

**Definitions:**

1. CICTS : Centre for Information and Communication Technology Services

---

**Notes:**

## Guidelines of UNIMAS Websites Presentation

**References:**
Policy Number: ICTguide003
Original Approved By: Senate Meeting 74
Date: 15 December 2005
Revision No: 1
Approved By: -
Date: -
Reference Authority: Technical Committee for Information Services
Authors: ICT Policy Taskforce
Access Level: All staff and students

**Preamble:**
UNIMAS strives to provide a usable, informative and up-to-date website that represents and promotes the teaching, research, values and culture of Universiti Malaysia Sarawak. It is desirable that all UNIMAS web presence should reflect the same corporate brand image.

These guidelines govern approved websites. Approved website being those that carry UNIMAS logo or otherwise stated.

**Procedures/ Guidelines:**

**1. Corporate Branding**

While recognizing the complexity and size of UNIMAS web presence, it is desirable to use the corporate brand image (the same look and feel) throughout the entire Universiti Malaysia Sarawak web presence as far as possible. Except in exceptional circumstances the logo must be a link back to UNIMAS Homepage. Cases where such linkage is not considered appropriate should be discussed with UNIMAS Web Master at the *Jawatankuasa Pemantapan Laman Web UNIMAS*.

Micro-sites are allowed to modify the standard template to reflect their various F/C/I/D provided that the corporate logo is visible on the top left hand corner. The logo must be linked to the UNIMAS Homepage.

**2. Colour Schemes**

Webpage situated in the main sections should reflect UNIMAS corporate colours, which are red, blue and yellow.

**3. Screen Sizes**

Websites should be developed to be flexible in their use of different screen sizes. The websites should be tested on a variety of screen sizes before they go "live" to ensure that the sites are easily viewed regardless of the monitor resolution.

**4. JavaScript**
It is not advisable to use too much JavaScript. This is because not everybody has hardware and software capable of making use of JavaScript. JavaScript dependent navigation should also be avoided. Usage of JavaScript for a specific task, within the webpages, should be discussed with UNIMAS Web Master.

**5. Bottom of Page**
Where appropriate the front page of a site should provide a contact email address and disclaimer.

**6. Minimal Download Time**
All Websites should keep download time of the webistes to the minimal. For example, images on a website should not be excessively large in terms of file size. Large file sizes can cause unacceptably long download times for those off campus. If possible a test should be conducted from off campus with a modem. File sizes can be limited by using appropriate image formats, saving images specifically for the web and limiting the number of colours in the image where appropriate. The bigger the file the longer it takes to download.

**7. Hanging Links**
Links should not be created to pages which are planned but do not yet exist. If such allowances are made, then the links should be hidden from public view until the content is available for viewing.

**8. Client Considerations**
Platforms, browsers and screen resolutions need to be considered when designing a site. All considerations must be taken into account, in ensuring the client is able to access the website using which ever browser that is available.

**9. Ease of Use**
The website should be easy to use. Users can access the information within 3 clicks.

**10. Navigation**
Users should be able to navigate through the Websites easily. The users should know where they are, where they have been, and where they can go.

**11. Search**
All Websites should provide a Search feature. This should include a Search box, a button to execute the search, and search results returned which are prioritised.

---

**Definitions:**

1. **Logo:** The official Universiti Malaysia Sarawak Web logotype is to be used throughout the main site and on the front page of all micro-sites.

   The logotype is to be placed in the top left-hand corner of the site. The logotype has an official size, which should not be deviated from. Designers of micro-sites are encouraged to use the logotype on all pages and where feasible the pages should adhere to the style requirements in this Policy. Visitors to the site could enter at any level and hence there

should be sufficient identification to ensure that they are aware they are at Universiti Malaysia Sarawak's website. They also need the ability to navigate to a higher level (micro-site home page or UNIMAS main home page).

2. **F/C/I/D –** Faculty/Centre/Institute/Division

3. **UNIMAS COLOURS –** Red, Blue, and Yellow

---

**Related Policies & Documents:**

1. **ICT011 –** Data Centre Management Policy

---

**Notes:**

---

## Micro-site Information

**References:**
Policy Number: ICTguide005
Original Approved By:
Date:
Revision No: -
Approved By: -
Date: -
Reference Authority:
Authors:
Access Level: All staff and students

**Preamble:**
Micro-sites are websites managed by the respective F/C/I/D to allow for prompt publication of information to the general public. Micro-sites can best convey the individual identity of the F/C/I/D, allowing for better transference of UNIMAS branding to the general public.

In view of the semi-autonomous nature of the various micro-sites, a set of guidelines are needed to govern the use/representation/presentation of information available on every micro-site residing on UNIMAS web-server(s).

**Procedures/ Guidelines:**

1. UNIMAS recognizes all material published/stored/archived within its web-server(s) as property of UNIMAS.
2. Information on micro-sites belongs to the F/C/I/D which manages the micro-sites; in particular and to UNIMAS in general.
3. The managers of the micro-site are responsible for the integrity and currency of the information published on their respective micro-sites.
4. UNIMAS shall not be liable for any loss or damage caused by the usage of any information obtained from any micro-site.
5. Administrators of the micro-sites are responsible for updating the information at least once a month and information must be relevant to the current academic semester.
6. All information published onto the micro-site should be and is deemed approved by the highest authority in the F/C/I/D.
7. Information published on the micro-site is to be managed using the designated content management system.
8. Published articles are to be archived within the content management system and kept for future references.

**Definitions:**

1. **F/C/I/D** – Faculty/Centre/Institute/Division

---

**Related Policies & Documents:**

1. **ICT006** – UNIMAS Web Policy
2. **ICTguide003** – Guidelines of UNIMAS Websites Presentation

---

**Notes:**

---

## Information Quality Guidelines

**References:**
Policy Number: ICTguide006
Original Approved By:
Date:
Revision No: -
Approved By: -
Date: -
Reference Authority:
Authors:
Access Level: All staff and students

**Preamble:**
Micro-sites are websites managed by the respective F/C/I/D to allow for prompt publication of information to the general public. Micro-sites can best convey the individual identity of the F/C/I/D, allowing for better transference of UNIMAS branding to the general public.

In view of the semi-autonomous nature of the various micro-sites, a set of guidelines are needed to govern the quality of information available on every micro-site residing on UNIMAS web-server(s).

**Procedures/ Guidelines:**

1. Presentation of information should adhere to *ICTguide003: Guidelines of UNIMAS Websites Presentation*.
2. Design and representation of information on university websites should adhere to the *Webometrics* criteria.
3. Web-pages should be geared towards increasing the standing of UNIMAS web presence in the eyes of scholars and general public in acknowledged world web-site rankings by adhering to the following:
    a. Information must be relevant to the primary users of the web-site/micro-site; namely staff and students, scholars/researchers
    b. Information must be relevant to researchers both within and outside UNIMAS,
    c. Information should promote scholarly pursuits,
    d. Plagiarism of information in any form is strictly prohibited,
4. Internal/external links should be to academic sources or sources relevant to the subject matter of the linking page. UNIMAS has the right to modify/delete links deemed not suitable for the purpose of the said website.
5. Any form of advertisement whether for personal gain or corporate gain; unless deemed beneficial or approved by the management of UNIMAS, is strictly prohibited.
6. Published pages should not exhibit malicious behaviour, such as phishing or installing viruses, trojans, or other malware.

**Definitions:**

1. **F/C/I/D** – Faculty/Centre/Institute/Division

---

**Related Policies & Documents:**

1. **ICT006** – UNIMAS Websites Presentation
2. **ICTguide003** – Guidelines of UNIMAS Websites Presentation
3. **ICTguide005** – Mandatory Features of University Websites\
4. **Webometrics** – http://www.webometrics.info

---

**Notes:**

---

## Governance of Micro-sites

**References:**
Policy Number: ICTguide007
Original Approved By:
Date:
Revision No: -
Approved By: -
Date: -
Reference Authority:
Authors:
Access Level: All staff and students

**Preamble:**
Micro-sites are websites managed by the respective F/C/I/D to allow for prompt publication of information to the relevant audience, staff, students, scholars and general public. Micro-sites can best convey the individual identity of the F/C/I/D, allowing for better transference of UNIMAS branding to the general public.

In view of the semi-autonomous nature of the various micro-sites, a set of guidelines are needed. These guidelines provide for a responsible approach to the use of micro-sites to further enhance UNIMAS image in the online arena.

**Procedures/Guidelines:**

1. **Ownership**
   - 1.1 All micro-sites that reside within UNIMAS web servers are deemed properties of UNIMAS.
   - 1.2 F/C/I/D is responsible for their respective micro-site(s).
   - 1.3 The homepage webmaster will act as the administrator of the homepage. The webmaster is appointed by Registrar's Office, with the recommendation by the Deputy Vice Chancellor (Research and Innovation).
   - 1.4 The Webmaster is responsible for the managing, maintenance, upgrading, and development of new features for the main website and web server as well as overseeing the micro-site webmasters of UNIMAS.
   - 1.5 The webmaster is also in-charge of super-vision of all micro-sites that have been approved.
   - 1.6 UNIMAS has the right to approve, reject, remove or reinstate any micro-site with or without prior notification.

**2. Naming Convention**

Micro-sites are to be named after the approved short-name of the respective F/C/I/D, followed by the prefix *unimas.my* for example, *www.cicts.unimas.my*.

**3. Structure of Micro-sites**

A micro-site is a representative of the said F/C/I/D as a whole and should house information from the various units/sub-units/project groups/research groups/programs under one URL.

**4. Micro-site Administrators**

4.1 Every micro-site must have designated administrators as approved by Assistant Registrar of respective F/C/I/D. The administrator is responsible for the maintenance of the respective site(s).

4.2 Administrator(s) of the micro-sites will be called micro-site Webmaster and are responsible for the daily upkeep of the micro-site.

4.3 Micro-site Webmasters are allowed to form a team of administrators for their respective micro-sites. Any formation of a team should be duly informed to UNIMAS Webmaster.

---

**Definitions:**

1. **F/C/I/D** – Faculty/Centre/Institute/Division
2. **URL** – Uniform Resource Locator

---

**Related Policies & Documents:**

1. **ICT006** – UNIMAS Web Policy
2. **ICTguide003** – Guidelines of UNIMAS Websites Presentation

---

**Notes:**

---