Information Systems Security Policies

Codes of Practice and Guidelines

Version 2, 11th July 2007

IT & MULTIMEDIA SERVICES (ITMS)
University Tenaga Nasional

CONTENTS

Acknowledgement

The University would like to thank the Imperial College of Science, Technology and Medicine London whose own security policies have been used as the basis upon which this document has been created.

Information Systems Security Policies

Codes of Practice and Guidelines

1. Introduction:

1.1 Information System plays a major role in supporting the day-to-day activities of the University. The availability, reliability, confidentiality and the data integrity of the University's information systems are essential to the success of its academic and administrative activities. Effective security is achieved by working with a proper discipline, in compliance with legislation and University policies and by adherence to approved University Codes of Practice.

1.2 The Information System Security Policies and associated Codes of Practice set out the responsibilities for ensuring the security of Information Systems within University and the procedures to be followed to safeguard the resources provided and the confidentiality and integrity of the information held thereon. The Guidelines provide good security practices that one can follow.

1.3 The Policies apply to all staff and students of the University and all other users authorized by the University. They relate to their use of University-owned/leased/rented and on-loan facilities, to all private systems, owned/leased/rented/on-loan, when connected to the University network directly or indirectly, to all University-owned/licensed data/programs, be they on University or on private systems, and to all data/programs provided to University by sponsors or external agencies.

1.4 The objectives of the Policies are to:

- Ensure that all of the University's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse.
- Ensure that all users are aware of and fully comply with this Policy Statement and all associated policies and are aware of and work in accordance with the relevant Codes of Practice.
- Ensure that all users are aware of and fully comply with the relevant Malaysian legislation.
- Create across the University the awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

1.5 Definitions of the terms used in the Policies and the supporting documentation may be found at Annex 1.

1.6 This Policy Statement has been approved by the Vice Chancellor who has delegated the implementation of it to the Senior Manager, Information Technology & Multimedia Services (ITMS) Department.

2. Responsibilities for Information Systems Security:

2.1 The Deputy Vice Chancellor is responsible for approving the IS Security policies and the associated Codes of Practice, and for ensuring that they are discharged to the various Academic Departments, Divisions and Centres, Academic Services, the University Central Administration and the university students through University Authorised Officers (UAOs), who normally will be the respective Heads of those units. A list of UAOs is appended at Annex 3.

2.2 University Authorised Officers are required to implement the Policies with respect to the systems that are operated by their Departments, Divisions or Centres. They are responsible for ensuring that staff, students and anyone else authorised to use those systems are aware of and comply with them and the associated Codes of Practice. To assist them in this, they are required to appoint a Custodian for each system operated by them, the duties of which are set out in a Code of Practice associated with the Policies.

2.3 It is the responsibility of each individual to ensure his/her understanding of and compliance with the Policies and the associated Codes of Practice.

3. Compliance with Legislation:

3.1 The University has an obligation to abide by all Malaysian legislation. Of particular importance in this respect is the Computer Crimes Act 1997. The requirement for compliance devolves to all users defined in (1.3) above, who may be held personally responsible for any breach of the legislation.

3.2 Summaries of the legislation most relevant to the University's IS policies may be found in the Guidelines accompanying the Policies. Full texts of the most relevant legislation are available from the University Library and the Information Technology and Multimedia Services (ITMS) department.

4. Risk Assessment and Security Review by Departments/ Divisions/ Centres:

4.1 Custodians must periodically carry out a risk assessment of the system that they are currently responsible for, including the IS security controls currently in place. This is to take into account changes to the operating systems, changing university requirements and priorities, and any changes in the relevant legislation, hence revising their security arrangements accordingly.

4.2 University Authorised Officers should establish effective Contingency Plans appropriate to the outcome of any risk assessment. In addition, they are required to carry out an annual assessment of the security arrangements for their Information Systems and submit a report on this to ITMS.

5. Breaches of Security:

5.1 The ITMS department will monitor network activity, reports from the Malaysian Computer Emergency Response Team (MyCERT) and other security agencies and take action/ make recommendations consistent with maintaining the security of the University IS.

5.2 Any University Authorised Officer suspecting that there has been, or likely to be a breach of IS security should inform the Senior Manager of ITMS immediately, who will then advise the University on what action should be taken.

5.3 In the event of a suspected or actual breach of security, the Senior Manager of ITMS may, after consultation with the relevant Custodian or University Authorised Officer, make inaccessible/ remove any unsafe user/ login names, data and/ or programs on the system from the network.

5.4 Any breach of security of an Information System could lead to destruction or loss of security of personal information. This would be an infringement of the Computer Crimes Act 1997 and could lead to civil or criminal proceedings. It is vital, therefore that users of the University's Information Systems comply with the Policies.

5.5 The Vice Chancellor or his Deputy has the authority to take whatever action is deemed necessary to protect the University against breaches of security.

6. Policy Awareness and Disciplinary Procedures:

6.1 The Registrar (Pendaftar) will give a copy of this Policy Statement to all new students, while new members of staff will have a copy given by the Human Resource Office. Existing staff and students of the University, authorised third parties and contractors given access to the University network will be advised of the existence of this Policy Statement and the availability of the associated policies, codes of practice and guidelines that are published on the University web site.

6.2 Failure of an individual student or member of staff to comply with the Policies may lead to the instigation of the relevant disciplinary procedures and in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

7. Supporting Policies, Codes of Practice and Guidelines Notes:

7.1 The Supporting Policies, Codes of Practice and Guidelines associated with this Policy Statement are available on the University Web. Staff, students and any third parties authorised to access the University Network to use the systems and facilities identified in paragraph 1.3 of this Policy Statement, are required to familiarise themselves with these and to work in accordance with them.

8. Status of the Information Systems Security Policies:

8.1 The Policies do not form part of a formal contract of employment with the University, but it is a condition of employment that employees will abide by the regulations and policies made by the University from time to time. Likewise, the Policies are an integral part of the regulations for Students.

Annex 1:

Definition of Terms Used in the Policies and Codes of Practice

1. The Policies: This term refers to the Policy Statement and all the Supporting Policies.

2. The University: For the purpose of the Policies and guidelines this term will be used to refer to Universiti Tenaga Nasional. The document will also use UTN to refer to the University.

3. Campus Network: A system of physical computer network apparatus and logical network connections that is identifiable with University Tenaga Nasional by an Internet network domain-identifier, such as .*uniten.edu.my*, .*utn.edu.my* or by some other means such as the 'UNITEN' domain name for Microsoft Windows. This definition shall also apply where, by agreement of the University, third-party network service providers provide facilities that are identifiable with the Universiti Tenaga Nasional Campus Network, for example 'virtual local area network' (VLAN) and 'virtual wide area network' (VWAN) type connections.

4. Local Area Network (LAN): The combination of networks serving a Department/ Division/ Centre or building and includes all those components up to, but not including the switch/ router and associated components that connect the network to the University backbone.

5. University Backbone: The combination of networks and components that link all the University LANs at the University campus together and provide a gateway to the Internet.

6. University Authorised Officer (UAO): A Head of an Academic Department/ Division/ Centre, Head of an Administrative Division/ Academic Service or other such person authorised by the Vice Chancellor to be responsible for ensuring that the appropriate mechanisms are in place to protect the information systems in their respective Departments/ Divisions/ Centres and the associated data from loss, misuse, corruption or unlawful access.

7. Custodian: A person appointed by the UAO of a University-wide or departmental system to be responsible for ensuring that the security measures adopted for systems under his/ her control meet the requirements of the Policies by carrying out the duties as set out in the Codes of Practice associated with the Policies. In the case of a large system some duties may be delegated, with the approval of a UAO, to named people whose particular duties are set out in writing, although the Custodian retains overall responsibility for the security of that system.

8. Department Network Manager: A person in a Department, Division or Centre responsible for the management of its local area network (LAN).

9. System Administrator: Staff or staff responsible for the day-to-day operation and management of an Information Server or an Information System.

10. Data Owner: A person who authorizes the use of a University information system to originate, store, edit and/ or publish material on that system, subject to the security procedures established by the Custodian of that system.

11. Data User: A person authorized by a data owner to access a University information system to originate, store, edit and/ or publish material on that system, subject to the security procedures established by the Custodian of that system, although the data owner may impose additional security on that data with the approval of the Custodian.

12. Information System (IS): A server or group of servers which stores and processes information for a discrete purpose to facilitate teaching, research and administrative activities, and which may be accessed by staff, students or third parties authorized to do so.

13. Information Server: Any computer system which may be used to store, publish, distribute, advertise or in some other way make available information such as text, images, video and sound to people and automated aspects on the Internet. Examples include but are not limited to: E-mail servers, mailing-list servers, Web servers, Usenet News servers (NNTP servers), FTP servers, Gopher servers, Index servers, Multimedia servers, Mirror archives, Internet Relay Chat servers.

14. Official Information: Information officially approved by a UAO, or an Information Server similarly approved.

15. Personal Information: Information, or a private Information Server, not officially approved but relevant to the authorised user's membership of Universiti Tenaga Nasional.

16. Information Systems Security Officer (ISSO): The Information Systems Security Officer is the person responsible for establishing and monitoring procedures to ensure that the University's administrative information is secure from unauthorised access, protected from inaccurate modification, and available to authorised users in a timely manner to enable them to perform their work.

17. Information Technology & Multimedia Services (ITMS): The department that provides computing services for the whole university. The department also handles the administration of the University Backbone, the University's Central Information Systems and the networks.

Annex 2:

List of Categories of Authorized Users

1. Any current employees of the University, who is working either on a full-time or part-time basis, and requires access to the University IT facilities to fulfill some or all of their job requirements.

2. All part-time or full-time students currently enrolled in the University.

3. Any person who is currently undergoing training or industrial attachment at the University, and requires access to the University IT facilities to fulfill some or all of their training/attachment requirements.

4. Contractors who require the use of the IT facilities in order to carry out their duties may be assigned temporary identification cards and login credentials. These amenities will be revoked as soon as they are done with their work.

Anyone who requires such access to the University IT facilities may apply for it from ITMS.

NB: Anyone found in violation of the University's Information Systems Security Policies can have their access revoked or suspended at any time.

Annex 3:

List of Categories of Authorized Officers

1. Heads of Academic/Colleges

Timbalan Naib Canselor (Akademik)
Dekan Kolej Pengajian Siswazah
Penyelaras (Pusat Perundingan)
Pendaftar
Ketua Pustakawan
Pengurus Besar (Hal Ehwal Awam)
Ketua, Perancangan Strategik & Korporat

Dekan Kolej Kejuruteraan
Ketua Jabatan (Kejuruteraan Elektrikal & Elektronik)
Ketua Jabatan (Kejuruteraan Mekanikal)
Ketua Jabatan (Kejuruteraan Bahan & Pembuatan)
Ketua Jabatan (Kejuruteraan Awam)
Ketua Jabatan (Sains Komputer & Teknologi Maklumat)
Ketua Jabatan (Sains Kejuruteraan & Matematik)

Dekan Kolej Teknologi Maklumat
Ketua Jabatan (Sains Komputer)
Ketua Jabatan (Informatik)

Dekan Kolej Pengurusan Bisnes dan Perakaunan
Ketua Jabatan (Kewangan & Perakaunan)
Ketua Jabatan (Sains Pengurusan & Pemasaran)
Ketua Jabatan (Ekonomi & Pembangunan Usahawan)

Dekan Institut Kajian Liberal
Ketua Jabatan (Bahasa & Komunikasi)
Ketua Jabatan (Kemanusiaan & Kemasyarakatan)
Ketua Jabatan (Pendidikan & Pedagogi)
Pengurus (Seksyen Pendidikan Masyarakat & Riadah)
Ketua Pusat Pengajian Islam dan Peradaban

2. Heads of Administrative Divisions University Officers

Timbalan Naib Canselor (Pengurusan)
Pengurus Kanan (ITMS)
Pengurus (Sumber Manusia)
Pengurus (Perkhidmatan Pengurusan Harta)
Pengurus (Keselamatan)
Pengurus (Perolehan dan Kontrak)
Pengawal Kewangan
Ketua, Pusat Jaminan Kualiti
Ketua , Hal Ehwal Pelajar
Ketua, Pusat Perhubungan Alumni

3. Kampus Sultan Haji Ahmad Shah, Pahang.

Timbalan Naib Canselor (KSHAS)
Provost Kampus Sultan Haji Ahmad Shah
Timbalan Pendaftar (Pejabat Pentadbiran Akademik & Am)
Pengurus (Pembangunan & Hal Ehwal Korporat)

Supporting Policy 1:

Information Technology (IT) Facilities Usage Conditions

The User agrees and accepts that:

1. Use of the IT facilities, such as the network, workstations, printers and the facilities associated with it e.g. software, data, e-mail, world wide web (WWW), bulletin boards, databases and other parts of the University computing system, must be for the purpose of University research, coursework, associated administration or other use. No 'private' work is permitted without prior authorisation.

2. All data/ programs created/ owned/ stored by the user on or connected to University IT facilities may in the instance of suspected wrong doing, be subjected to inspection by University Authorised Officers or any personnel who has been authorised by University Authorised Officers. Should the data/ programs be encrypted the User shall be required to provide the decryption key to facilitate decryption of the data/ programs. Where evidence is found of misuse or of the illegal use of material it will be subject to removal/ deletion.

3. The User must comply with all contemporary statutory and other provisions, Codes of Practice regulations and local rules in force and applicable to IT facilities provided by the University and third parties. Specifically but not exclusively, the User must:

   Not disclose to others her/ his login name/ password combination(s) or access or attempt to access computers or computing services at the University or elsewhere for which permission has not been granted or facilitate such unauthorised access by others.

   Not use or produce materials or resources to facilitate unauthorised corruption, changes, malfunction or access to any University or external IT facilities.

   Not display, store or transmit images or text which could be considered offensive e.g. material of a sexual, pornographic, paedophilic, sexist, racist, libellous, threatening, seditious, defamatory nature, of a terrorist nature or likely to bring the University into disrepute.

   Not forge e-mail signatures and/ or headers, initiate and/ or forward 'chain' or 'junk' or 'harassing' mail.

   Not play computer games.

   Not prevent other bona fide users from accessing computer resources by either hardware or software means (locked screen savers, etc).

Respect the copyright of all material and software made available by the University and third parties, and not use, download, copy, store or supply copyright materials including software and retrieved data other than with the permission of the Copyright holder or under the terms of the license held by the University.

When responsible for INFORMATION SERVERS or the information held thereon, abide by the UNIVERSITY POLICY ON INFORMATION SERVERS, and always ensure that the confidentiality, integrity and availability of the information is never compromised.

4. For a list of other misdemeanours, refer to the list of offences as found in Table 1 and 2 of Guideline 1 accompanying this document.

5. Other than any statutory obligation, the University will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any IT facility provided and/ or managed by the University.

6. While the University takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data, personal or other. The same applies to other IT material submitted to or processed on facilities provided or managed by the University or otherwise deposited at or left on it premises.

7. A user's name, address, photograph, status, e-mail name, login name, alias, University Identifier (UID) and other related information will be stored in computerised form for use for administrative and other operational purposes (e.g. monitoring system usage).

Breaking these conditions may lead to University disciplinary procedures being invoked, with penalties, which could include suspension from the use of all University computing facilities for extended periods and/or fines. Serious cases may lead to expulsion or dismissal from the University and may involve civil or criminal action being taken against the user.

Supporting Policy 2:

Policy on Connecting the University Network

The University depends heavily upon its IT network for research, teaching and administrative activities. It is essential that all members of the University safeguard the stability, integrity and security of the University IT network for use.

To assist in ensuring the availability of an effective, highly available network and to facilitate the rapid tracking down and resolution of any problems by ITMS, the University has implemented the following policy:

1. User Responsibilities

1.1 All users of the network must be aware that they are bound by the University's Information Systems Security Policies.

1.2 All equipment connected to Local Area Networks (LAN) must conform to the appropriate IEEE specifications and run only across the backbone of those protocols supported by the University.

1.3 Only the Department Network Manager may make connections of equipment to the LAN, or someone delegated by the Department Network Manager, not by individual users.

1.4 Users are not allowed to connect network devices that extend networking capabilities to others, such as switches and wireless access points, without the knowledge and permission of ITMS.

1.5 Side-entry connections to the University network, for example via modem connection to the asynchronous port of a workstation, are permitted only with the permission of University Authorised Officers. The modem installation should be supervised or performed by ITMS. Access must be restricted to fully authorised University users and require those users to login formally using a secure login-name/ password combination.

1.6 Students in hostels may connect computing equipment to the University network only with the permission of the Warden or University Authorised Officers. Such systems are then subject to all the statutory and University rules/ regulations currently in force and which are applicable to the fields of computer information systems.

1.7 System administrators must ensure that only authorised University users have access to the Network from their systems.

2. ITMS Responsibilities

2.1. All network addresses, including IP addresses, will be allocated and administered by ITMS.

2.2. All requests for network connection should be diverted to ITMS.

1.3. The only protocol currently approved by the University for use over the University backbone is TCP/IP.

1.4. Physical connections to the University backbone may be made only by ITMS.

1.11. ITMS may, on behalf of the University, and subject to appropriate consultations, restrict excessive use of the backbone bandwidth.

1.12. In the event of unacceptable network events occurring on a LAN, ITMS has the right to gain access to and inspect the configuration of devices or equipment on that network and to request the immediate removal of any devices or equipment that it believes could be the source of the problem.

1.13. In the event of unacceptable events on a LAN causing problems on another part of he University network or on an external network, ITMS has the right to disable any part of the LAN, as necessary, in order to remove the source of the problem. While every effort will be made to contact the Departmental Network Manager, Head of Department and/ or other appropriate staff, this may not always be possible. All services will be reconnected at the first opportunity.

1.14. Failure to comply with the rules for connection to the University network may result in immediate disconnection from the network.

Supporting Policy 3:

Electronic Mail Systems (e-mail) Policy

1.Introduction:

Electronic mail (e-mail) is an important means of communication for the University and it provides an efficient method of conducting much of the University's business. This document sets out the University's policy on the proper use of the e-mail for University purposes, including teaching, research and administration.

2. E-mail Access:

2.1 The University reserves the right to provide current University staff, students, people with honorary appointments and approved third parties with an e-mail account and address. Please contact ITMS for more information on applying for an e-mail account.

2.2 The University reserves the right to revoke or limit the User's access to this e-mail account and address at any time. Common reasons for e-mail access revocation include:

2.2.1 Failure to comply with the University's policies.

2.2.2 The termination of the employee's service with the University.

2.2.3 The student graduating from or leaving the University.

2.3 Should e-mail access be revoked, the User may request that any e-mail sent to his/her e-mail address to be forwarded to another external, non-University related e-mail account, up to a period of no more than 1 month after access revocation. The University however reserves the right to grant/deny this facility to the User.

3. Appropriate Use of University E-mail Resources

Use of e-mail facilities is subject to all the same laws, policies and codes of practice that apply to the use of other means of communications, such as telephones and paper records and shall comply with the University Policy on "Information Technology (IT) Facilities Usage Conditions". Access to and publication of information on the Web shall also be subject to this policy and to that for "Official and Personal Information Servers Connected to the University Campus Network".

3.1 Users may not use University resources and facilities to transmit:

- Commercial material unrelated to the illegitimate educational business of the University, including the transmission of bulk e-mail advertising (spamming).
- Bulk non-commercial e-mail unrelated to the legitimate educational activities of the University that is likely to cause offence or inconvenience to those receiving it. This includes the use of e-mail exploders (i.e. listservers) at the University and elsewhere, where the e-mail sent is

unrelated to the stated purpose for which the relevant e-mail exploder was to be used (spamming).

- Unsolicited e-mail messages requesting other users, at the University or elsewhere to continue forwarding such e-mail messages to others, where those e-mail messages have no educational or informational purpose (chain e-mails).
- E-mails that purport to come from an individual other than the user actually sending the message, or with forged addresses (spoofing).
- Material that is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/ or offensive.
- Material that advocates or condones, directly or indirectly, criminal activity, or which may otherwise damage the University's research, teaching and commercial activities, in Malaysia or abroad.
- Text or images to which a third party holds an intellectual property right, without the express written permission of the copyright holder.
- Material that is defamatory, libelous or threatening. Material that could be used in order to breach computer security, or to facilitate unauthorised entry into computer systems.
- Material that is likely to prejudice or seriously impede the course of justice in Malaysian criminal or civil proceedings.
- Material containing personal data about third parties, unless their permission has been given explicitly.

3.2 Whilst the University provides staff with access to e-mail systems for the conduct of University-related business, incidental and occasional personal use of e-mail is permitted so long as such use does not disrupt or distract the individual from the conduct of University business (i.e. due to volume, frequency or time expended) or restrict the use of those systems to other legitimate users.

4. Penalties for Improper Use of E-mail Facilities.

4.1 Failure to comply with this e-mail policy could result in access to the facility being withdrawn or, in more serious cases, to disciplinary action being taken.

4.2 The Senior Manager of ITMS shall be the final arbiter of whether e-mail messages are in breach of this e-mail policy or not.

5. Privacy.

5.1. Data users must assume that all e-mail by default is not secure and thus, they should not send via e-mail any information that is confidential, private or sensitive in nature. The use of e-mail encryption technologies such as PGP (Pretty Good Privacy) will improve the confidentiality of the e-mail, although they are by no means perfect.

5.2 Users may not, under any circumstances, monitor, and intercept or browse other users' e-mail messages unless authorised to do so.

5.3 In all other circumstances, monitoring, interception and reading of other users' e-mail by network and computer operations personnel or system administrators may only occur with the permission of the Senior Manager of ITMS.

5.4 The University reserves the right to access and disclose the contents of a user's e-mail messages, in accordance with its legal and audit obligations, and for legitimate operational purposes. The University reserves the right to demand those encryption keys, where used, be made available so that it is able to fulfil its right of access to a user's e-mail messages in such circumstances.

Supporting Policy 4:

Policy of Official and 'Personal Information Servers' Connected to the University Campus Network

1.The provision and use of any Information Server (IS) connected to the University Campus Network is subject to the following conditions:

1.1. Each Data Owner(s) agrees to be bound by the 'Conditions of Use of Information (IT) Facilities' and the relevant Codes of Practice.

1.2. Each Data Owner and Systems Administrator agrees to take at all times every reasonable care to ensure that all material held on a server:

- Is lawful.
- Complies with the Information Technology (IT) Facilities Usage Conditions"
- Does not contain links to unlawful material or material that does not comply with the University *Information Technology (IT) Facilities Usage Conditions*
- Does not, purport to promote or comment, in the University's name, upon any commercial goods, products or services, unless approved by a UAO.
- Does not purport to promote or comment upon any company, partnership, consortium or consultancy or any 'private' activity of the Information Owner or any other person, unless approved by the UAO.
- Each Information Server may serve either official or personal information but not both.

The University reserves the right to bar access to Information Servers containing material considered illegal or likely to bring the University into disrepute. Such action will be normally invoked as a result of a request by a UAO to the Senior Manager of ITMS. The University also reserves the right to take disciplinary action in these circumstances.

The University will not be liable for any loss or damage suffered by the Information Owner as a result of barring access to or removal of material. Where the Information Owner considers that the University has acted disproportionately, inappropriately or *ultra vires* in barring access to and/ or removing the material then she/ he has the right of appeal through the normal University grievance procedures.

The Data Owner or System Administrator must ensure that procedures exist for the immediate disconnection of the Information or Information Server from the campus network at all times including evenings, nights, weekends, bank holidays and during periods of University closure.

Additionally for University Information and Information Servers:

- All Official Information Servers must be authorised by a UAO and registered with ITMS.
- All material published must be duly authorised by a UAO.
- All material is subject to both the statutory requirements applying to any publisher and also to the University Regulations applying to University publications.

- An approved University identifier must appear on official information.

Additionally for Personal Information and Information Servers:

- No coat-of-arms, crest, logo, logotype, page layout, format or any other device belonging to the University may appear, unless approved by a UAO.
- The material must be relevant to or associated with the data owner's authorisation to use the University's IT facilities.

These regulations and the appearance of Personal Information, how so ever referenced, do not imply in any way whatsoever that the University approves or endorses the Personal Information or takes any responsibility for the Personal Information itself or any material or opinions contained therein.

An approved disclaimer must appear on all Personal Information indicating that the University does not formally publish this information.

Code of Practice 1:

Appointment and Role of Custodians of Information Systems

1. University Authorised Officers must appoint, for each Information System (IS), a Custodian who will be responsible for that system.

2. Custodians must ensure that the security of their system(s) meet(s) the requirements of the University Information Systems Security Policies in terms of both physical and data security, guarding against the illegal access and the use of illegal copyright systems, applications and data. To this end they should ensure that:

2.1 All staff, students and other users are authorised before they may access or use University IT facilities.

2.2 All computers connected to the University campus network are registered with the ITMS Department.

2.3 The authorised owner of each user/login name registered on their systems can be readily, uniquely and precisely identified.

3. Custodians must adopt appropriate levels of security according to the value/ sensitivity/ access requirements of the system/ data to the Department/ Division and/ or sponsor. They must facilitate change control and set up procedures for dealing with contingencies and recovering from them. (*See Code of Practice on Contingency Planning*)

4. Custodians must report, in writing or electronically to the Senior Manager of ITMS and to their UAO, any incident that results in, or has the potential to result in, a breach of security of that system, whether that be physical security or information security using a standard report form. (*See Code of Practice Reporting of IT Security Incidents*)

5. Custodians must carry out an annual security assessment of their system(s) and provide a written report of the outcome for their UAO who will then collate a single report for all the systems under his/her control and send it to the IS Security Officer. (*See the relevant Administrative Guide*)

6. A Custodian, particularly of a large system, may delegate some of his/her duties, but is ultimately responsible for ensuring that they are carried out.

Custodians must ensure that, where there is a business need for access to the University IT facilities by a third party from another organisation, a security risk analysis should be carried out to determine the security implications and control requirements. The risk analysis should take into account the type of access required, the value of the information, the security measures employed by the third party and the implications of access for the security of the University's IT infrastructure. The controls should be

agreed and defined in a contract with the third party who will be required to comply with the University's IT policies. (*See Guidance Note on Information Security Conditions in Third Party Contracts*)

Code of Practice 2:

Contigency Planning (Planning to minimise the chances of disasters occurring and to recover speedily from any which do occur)

1. Introduction:

All IT entails the processing of data via licensed, third party shareware, freeware or originally developed software on appropriate computer hardware. That data and software (hereinafter collectively referred to as data) represents a significant University and personal investment. Its loss, whether by human error, deliberate damage or hackers, hardware or software failure, media failure or building disaster e.g. a fire, could seriously degrade the ability of a Department/ Division/ Centre or some component of it to continue to function effectively. Even more importantly, confidential or personal data falling into the wrong hands could prejudice a research contract or result in a prosecution for failure to comply with legislation covering data security.

Individual members of staff, students and authorised third parties are responsible for taking such steps as are necessary to minimise the chances of the loss or corruption of data as a result of such a contingency occurring. To ensure that such an event is not catastrophic, University Authorised Officers must ensure that adequate procedures are put in place to facilitate business continuity (disaster recovery) in respect of the systems under their control, whether that is for teaching, research or administration

2. Business Continuity (Disaster Recovery) Planning Framework:

2.1 In the case of computers, a business continuity plan should specify clearly the conditions for its activation, as well as the individuals responsible for executing each component of the plan. Plans should be consistent with established University emergency procedures for such matters as provision of computing services, telecommunications, office/ laboratory accommodation etc.

2.2 A business continuity plan will typically have four main components:

- Emergency procedures, which describe the immediate action to be taken following a major incident which jeopardises business operations and/ or human life;
- Fallback procedures, which describe the action to be taken to move essential business activities and support services to alternative temporary location;
- Resumption procedures (disaster recovery), which describe the actions to be taken to return to normal full business operations.
- A test schedule, which specifies how and when the plan will be tested and which requires the results of any test to be documented so that it can be subject to audit.

2.3 UAOs are responsible for ensuring the provision of fallback arrangements for the provision of alternative, suitable facilities for teaching, research and administration e.g. computers, disk space, applications, software and workstations.

2.4 ITMS will give assistance and support in the preparation of fallback arrangements for the provision of alternative technical services, such as computers and communications, as appropriate.

2.5 UAOs should ensure that the contingency plans are regularly updated in order to protect the investment made in developing the original plan and to ensure its continuing effectiveness.

2.6 Contingency plans should be dated and copies held centrally by UAOs so that they are available for inspection, having been given due notice, by the IS Security Officer.

3. Backup Procedures:

3.1 In order to effect the swift and successful operation of a contingency plan, procedures should be established for the backing up of work done on computers on a regular and systematic basis, whether that data is held on the hard disk of a stand-alone computer, remotely on a server operating in relation to a cluster of PCs or on a large system.

3.2 Backup procedures are essential to protect against loss as well as ensuring that both data and software are regularly and securely backed up.

3.3 Disaster recovery procedures are necessary to ensure that, should an entire hardware system be stolen and/ or destroyed, replacement hardware can be acquired. The operating system, applications and data can readily be reloaded onto the replacement hardware. To facilitate a rapid recovery from an emergency, copies of the backup and relevant documentation, including software licenses, must be stored remotely. To do this, adequate backup procedures/ facilities must have been instigated and the backup media, records and licensing documentation must be available and the media must be readable by the replacement hardware.

3.4 Detailed guidance on procedures that should be adopted to meet the requirements of this Code of Practice may be found in the Information Systems Administrative Guide. Additionally, ITMS can provide information regarding backup strategies, hardware, software and on its central backup service.

4. Responsibilities & Guidance:

ITMS is responsible for backing up the University's Central Information Servers. The responsibility for ensuring the backing up of other systems lies with the Custodians of those systems. Responsibility for the backing up of data and software held on individual computers lies with the users.

Code of Practice 3:

Employment, Education & Training

To reduce the risks of human error, theft, fraud or misuse of facilities, the matter of information security should be addressed at the recruitment stage. Job descriptions should identify all relevant security responsibilities and potential recruits should be adequately screened.

1. Security in Job Descriptions

Security roles and responsibilities, as laid down in the University IS Security Policy, should be included in job descriptions, where appropriate. These should include any general responsibilities for implementing the security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.

2. Recruitment Screening

Applications for employment should be screened if the job involves access to University Information Systems for the handling of commercially or otherwise sensitive information, as identified by the relevant Custodian. The checks should include obtaining two character references, checking the accuracy of CV's, confirmation of academic or professional qualifications and carrying out an identification check.

3. Confidentiality Agreement

When signing acceptance of conditions of employment or Student Regulations, users of IT facilities will be required to agree to respect the confidentiality of any information that they encounter in the course of their work/studies. Agency staff and approved third party users of University Information Systems will be required to sign a confidentiality agreement as part of their contract. Confidentiality agreements should be reviewed when there are changes to the terms of employment or when contracts are due to be renewed.

4. Information Security Education and Training

New users of IT facilities, staff, students and approved third parties, should be instructed on the University policies and codes of practice relating to information security and given training on the procedures relating to the security requirements of the particular work they are to undertake and on the correct use of the University's IT facilities in general before access to IT services is granted. They should be made aware of the reporting procedures to be adopted in respect of different types of

incident (security breach, threat, weakness or malfunction) which might affect the security of information they are handling, as set out in Code of Practice 6 of the Information Systems Security Policy.

Code of Practice 4:

Firewall Installation

1. Introduction

To facilitate its teaching, research and administration the University provides staff, students and authorised third parties with access to the Internet. One disadvantage of this is that other from outside the University will attempt to obtain unauthorised access to the University network, a process known as *hacking*. To preserve the integrity of its systems and the confidentiality of the data contained therein, a balance has to be achieved between allowing others with no access to the University network and free access to it. It is recommended practice that firewalls are placed between the University systems and the Internet, ensuring that access is provided only to those authorised to do so. In the case of University systems holding very sensitive data, firewalls will also need to be established to prevent internal hacking.

2. Firewall Function

The overall strategy in the development of firewalls is based on meeting some or all of the following requirements.

(a) The prevention of unwanted traffic on the insecure external network getting access to the secure private network.

(b) The separation of those applications that need to gain access to the secure private network from computers that require maximum protection e.g. Mail and WWW.

(c) The provision of an encryption/ decryption service to clients accessing the data held on computers on the private network.

Prohibiting access to those who are not expressly permitted provides a more precise control than permitting access to those who are not expressly prohibited.

3. Firewall Construction

Firewalls consist of one or more filters and gateway separating a private system from the Internet. They can be configured to perform Packet Filtering, Applications Filtering or Encryption/ Decryption. Packet filtering, in addition to filtering out those packets of data which are flowing from the public

network that are not wanted on the private network, also permit packet monitoring in which hacker activity can be identified and traced.

Application gateways should be installed to ensure that applications such as e-mail and WWW services are run on a dedicated machine, thus protecting the main processing computer on the private network. Encryption should be used to protect sensitive data travelling to authorised users on a network to protect it from being read by hackers.

4. Firewall Strategy

To meet the security challenge posed by hackers, the University adopts a hierarchical approach using the various firewall techniques:

- Routers are situated between the University network and the outside world. The University does a limited amount of packet filtering to hamper several well-known methods of attack. Spot checks are carried out for unusual activity e.g. an excess number of accesses from a particular site, while sites known or suspected to be harbouring hackers can be banned.
- Each departmental system consists of its own routed and hence trusted segments. A department cannot 'snoop' data from another department. Packet filtering is not carried out but unusual activity is monitored.
- A mail relay and servers have been set up to handle all mail entering and leaving the University. This gateway then communicates with the departmental mail servers. Those looked after by KMC are upgraded with all the applicable security patches as soon as they have been received and authorised. Mail servers are known to be a specific target of hackers so individual departments, divisions and centres should not set up their own mail servers. Any department wishing to set up their own mail servers must first obtain the permission of KMC.
- Currently there are no FTP sites available for anonymous access at the University. All other departments are strongly advised against offering their own anonymous FTP services and certainly not on departmental computers and file servers. Any department that wishes to offer their own anonymous FTP service must first obtain the permission of KMC.
- The use of encryption should be considered to enhance the privacy of transmitted data to provide even greater security e.g. Telnet and Mail.
- The use of firewall technology should be considered to protect specifically sensitive parts of the network.

Code of Practice 5:

Reporting of IS Security Incidents

1. It is essential that incidents affecting the security of the University Information Systems, or with a potential to do so, should be reported immediately to the Senior Manager of ITMS or Information Systems Security Officer, who will take whatever immediate action is deemed necessary. Likewise, Custodians should be informed of any such incidents identified at the network end by ITMS.

2. Users of the University's IT systems should report any observed or suspected security weaknesses in, or threats to, those systems to their system Custodian. In no instance should they attempt to prove a suspected weakness as this could lead to a potential misuse of the system.

3. If users should notice any software that does not appear to be working correctly, i.e. according to specification, they should report the matter to their local IT support staff. If they suspect that the malfunction is due to a malicious piece of software e.g. a computer virus, they should stop using the computer, note the symptoms and any messages appearing on the screen and report the matter to their local IT support staff.

4. Formal reports of any such incidents or suspected weaknesses should be recorded by system Custodians on the form attached and sent to the University IS Security Officer as soon as possible afterwards in order that the effectiveness of the implementation of the IS Security Policies can be monitored.

5. Where incidents take the form of misuse of a system or data contained thereon by a member of staff, a student or a third party, the action taken by ITMS or the Custodian should also be reported. (See Guidelines on Disciplinary Action for Misuse of Computing Facilities by Students).

6. The IS Security Officer should liaise with the Senior Manager of ITMS, the Vice Chancellor or other senior University Officer, as appropriate, to determine what further action should be taken, if any, and to record the outcome. He or she will also collate and analyse records of such incidents and will report to the Information Security Group any trends which emerge and recommend any additional action that should be taken on a University-wide basis to try to prevent their occurrence in the future.

7. A sample report form to be used for reporting security incidents to the IS Security Officer is annexed to this Code of Practice. A copy is available on the University web site.

Guidelines 1:

Misuse of University IT Facilities Recommended Levels of Punishment for Students

As part of the entry conditions imposed on students entering the University, summary punishment may be imposed on students breaking the University regulations, and this punishment may comprise of a fine or a penalty.

In cases of the misuse of University IT facilities, it has been agreed upon that the appropriate authority to impose summary punishment should be the relevant Head of Department/Division, in accordance with the Students' Code of Conduct. ITMS will assist Departments/Divisions in identifying the perpetrators of misuse and give advice on the appropriate level of summary punishment to ensure consistency across University.

The following lists of misuse/abuse categories together with their seriousness ratings were compiled by ITMS for the purpose of helping the Heads of Department, Divisions and Centres reach a decision on the level of punishment to be imposed.

Broad ranges of seriousness ratings (on a scale of 1 to 10, with 10 being the most serious cases) are given to cover degrees of offence, wastage and misuse. Attention should be paid to the magnitude and nature of misuse the level and content of offensiveness, obscenity, abusiveness, harassment and criminality could upgrade a simple misuse to serious or even criminal misuse. Misuse affecting external institutions and that which brings University into disrepute should be viewed even more seriously.

The guidelines present IT offences in three sections:

1. Misuse violation of the Conditions of Use of University IT facilities and associated Codes of Practice.

2. Serious misuse more serious violations requiring disciplinary hearing and/or legal proceedings.

3. Criminal misuse very serious violations necessitating legal proceedings. In some circumstances `Community Service' of some description may be more appropriate than a fine.

In some circumstances, some form of community service may be more appropriate than that of a fine.

1. Misuse – Violation Of The Conditions Of Use Of University IT Facilities And Associated Codes Of Practice:

Short Name	Offence Description	Seriousness Rating
Disclosure	Unauthorised disclosure of a login name/ password to another person, thus giving unauthorised access to University IT facilities.	3 to 6

Trash Printing	Printing of non-course related material. Printing of multiple copies to avoid photocopying charges.	1 to 4
Chain Lettering	Originating or propagating chain mail.	1 to 4
Misappropriation	Use of computing resource for private work without the permission of the owner of that resource.	1 to 4
Lewd Materials	Display or Printing of Offensive Material as defined by the Code of Practice.	3 to 7
Strangers	Admitting non-authorised person to controlled areas such as the university's computer rooms.	5 to 8
Game Playing	Annoyance & Denial of Service to Students	2 to 4
Hot Webbing	Setting up a Web site that does not conform to the University's policies.	4 to 8
Bad Links	Setting up WWW links on a Web Site to material of an objectionable nature on any computer connected to the University network.	3 to 7
Broadcasting	Broadcasting e-mail indiscriminately.	2 to 5
Spoofing	Sending e-mail under an alias or pretending to be someone else.	4 to 9
Spamming	Filling up someone's mailbox with unsolicited e-mail	3 to 6
Harassment	Sending e-mail of an offensive nature or the repeated sending of inoffensive materials.	5 to 10
Bad Files	Offensive and/ or non-academic material kept on file space on a University server or any computer connected to the University network.	4 to 8

Table1

NB: If the content of the material is threatening, racist, seditious or of an obscene nature then this has to be considered as serious or possibly criminal misuse and dealt with accordingly.

2. Serious Misuse – more serious violations requiring stricter disciplinary and/ or legal Proceedings

Short Name	Offence Description
Snooping & Trapping	Setting up software to capture user names, passwords and other sensitive information. Examples include, but are not limited to: key-loggers, network sniffers.
Hacking	Attempting to gain unauthorised access to a computer.
Pirating	Transfer of copyright software to a private computer without the University's permission. Illegal use, possession or provision of copyright software/ data.
Harassment	Sending e-mail or chat room material of a threatening, racist or obscene nature on a computer connected to the University network.
Criminal Webbing	Putting material on a web site that is forbidden by Malaysian laws using any computer connected to the University network
Denial of Service	Preventing access of bona fide students to computing resources by hardware or software means (locked screen savers, etc.)
Trashing	Unauthorised alteration or destruction of data held on a computer or server.
Rogue Posting	Sending of objectionable material to a Bulletin Board or Chat Room while logged on to the University network.
Trashing UTN	Having material on an external information server that directly or by association brings the University into disrepute.
Defamation	Posting material that is slanderous or libellous using any computer connected to the University network computer.
'Hot' Files	Having files containing material of a criminal nature held on any computer connected to the University network.

Table2

NB. Many of the actions involve violation of national legislation in such areas such as Computer Crimes, Data Protection, Pornography, Defamation etc.

3. **Criminal Misuse** – very serious violations necessitating legal proceedings Serious Misuse, an activity with intent to harm, can become Criminal Misuse if the scale is of sufficient magnitude. In this event, the University may be obliged to call in the police.

Guidelines 2:

Security Conditions In Third Party Contracts

Arrangements involving third party access to the University's Information systems should be spelled out in a formal contract to ensure compliance with the University's general and supplementary policies on Information Security and knowledge of the accepted Codes of Practice. The contract should be in place before access to any system is provided and a copy of the relevant policies and codes of practice provided.

The following items should be considered for inclusion in the contract:

a) A description of each Information System to be made available.

b) A requirement to maintain a list of individuals authorised to use the service.

c) The times and dates when the service is to be available.

d) The respective liabilities of the parties to the agreement.

e) Procedures regarding the protection of the University's assets and the confidentiality of the information contained therein.

f) Restrictions on the copying and disclosure of information.

g) Responsibilities to comply with current Malaysian legislation and University policies.

h) The right of the University to monitor and revoke user activity.

i) Measures to ensure the return or destruction of information and assets at the end of the contract.

j) Responsibilities regarding hardware and software installation and maintenance.

k) Involvement by the third party with subcontractors and other participants.

Guidelines 3:

Malware protection

1. Introduction:

A malware, short for malicious software, is any application whose purpose is to infiltrate or damage a computer system without the owner's informed consent. There are many types of malware, but generally they can be categorised into 5 major categories:

- Virus
- Worm
- Trojan
- Spyware
- Adware

A computer virus is a piece of software that infects other executable software and causes damage on the computer. A worm is a piece of software deliberately designed to distribute itself from one computer system (PC or MAC) to another unbeknownst to the user of the system. They spread rapidly from one computer to another causing increasing disruption and damage. Computer users are required to run an up to date suite of virus protection programs to safeguard their own computers and indirectly, the others in the community. As well as running anti-virus software you are advised to take other precautions to avoid infection.

Another type of malware is called a Trojan or a Trojan horse. A Trojan is a program or a piece of code that appears harmless, yet it contains malicious logic that allows the unauthorised collection, falsification or destruction of data. It tends to masquerade as a benign application e.g. a game, a useful application etc. Unlike viruses, Trojans tend not to replicate themselves, but they can be just as destructive, as it allows others to control your computer without your knowledge.

Spywares basically collect information about what is on your computer and whatever it is you are doing on your computer, before sending the data to another third party. Adwares are a type of spywares which will use the information gathered to display targeted advertisements on your computer.

2. Viruses types and effects:

There are two types of virus:

- Benign. These do no real damage to the computer. They may wait a predetermined date or time and then display some sort of message.
- Malignant. These inflict malicious damage on the computer. A malicious virus might alter programs or data or cause the computer to not work. Some of the more malignant viruses will delete files or erase your entire hard disk.

Most of these viruses work at operating system level. Increasingly, viruses are written in the macro language of applications such as Microsoft Word and potentially can infect any platform that can run those applications. The infected program might terminate abnormally and write incorrect information on one of your system areas.

There are also Hoaxes about viruses that are sent via e-mail which disrupt normal activity by being sent onwards by the recipients in their own e-mails, thus cascading to an ever-increasing number of persons. Do not, therefore, perpetuate a known hoax by copying it on to others. If you are not sure whether a warning about a virus is a hoax, check with KMC.

3. How Viruses Spread:

The most common way in which a virus is spread is via an infected thumb drive or e-mail attachment. Viruses can be of different types such as:

- Transferring infected documents and data files as e-mail attachments can spread macro viruses
- Boot sector viruses can only be transmitted by a diskette. People who use diskettes that have been used on a number of different computers increase their chances of picking up an infected diskette and spreading the virus. As diskettes become less used, due to the increasing popularity of thumb drives, boot sector viruses are not so common nowadays.
- Shareware, free disks and games downloaded from the Internet, are a common source of viruses and they can often be found in shrink-wrapped software distributed by major companies and on diskettes accompanying hardware. Diskettes should always be scanned for viruses before they are used.
- File viruses can be spread by downloading infected programs from bulletin boards and the Internet or as e-mail attachments. You should take care to check any software transferred over a network or communications link before using it.

Infections can affect both networked and stand-alone computers. Particular care should be taken to protect networked file servers from infection.

Worms on the other hand, usually spread through the network by exploiting vulnerabilities on one's computer. Operating systems such as Windows have vulnerabilities which can be exploited by worms to gain entry.

4. Protecting your Computer from Virus and Trojan Infection

- Ensure your computer is running the most up to date version of an anti virus tool. ITMS will recommend one and has copies available. There are also some good and free anti-virus software available from the Internet, such as AVS and AVG. The anti-virus software should be configured to scan all files coming into your computer, and be updated regularly and constantly.
- Ensure your computer has a personal firewall running (Windows XP Professional comes with a free personal firewall).

- Ensure your computer is running the most up to date version of an anti-spyware tool. ITMS will recommend one and has copies available. There are also some good and free anti-spyware software available from the Internet, such as Windows Defender and Spybot S&D. Remember to update your anti-spyware regularly and constantly.
- Update your computer operating system and applications with the latest software patches regularly. Software patching is essential to ensure the security of one's computer.
- Make sure that your e-mail client e.g. Microsoft Outlook does not open attachments automatically when reading e-mails.
- Always scan media received from unreliable/unknown/unrecognised resources and shrink-wrapped software attached to publications or new hardware.
- If you lend your diskette to someone, always scan it when it is returned. This applies to other forms of portable media such as thumb drives and portable hard disks.
- To avoid being infected by viruses/worms from thumb drives and portable hard disks, it is recommended that you disabled the autoplay/autorun feature for Windows XP/Vista PCs.
- Always scan files downloaded from the Internet or Bulletin Boards, including shareware.
- Avoid direct opening or executing e-mail attachments. Always save the email attachment and scan for viruses before reading or executing them.
- Set a screensaver password and bootup password in your computer to prevent an unknown/unauthorised user from using it.
- Disable the facility to boot computer from the floppy drive and set the CMOS password to prevent others from changing the settings.

Guideline 4:

Securing Your Password(s)

One of the fundamental methods of protecting an Information System is via the use of a login name/ password pair. Having a strong, hard-to-guess password is very important, as it is the crux of security. Hence, the University provides the guidelines below to help the user understand what a strong password should be like:

1. The length of the password should be at least 8 characters. Although there is theoretically no limit to the maximum length, bear in mind that the longer a strong password is, the harder it is to remember it.
2. The password should consist of a mix of characters from at least **three** of the following group:
    - Upper-case alphabets: A, B, C, D, E,..Z
    - Lower-case alphabets: a, b, c, d, e, ..z
    - Numbers: 0, 1, 2, 3, 4, .. 5
    - Special characters: %, !, (, +, # .. etc.
3. The password should **not** be an easily deducible word, such as:
    - A dictionary word e.g. *password*, *love* etc.
    - A relative's name, e.g. your wife's name, your dog's name.
    - Brand, product or company name, e.g. *Marlboro, Toshiba.*
    - A place or country's name, e.g. *Singapore*, *Thailand*.
    - Obscene words or derivatives of it.
4. Avoid simple letter/ numeric in any of the above, e.g. substituting 'o' with '0' or 'l' with '1'.

The password is assigned for **your** use alone. Hence, it is important that you follow the steps below to ensure that your password is not compromised:

- When you first obtain the login name/password, immediately change it a new one instead of using the default password.
- Never disclose your passwords to anyone else **unless** he or she is an authorised officer of the University. Even then, make sure that he or she is really who they claim to be.
- Never type in your password while someone is behind you and possibly looking on.
- Never send your password to someone else by phone, e-mail or mail.

- If you suspect that your password has been compromised, immediately change it to a new one. In the case of a suspected breach, contact the nearest KMC staff or the Custodian immediately.
- When changing your password, always choose a new one that is quite unlike your old one. Avoid substituting just a few characters.

Tips:

- Never to write down your password: try to memorise it if you can.
- Configure your system to make it so that they will prompt you for a password (i.e. do not configure it to store your password in a local profile).
- Never to use the same password for more than one system - whether or not the second or subsequent system is at the University.
- Change your password regularly.
- Never tape passwords to a wall, under a keyboard or in other easily discoverable areas.
- A commonly used practice is the use of an acronym of a sentence as a password. It is easier to remember a sentence than a random mix of characters. For example, a password such as *IluvUTN2m* is easier to remember as "I love Universiti Tenaga Nasional too much" than as it is. Of course, please do not use this example password!