ICT SECURITY POLICY

University of Malaya (UM)

4th February 2013

Version 2.0

DOCUMENT HISTORY

VERSION	APPROVAL	DATE
1.0	ICT COUNCIL MEETING # 1/2011	3 MAY 2011
2.0	ICT COUNCIL MEETING # 1/2013	4 FEB 2013

UM ICT SECURITY POLICY AMMENDMENT SCHEDULE

DATE	VERSION	AMMENDMENT DETAILS
10 December 2012	2.0	i. **New Title: ICT Security Risk Assessment,** page number 17 ii. **ARTICLE 020103 Chief Technology Officer (CTO),** page number 21-22: CTO role and responsibilities amendments. iii. **ARTICLE 020104 ICT Security Officer (ICTSO),** Page number 24: ICTSO role and responsibilities amendments. iv. **ARTICLE 020106 User** paragraph (c), page number 26: undergoing security filtering if required to manage high-level official information. v. **ARTICLE 020108 UMCERT Team,** page number 29: UMCERT membership amendments. vi. **ARTICLE 110104 Legislative Requirements,** page number 99: List of additional legislations and rules that must be followed by all users at UM.

TABLE OF CONTENTS

INTRODUCTION

The UM ICT Security Policy contains rules that must be read and adhered to in the usage of UM information and communication technology (ICT) assets. This policy also states to all users at UM, their roles and responsibilities in protecting these UM ICT assets.

OBJECTIVES

The UM ICT Security Policy was created to ensure that UM activities proceed smoothly and to minimize the effect of ICT incidents.

This policy is also intended to make the sharing of information relevant to the operational need of UM easier. This can only be achieved by ensuring that all ICT assets are protected.

Therefore, the main objectives of UM ICT Security are as follows:

(a) Ensure that UM operations proceed smoothly and minimize damage or destruction;

(b) Protect the interests of all parties that rely upon information systems from the effects of failure or weaknesses in terms of secrecy, integrity, readiness, information validity and communications; and

(c) Prevent the misuse or theft of UM ICT Assets.

POLICY STATEMENT

Security is defined as a state that is free of unmitigated threats or risks. Security enforcement is a never ending process. It involves scheduled activities that must be performed from time to time in order to ensure security as the potential threats and risks are always changing.

ICT Security is a state where all transactions involving the supply or provision of ICT system based services proceeds seamlessly without any interruptions that could compromise security. ICT Security is closely related to the protection of ICT assets. ICT Security consists of four (4) components that are:

(a) Guarding official secrets and university secrets from access by illegal entities;

(b) Ensuring the validity and completeness of all information;

(c) Ensuring the availability of information when required by users; and

(d) Providing access only to legal users and legal information recipients.

The UM ICT Security Policy encompasses all forms of electronic information and is intended to protect the safety of that information as well as the availability of that information to all valid users. The main features of information security are as follows:

(a) Secrecy – Information cannot be randomly exposed or accessed without authorization;

(b) Integrity – Data and information must be accurate, complete and current. It can only be modified using allowed methods;

(c) Non refuted - Data and information sources must be from the source of origin and can not be refuted;

(d) Validity – The validity of data and information must be ensured; and

(e) Availability – Data and information must be accessible at all times.

Other than that, the measures towards ensuring ICT security are based on assessments relevant to current intrinsic weaknesses in ICT assets; threats arise from those weaknesses; risks that may arise; and the appropriate preventative measures that can be taken to combat those risks.

SCOPE

UM ICT assets consist of hardware, software, services, data or information as well as humans. The UM ICT Security Policy sets the following basic requirements:

(a) Data and information should be accessed continuously, accurately, easily and validly. This is critical to allow decisions and service delivery to be made well and effectively; and

(b) All data and information confidentiality must be protected and handled with care at all times to ensure the accuracy and completeness of the information as well as to protect the interests of UM, service and the community.

In order to ensure that ICT asset security is ensured at all times, the UM ICT Security Policy encompasses protecting all forms of university information whether entered, created, destroyed, stored, generated, printed, accesses, distributed, transmitted and that has been made as a security duplicate. This will be done via the creation and enforcement of a control system and procedures in the handling of the following:

(a) Hardware

This includes all assets that support the processing of information as well as UM storage facilities. For example computers, servers, communications equipment and etcetera;

(b) Software

This includes programs, procedures and rules that are written and the relevant documentation as pertains to the computer operating systems, data center systems, network system software, or office applications that provide information processing for UM;

(c) Services

This includes services or systems that support other assets in performing their functions. Examples are:

i. Network services like LANs, WANs and so on;
ii. Access control systems such as card access systems; and
iii. Support services such as electrical facilities, air-conditioners, fire control systems and others.

(d) Data and Information

This includes information on paper or electronic messages that contain information that is used to achieve that mission and objective of UM. For example, documentation systems, operating procedures, UM records, customer profiles, data centers and data files, archived information and others;

(e) Humans

Individuals who have the knowledge and ability to perform the daily UM job scope to achieve the mission and objective of the agency. These individuals are assets based on the tasks and functions that are performed; and

(f) Computer and Communication Premises

All facilities and premises that are used to house items **(a)** - **(e)** above.

Every Item above must be closely guarded. Any security breach or protective weakness is seen as an infringement of the security rules.

PRINCIPLES

The principles that form the foundation of the UM ICT Security Policy that must be adhered to are as follows:

(a) Need-to-know access policy

Access to the use of ICT assets is only provided for specific purposes and is limited to certain users on a need-to-know basis only. This means that access is only **provided is the function** or role of a particular user required that information. Consideration for access is given based on the information category as stated in the Security Orders document paragraph 53, page 15;

(b) Minimum access rights

User minimum access rights are given at the minimum a set level that is to view and/or to read only. Authorization is necessary in order for a user to create, store, update, alter or delete any information. This access right will be reevaluated from time to time based on that roles and responsibilities of the user in question;

(c) Accountability

All users are responsible for all their actions as pertains to UM ICT assets. This responsibility must be expressed clearly with the appropriate level of sensitivity for every ICT source. To ensure that this responsibility is adhered to, ICT systems must be capable of supporting facilities to detect and confirm that information system users are held accountable for their actions.

Accountabilities and responsibilities of users include:

i. Preventing exposure of information to unauthorized parties;

ii. Checking information from time to time to ensure that it is accurate and complete;

iii. Ensure that the information is readily usable;

iv. Protect the confidentiality of passwords;

v. Follow set security standards, procedures, measures and guidelines;

vi. Pay attention to information at all stages especially during creating, processing, storage, transmission, delivery and destruction; and

vii. Protect the secrecy of the ICT security measures from the general public.

(d) Separation

The task of creating, deleting, updating, modifying and verifying data needs to be separated in order to avoid unauthorized access as well as to protect ICT assets from errors, minor information leaks or manipulation. Separation also encompasses segregation between operations and network groups;

(e) Auditing

Auditing is the action of identifying incidents involving security or identifying situations that threaten security. It involves protection of all records related to security actions. Therefore, it must be ensured that ICT assets such as computers, servers, routers, firewalls and networks are capable of generating and storing security action logs or an audit trail;

(e) Compliance

The UM ICT Security Policy must be read, understood and obeyed to avoid any form of violation against it that could result in threats to ICT security;

(f) Recovery

System recovery is indispensable to ensure readiness and availability. The main objective is to minimize any disturbances or losses caused by unpreparedness. Recovery can be performed via backing-up and creation of a disaster/catastrophe recovery plan; and

(g) Mutual Dependency

All the above principles are interrelated and mutually dependent. Therefore, varying approaches, organizing and designing as many security mechanisms as possible is necessary to ensure maximum security.

ICT SECURITY RISK ASSESSMENT

UM must take into account the existence of risks to ICT assets due to the proliferation of threats and vulnerabilities today. Due to that, UM needs to take the appropriate proactive steps to evaluate the level of risk to ICT assets so that the most effective solutions and decisions as pertains to the protection and control over ICT assets can be identified.

UM must execute ongoing scheduled risk assessments relating to ICT security requirements and requirement changes, and subsequently take follow-up action and/or the appropriate measures to control and minimize the ICT security risks based on the risk assessment findings.

ICT security risk assessment must be performed on all UM information systems including applications, software, servers, networks and/or processes and procedures. This risk assessment must be performed on the premises where information technology resources are located including data centers, media storage rooms, utilities and other support systems.

UM is responsible in mitigating and managing ICT security risks in line with the requirements of the General Circular Number 6 Year 2005: Public Sector Information Risk Assessment Guidelines.

UM must identify the appropriate measures to mitigate the possibility of risks existing and take the following actions:

(a) Reduce risks by executing the appropriate control measures;
(b) Receive and/or be prepared to face risks that may occur while fulfilling criteria that have been set by management;
(c) Avoid and/or prevent risks that occur by taking preventative measures that avert and/or prevent the occurrence of risks; and
(d) Transfer the risk to other parties such as suppliers, consultants and others who have interests.

ARTICLE 01 DEVELOPMENT AND MAINTENANCE POLICY	
0101 ICT Security Policy	
Objective: To explain the direction and management support for information security in accordance with UM requirements and related legislative requirements.	
UM-010101 Policy Implementation	
Implementation of this policy will be carried out by the Vice Chancellor of UM assisted by the ICT Security Management Team consisting of the Deputy Vice-Chancellor (Development) as the Chief Information Officer (CIO), Director of Center for Information Technology cum ICT Security Officer (ICTSO), and all Heads of the CoR (Center of Responsibilities).	Vice Chancellor
UM-010102 Policy Dissemination and Use	
This policy is to be disseminated and is applicable to all users of UM ICT assets (including staff, students, vendors, consultants, etcetera…)	ICTSO

UM-010103 Policy Maintenance	
The UM ICT Security Policy is subject to revisions and amendments from time to time in line with changes in technology, applications and procedures of legal and social importance. The following is the procedure to be followed in relation to the maintenance of UM ICT Security Policy: (a) Identify and define the necessary amendments; (b) Submit the proposed amendments in writing to ICTSO for presentation and approval by the ICT Security Committee Meeting (ICTSC); (c) Changes are to be agreed upon by ICTSC and communicated to all users; and (d) This policy shall be reviewed at least once a year.	ICTSO
UM-010104 Policy Exemption	
The UM ICT Security Policy is applicable to all users of any UM ICT assets without exemption.	All

ARTICLE 02 ICT SECURITY ORGANIZATION	
0201 Internal Organizational Infrastructure	
Objective: To describe the roles and responsibilities of the individuals involved clearly and systematically to achieve the UM ICT Security Policy objectives.	
UM-020101 Vice Chancellor	
The Vice-Chancellor has roles and responsibilities in matters such as the following: (a) Ensure that all users understand the provisions under the UM ICT Security Policy; (b) Ensure that all users comply with the UM ICT Security Policy; (c) Ensure that all the needs of the organization (financial resources, human resources and safety protection) are sufficient; and (d) Ensure that risk assessment and implementation of ICT security program are implemented as in UM ICT Security Policy;	Vice Chancellor

UM-020102 Chief Information Officer (CIO)	
The UM Chief Information Officer (CIO) is the Deputy Vice-Chancellor (Development). The CIO's roles and responsibilities are as follows: (a) Assist the Vice Chancellor in the implementation of tasks involving ICT security; (b) Chair the UM ICT Security Committee Meeting (ICTSC). (c) Ensure ICT security requirements; (d) Coordinate and manage training plans and ICT security awareness programs such as the preparation of the UM ICT Security Policy and risk management and auditing, and (e) Responsible for matters related to ICT security UM.	CIO
UM-020103 Chief Technology Officer (CTO)/ ICT Manager	
Chief Technology Officer (CTO) cum ICT Manager for UM is the Director of the Center for Information Technology, UM. The CTO's roles and responsibilities are as follows: (a) Enforce the UM ICT Security Policy; (b) Review and implement ICT security controls in accordance with UM requirements;	CTO

(c) Determine the access controls for all users of UM ICT assets; (d) Ensure that the proper keeping of records, material evidence and the latest reports on UM ICT security threats is implemented. (e) Carry out his/her roles and responsibilities as the UMCERT Director; (f) Prepare the ICT Strategic Plan for Center for Information Technology which contains planning for ICT Usage in supporting achievement of the mission and vision of UM; (g) Streamlining and integrating "cross functional" processes between departments to deliver more efficient and effective services; (h) Develop, operate and manage systems and IT infrastructure that are intact and safe as well as based on modular features, "connectivity", "inter-operability" and "Portability"; (i) Protect the integrity of electronic data, promote the sharing of information and provide a method for dissemination of information electronically to legitimate users whether within or outside the agency; (j) Be a member of the ICT Council which formulates policy and reports directly to the Vice-Chancellor; and (k) Promote the effective use of IT and, in tandem, achieve the agency's strategic goals and acts as an agent and as a pioneer of change ("champion of change").	

UM-020104 ICT Security Officer (ICTSO)	
ICT Security Officer (ICTSO) for UM is the Head of ICT Security, Center for Information Technology, UM. Roles and responsibilities ICTSO appointed are as follows: (a) Plan and manage the overall UM ICT security programs; (b) Implement the UM ICT Security Policy; (c) Provide information and exposure on the UM ICT Security Policy UM to all users; (d) Report any matters or findings on ICT security to the ICT Manager; (e) Establish guidelines and procedures in line with the UM ICT Security Policy; (f) Implement risk management; (g) Perform the audit, review, formulate responses for university management and based on the findings and prepare a report as relevant; (h) Issue warnings to the UM campus community on the existence of dangerous threats such as viruses and offer advice and provide the appropriate protective measures;	ICTSO

(i) Carry out his/her roles and responsibilities as the Manager of the UMCERT Team; (j) Report on ICT security incidents to the UM Computer Emergency Response Team (CERT) and inform the ICT Manager and the CIO; (k) Cooperate with all relevant parties in identifying the source of threats or security incidents and certify ICT remedial measures immediately; (l) Formulate and implement awareness programs on ICT security; (m) Conduct assessments to ensure adequate ICT security levels and take remedial or strenghthening action to increase the level of ICT infrastructure security so that new incidents can be avoided.	

UM-020105 ICT System Administrator	
UM ICT Systems Administrators are all the Heads of Division in the Centre for Information Technology (PTM), UM. The roles and responsibilities of the ICT system administrators are as follows: (a) Take appropriate action immediately when notified of UM employees who resign, retire, transfer, take a long vacations or experience changes in job scopes; (b) Ensure the accuracy and completeness of access levels based on the instructions of the resource information owners as specified in the UM ICT Security Policy; (c) Monitor the daily access activities in system user applications; (d) Identify abnormal activities such as violation and modification of unauthorized data and cancel or stop the activities immediately; (e) Analyze and keep audit trail records; (f) Provide a report on access activities on a regular basis; and (g) Responsible for monitoring that ICT hardware distributed to users, such as personal computers, laptops, printers, scanners, etcetera are in good condition.	ICT System Administrator

UM-020106 Users	
Users have the following roles and responsibilities: (a) Read, understand and comply with UM ICT Security Policy; (b) Know and understand the impact of ICT security implications of its actions; (c) Undergo security vetting if required to deal with classified official information (d) Implement the principles of UM ICT Security Policy and maintain the confidentiality of information about UM; (e) Report any activity that threatens ICT security to ICTSO immediately; (f) Attend awareness programs on improving ICT security; and (g) Sign the Letter of Compliance on UM ICT Security Policy as in **Appendix 1**.	Users

(i) Non-permanent members are as follows:

- The two deans representing the science stream with their respective alternate member.
- The two deans representing the arts stream with their respective alternate member.
- Two staff: one representing the science stream and another representing the arts stream with their respective alternate members.

The secretariat for ICTSC UM is the secretariat of the ICT Council.

Jurisdiction:

(a) Recommend / approve UM ICT Security Policy (ICTSP) documents;

(b) Monitor the level of ICT security compliance;

(c) Certify guidelines and procedures for specific applications in conformity with the requirements of the UM ICTSP;

(d) Assessing and recommending appropriate technology solutions for ICT security requirements;

(e) Ensure that the UM ICTSP is in accordance with the ICT policies of the current government;

(f) Receive the report(s) and discuss matters relevant to the current state of ICT security;

(g) Discuss actions involving violation of the UM ICTSP; and

UM-020107 ICT Security Committee	
The ICT Security Committee (ICTSC) is the committee responsible for ICT security and serves as an advisor and catalyst in the development of plans and strategies for UM ICT security. At UM, the ICTSC role is played by ICT Council. UM ICTSC membership is similar to the composition of the ICT Council: (ii) Permanent Chairman: Chief Information Officer (CIO) (iii) Permanent Secretary: Director of PTM (iv) The permanent members are as follows: • Bursar • Registrar • Chief Librarian • Director of Institute of Research Management and Monitoring (IPPP) to represent the research field with the Dean of Institute of Graduate Studies as the alternate member.	UM ICTSC

(h) Decide what action should be taken for any incident that occurs.	
UM-020108 UM ICT Computer Emergency Response Team (UMCERT)	
UMCERT membership is as follows: Director : CTO Manager : ICTSO Members : (1) Information Technology Officer at ICT Security Section, PTM; (2) Assistant Information Technology Officer at ICT Security Section, PTM; (3) Representatives of all divisions in PTM;	

Roles and responsibilities of UMCERT are as follows:

(a) Receive and track complaints and assess the level of ICT security and types of incidents;

(b) Record and carry out preliminary investigations of incidents received;

(c) Take action on ICT security incidents reported;

(d) Handle responses to ICT security incidents and implement repairs;

(e) Advise the CoR (Center of Responsibilities) to take recovery and fortification action if the incident that occurred involves ICT assets that are under the responsibility of the CoR;

(f) Contact and report the incident to MAMPU GCERT;

(g) Prepare incident handling reports for ICT Security Committee;

(h) Provide advisory services to users in locating, identifying and handling of any ICT security incidents;

(i) Disseminate information to assist in the strengthening of ICT security in UM from time to time;

(j) Conduct assessments to ensure ICT security is adequate and take remedial or strengthening action to increase the level of ICT infrastructure security so that new incidents can be avoided; and (k) Increase knowledge and awareness of ICT security through ICT security awareness programs. Each user should be given ICT training and awareness programs in performing their duties and responsibilities.	

0202 Third Parties

Objective:

Ensure the safety of all ICT assets used by third parties (suppliers, Consultants and etcetera)

UM-020201 Requirements of Security Contracts with Third Parties

This is to ensure that the use of information and information processing facilities by third parties are controlled. Matters that need to be complied with are as follows: (a) Read, understand and comply with the UM ICT Security Policy; (b) Identify information security risks and information processing facilities and implement appropriate controls before granting access permissions; (c) Identify the security requirements before authorizing access or usage to third parties; (d) Access to ICT assets UM should be based on a contractual agreement; (e) Ensure that all security requirements are clearly specified in agreements with third parties. The following items should be included in the sealed agreement:	CIO, ICTSO, ICT Manager, ICT System Administrator and Third Parties

i. The UM ICT Security Policy; ii. Security Vetting; iii. Official Secrets Act 1972 Declaration; iv. Intellectual Property Rights; (f) Sign a Letter of Compliance with UM ICT Security Policy as in **Appendix 1**.	

ARTICLE 03 ASSET MANAGEMENT	
0301 Asset Accountability	
Objective: Ensure that all ICT assets are provided the appropriate control and protection by the owners or the respective trustees.	
UM-030101 ICT Asset Inventory	
This is to ensure that all ICT assets are given the appropriate control and protection by the owner or respective trustee. Matters that need to be complied with are as follows: (a) Ensure that all ICT assets are identified and asset information is recorded in the registered capital assets form and inventory is constantly updated; (b) Ensure that all ICT assets have owners and are operated by authorized users; (c) Ensure that all users confirm the placement of ICT assets placed at UM; (d) Rules for handling the assets should be identified, documented and implemented; and	System Administrators and All

(e) Each user is responsible for all ICT assets under his/her control.	
0302 Information Classification and Handling	
Objective: Ensure that all information or ICT assets are given the appropriate level of protection.	
UM-030201 Information Classification	
Information should be classified or labeled by an authorized officer in accordance with Security Instructions document. All classified information must have a security level as specified in the Security Instructions document which are as follows; (a) Top Secret; (b) Secret; (c) Confidential; or (d) Limited.	Office of the Registrar, the Bursar's Office and All CoR

UM-030202 Information Handling	
Information handling activities such as collecting, processing, storing, transmitting, delivering, changing and destroying shall take into account the following security measures: (a) Prevent the disclosure of information to unauthorized parties; (b) Examine the information and determine it is accurate and complete from time to time; (c) Ensure that the information is ready for use; (d) Protect the confidentiality of passwords; (e) Comply with the standards, procedures, guidelines and safety measures prescribed; (f) Pay attention to classified information, especially during creation, processing, storage, transmission, delivery, transfer and destruction; and (g) Maintain the confidentiality of ICT security measures from public knowledge.	All

ARTICLE 04 HUMAN RESOURCE SECURITY	
0401 Human Resource Security in Daily Tasks	
Objectives: Ensure that all human resources involved, including employees, suppliers, consultants and other parties involved understand their responsibilities and their role in the security of ICT assets.	
UM-040101 Prior to Service	
Matters that need to be complied with are as follows: (a) Stated fully and clearly the roles and responsibilities of officers and UM staff and third parties involved in ensuring the security of ICT assets before, during and after the service; (b) To carry out security vetting for officers and UM staff and third parties involved based on legislative requirements, rules and etiquette applies in accordance with the requirements of the service, level of information that will be achieved, and the expected risk; and (c) Comply with all terms and conditions of the services offered and current regulations which came into effect based on the agreement that has been set.	All

UM-040102 During Service	
Matters that need to be complied with are as follows: (a) Ensure that officers and employees of UM and interested third parties manage the security of ICT asset based on the legislation and regulations set by UM; (b) Ensure the awareness training related to the ICT assets security management given to UM ICT users on an ongoing basis to perform their duties and responsibilities, and possibly it should be given to interested third parties from time to time; (c) Ensure the disciplinary process and / or by-laws of the officers and staff of the UM and interested third parties in the event of a collision with the laws and regulations set by the UM; and (d) To enhance the knowledge related to the application of ICT so that every ICT facilities are used in the right ways and means to ensure the importance of ICT security. Any courses and technical training required, the user can refer to the Human Resources Division of, UM.	All

UM-040103 Change or End of Service	
Matters that need to be complied with are as follows: (a) Ensure that all ICT assets are returned to UM in accordance with the rules and / or terms of service set; and (b) Removal or withdrawal of all the access permissions for the information and facilities of the information processing in accordance with the regulations set by UM and / or terms of service.	All

ARTICLE 05 PHYSICAL AND ENVIRONMENTAL SECURITY	
0501 Area Security	
Objective: Protecting premises and information from any form of aggression, threat, damage and unauthorized access.	
UM-050101 Areas of Control	
This is to prevent unauthorized access, damage and physical interference to the premises and university information. Matters that need to be complied with are as follows: (a) The area of physical security should be clearly identified. Location and the strength of physical security must rely on the need to protect assets and revenue risk assessment; (b) Using the security perimeter (barriers such as walls, fences control, security guards) to protect the area containing information and information processing facilities; (c) Install an alarm or camera; (d) Limiting the road access; (e) To provide counter control;	Director of Security Office, JPPHB, CIO dan ICTSO/

(f) Provide a safe or a special room for visitors; (g) Establish a Security Control Services; (h) Protect the limited area by appropriate entry controls to ensure that only authorized personnel can pass through this gateway; (i) Design and implement physical security in the office, room and facilities; (j) Design and implement physical protection from fire, flood, explosion, chaos and disaster; (k) Provide guidelines for staff working in restricted areas; and (l) Ensure the delivery and loading areas and also other places are controlled from the unauthorized entering.	
UM-050102 Physical Entry Control	
Matters that need to be complied with are as follows: (a) Each user at UM should wear or impose security pass during the hours of duty; (b) All security pass must be handed back to the university when the user resigns or retires;	All

(c) All visitors must register and get the Visitors Security Pass at the UM entrance gate or at the visited place and must be returned after the visit; and (d) Loss of visit pass must be immediately reported;	All
UM-050103 Prohibited Areas	
Restricted area is defined as an area where entry is restricted to certain officers only. Is implemented to protect ICT asset available in the area. Protected area in UM is Vice-Chancellor room, the rooms of the Deputy Vice-Chancellor, data center and network room. (a) Access to restricted areas is limited to only authorized officers; and (b) All third parties are prohibited from entering restricted areas except in certain cases such as when providing support services or technical assistance, and they must be accompanied at all times until the task is completed in the area.	System Administrators

0502 Equipment Security	
Objective: Protect UM ICT equipment from loss, damage, theft as well as interference with that equipment.	
UM-050201 ICT Equipment	
Matters that need to be complied with are as follows: (a) Users should check and ensure that all ICT equipment under their control functions properly; (b) Users are solely responsible for their own computers and are not allowed to make any changes in hardware and configurations that have been set; (c) Users are strictly forbidden to add, disassemble or replace any specified ICT hardware; (d) Users shall not make any additional software installation without permission from ICT System Administrator; (e) Users are responsible for damage or loss of ICT equipment under their control; (f) Users must ensure that the antivirus software in their personal computers is always activated and updated as well as perform scans on the storage media used;	All

(g) Usage of passwords to access to the computer system is required; (h) All support ICT equipment must be protected from theft, damage, abuse or unauthorized modifications; (i) The critical equipment must be supported by the uninterruptable Power Supply (UPS); (j) All ICT equipment shall be stored or placed in an organized, clean location with security features. Networking equipment such as switches, hubs, routers, etc. should be placed inside the special racks and locked; (k) All constantly used equipment must be placed in an area with appropriate temperature control; air-conditioned and ventilated); (l) The ICT equipment to be taken out from UM premises must be approved by an ICT Systems Administrator and be recorded for monitoring purposes; (m) The loss of ICT equipment should be immediately reported to ICTSO and Assets Officer; (n) The Handling of ICT equipment shall comply with and refer to the current enforcement regulations; (o) Users are not allowed to move the computer from its original location without the permission the ICT System Administrator;	All

(p) Any damages of the ICT equipment must be reported to the ICT System Administrator to be repaired; (q) Any stickers other than those intended for official purposes are not allowed. This is to ensure that equipment remains in pristine condition; (r) IP address configuration is not allowed to be modified from the original IP address; (s) Users are strictly forbidden from changing administrator password set by the ICT systems Administrator; (t) Users are responsible for the hardware, software and information under their supervision and these shall be used for the official work only; (u) The user shall ensure that all computer hardware, printers and scanners are switched "OFF" when leaving the office; (v) Any form of fraud or misuse of the ICT equipment shall be reported to ICTSO; and (w) Ensure that the plug is disconnected from the main switch (main switch) to prevent hardware breakdown before leaving the office in the event such as thunder, lightning and so on.	

UM-050202 Storage Media	
Storage media is any form of electronic equipment that is used to store data and information such as diskettes, compact discs, magnetic tapes, optical disks, flash drives, CD ROMs and other storage media. Storage media should be ensured to be in good condition, safe, with confidentiality guaranteed, integrity and availability for use. Matters that need to be complied with are as follows: (a) The storage media should be kept in an appropriate storage space with the relevant security features in accordance with its informational content; (b) Entry access to the media storage areas shall be limited to authorized users only; (c) All storage media must be controlled to prevent unauthorized access, theft, and destruction; (d) All storage media containing critical data must be stored in a safe with security features including resistance to break-downs, fire, water and magnetic fields; (e) Access and movement of the storage media should be recorded;	All

(f) The backup hardware should be site controlled; (g) To provide a copy or replication (backup) on a second storage media for the security purposes and to prevent loss of data; (h) All storage media to be retired must be destroyed properly and securely. (i) Approval from the owner must be obtained prior to the deletion of information or media content.	
UM-050203 Digital Signature Media	
Matters that need to be complied with are as follows: (a) The user shall be solely responsible for the media digital signatures to protect against theft, loss, damage, abuse and replication; (b) Media cannot be transferred or loaned; and (c) Any incidents of media loss incurred should be immediately reported to ICTSO for further action.	All

UM-050204 Software Media and Applications	
Matters that need to be complied with are as follows: (a) Only certified software is approved for use at UM; (b) UM in-house applications is not allowed to be demonstrated or distributed to other parties except with the consent of the ICT Manager; (c) Software Licenses (registration code, serials, CD keys) must be kept separate from the CD-ROM, disk or related media to prevent from the occurrence of theft or piracy; and (d) System source code should be stored properly and any modifications must be in accordance with established procedures.	All
UM-050205 Hardware Maintenance	
Hardware must be properly maintained to ensure its availability, confidentiality and integrity. Matters that need to be complied with are as follows: (a) All hardware must be maintained according to specifications set by the manufacturer; (b) Ensure that the hardware will only be maintained by authorized personnel or parties only;	Property Management Division (JPPHB) & PTM

(c) Responsible for all hardware as pertains to hardware maintenance either within the warranty period or after the expiry date; (d) Examine and test all the hardware before and after the maintenance process; (e) Inform the user before performing the maintenance according to the preordained schedule or according to requirements; and (f) All the maintenance activities of ICT assets must be with approval from the ICT Manager.	
UM-050206 The Equipment Outside Premises	
The hardware taken out of the premises of UM is exposed to various risks. Matters that need to be complied with are as follows: (a) Equipment should be guarded and protected at all times; and (b) Storage or placement of equipment should consider the appropriate security features.	All

UM-050207 Hardware Disposal	
Disposal involving all damaged ICT equipment, obsolete and cannot be repaired either capital assets or inventory supplied by UM and located in UM. ICT equipment must be disposed of through the current disposal procedures. Disposal should be done in a controlled and comprehensive manner to ensure that information is not lost from UM controls. Matters that need to be complied with are as follows: (a) All the content of equipment especially the official secret information shall be eliminated prior to disposal either by shredding, grinding, degaussing or burning; (b) If the information required to be kept, then the user can make a back-up copy; (c) The data in the storage of ICT equipment to be disposed of before-transferable must be ensured as written off in a safe manner; (d) Assets Officer shall identify whether certain equipment can be disposed or otherwise; (e) Equipment to be disposed shall be kept at the place designated with security features to ensure the safety of the equipment;	All, Division of Property Management and PTM

(f) The asset officer is responsible for recording the disposal details and update the disposal records of ICT equipment in the Integrated Property Management System;

(g) Disposal of ICT equipment is to be done centrally and in accordance with the current disposal procedures that are in effect; and

(h) The ICT user is STRICTLY PROHIBITED from doing the following:

i. Retain any of ICT equipment to be disposed for personal ownership;

ii. Disconnect, dismantle and store additional CPU internal devices such as RAM, hard-disk, motherboard and so forth;

iii. Store or transfer external computer hardware such as AVR, speakers and any related equipment to any part of UM;

iv. Moving any hardware that is to be disposed out of UM;

v. Self-disposing the ICT equipment because the duty of disposal is the responsibility and jurisdiction of UM; and

vi. The ICT users are nonetheless responsible to ensure all private and confidential information in the computer are copied into the secondary storage media such as floppy disks or flash drives before deleting information from computer equipment which is supposed to be disposed of.

0503 Environmental Safety	
Objective: Prevent UM ICT assets from any form of environmental threat caused by natural disasters, errors, negligence or accident.	
UM-050301 Environmental Control	
To avoid damages and disruption to the premises and the ICT assets, all proposals related to the premises whether to acquire, rent, renovate or purchasing should be consulted first to JPPHB and Security Office. To ensure the safety of the environment, the following items shall be observed: (a) Thoroughly plan and prepare an overall layout plan of the data center including printing space, computer equipment space, office layout space and etcetera; (b) All office spaces particularly areas with the ICT facilities should be equipped with adequate and authorized security protection such as firefighting and emergency exits; (c) Protective equipment should be installed in the right places, easily recognized and handled; (d) Flammable materials should be stored outside keeping space for supporting facilities of ICT asset;	PTM, JPPHB, Security Office and All

(e) All liquid substances shall be placed in the right location and distance from the ICT asset; (f) Users are prohibited from smoking or using cooking utensils such as electric kettles near the computer equipment; (g) All protective equipment must be checked and tested at least two (2) times a year. Activities involved in and the results of this test should be recorded for ease of reference and action if necessary; and (h) Access to the riser vessel must always be locked.	
UM-050302 Power Supply	
The power supply is the source of electrical power supplied to the ICT equipment. Matters that need to be complied with are as follows: (a) All ICT equipment should be protected from power failures and appropriate power supplies should be channeled to the ICT equipment; (b) Equipment support such as Uninterruptable Power Supply (UPS) and generator can be used for critical services such as data center and network room to get constant power supply; and (c) All power supply supporting equipment must be checked and tested regularly.	PTM, JPPHB and ICTSO

UM-050303 Cables	
Computer cables must be protected as it could lead to the exposure of information. The security measures that should be taken are as follows: (a) Using cables in accordance with the defined specifications; (b) To protect the cables from intentional or unintentional damage; (c) Protect the cable installation route completely to avoid the threat of damage and wiretapping; and (d) All cables should be clearly labeled and must be through trunking to ensure the safety of cable from damage and information interception.	PTM and ICTSO
UM-050304 Emergency Procedures	
Matters that need to be complied with are as follows: (a) Each user must read, understand and comply with emergency procedures with reference to UM Safety Guidelines; and (b) Emergency of environment such as fire as must be reported to the Security Officer of UM;	All and UM Security Officers

0504 Document Security	
Objective: To protect UM information from any form of environmental threats caused by any form of natural disasters, accidents or negligence.	
UM-050401 Documents	
Matters that need to be complied with are as follows: (a) Each document shall be filed and labeled in accordance with safety/security classification such as Open, Restricted, Confidential, Secret or Top Secret; (b) Movement of files and documents should be recorded and must follow safety procedures; (c) Loss and damage of all types of documents need to be notified in accordance with safety instructions procedure; (d) Disposal of documents should be performed in accordance with current safety procedures such as safety instructions, Practice Direction (Records Disposal Schedule) and the procedures of the National Archives; and (e) Using encryption on the official secret documents prepared and transmitted electronically.	All

ARTICLE 06 OPERATIONS MANAGEMENT AND COMMUNICATIONS	
0601 Operating Procedure Management	
Objective: Ensure proper functioning of operational management and safe from threats and harassment.	
UM-060101 Conduct of Procedures	
Matters that need to be complied with are as follows: (a) All established, operational management procedures that have been identified and still apply shall be documented, stored and controlled; (b) Each procedure must include clear instructions, be well-organized and complete as pertains to capacity requirements, handling and processing of information, error handling and shipping, handling output, technical assistance and recovery in the event the processing disrupted or stopped; and (c) All procedures should be updated from time to time or as required.	All
UM-060102 Change Management	
Matters that need to be complied with are as follows:	All

(a) Modification involving hardware, systems for information processing, software, and procedures may only be performed with permission from superiors or the ICT asset owners; (b) Activities such as installing, maintaining, removing and updating any ICT system components shall be conducted by authorized and knowledgeable officers or those directly involved with the ICT asset; (c) All activities on ICT system component modification shall comply with the change specifications set; and (d) All modification or change activities should be recorded and controlled in order to avoid errors whether or not intentional.	
UM-060103 Segregation of Duties and Responsibilities	
Matters that need to be complied with are as follows: (a) Scope of duties and responsibilities need to be separated to reduce the chances of abuse or an unauthorized modification of ICT assets; (b) The tasks of creating, deleting, updating, modifying and validating data should be segregated to prevent unauthorized access and to protect ICT assets from errors, classified information leaks or manipulation; and	ICT manager and ICTSO

(c) The hardware used for developing, updating, maintaining and testing applications shall be separated from the hardware used in production. Segregation also includes segregation of operational groups and networks.	
0602 Third Party Management Delivery Services	
Objective: Ensure the implementation and maintenance of information security levels and appropriate service delivery in accordance with service agreements with third parties.	
UM-060201 Delivery Service	
Matters that need to be complied with are as follows: (a) Ensure the security, service terms and delivery levels contained in the agreement are complied with, implemented and maintained by third parties; (b) Services, reports and records provided by third parties need to be constantly monitored, reviewed and audited from time to time; and (c) Management of changes in policy must take into account the critical level of the system and the processes involved as well as the reassessment of risks.	ICT System Administrator, ICTSO, Computer Manager

0603 Planning and System Acceptance	
Objective: Minimize the risk of causing disruption or failure of the system.	
UM-060301 Capacity Planning	
Matters that need to be complied with are as follows: (a) The capacity of a component or ICT system should be planned, managed and monitored closely by the relevant officers to ensure that requirements are adequate and appropriate to the development and use of ICT systems in the future; and (b) The requirements of this capacity should also consider ICT security features to minimize the risk of such disruptions and loss of service due to unplanned modification.	ICT System Administrator, ICTSO, Computer Manager
UM-060302 System Acceptance	
Matters that need to be complied with are as follows: (a) All new systems (including systems updated or modified) shall meet the criteria before being accepted or agreed. (b) Perform proper testing on the new system during development and prior to acceptance of the system.	ICT System Administrator, ICTSO

0604 Hazardous Software	
Objective: Protecting the integrity of software and information from disclosure or damage caused by malicious software such as viruses, trojans and the like.	
UM-060401 Protection from Hazardous Software	
Matters that need to be complied with are as follows: (a) Install security systems to detect software or hazardous programs, such as antivirus, Intrusion Detection System (IDS) , Intrusion Prevention System (IPS) and follow the correct procedures and safe use; (b) Install and use only genuine software, registered and protected under any enforcement written law; (c) Scan all software or systems with antivirus software before use; (d) Keep antivirus programs updated with the latest virus definitions; (e) Review system files or information periodically to detect unwanted activities such as loss and damage information; (f) Attend awareness sessions about hazardous software threats and how to manage them;	All

(g) Submission of liability clause for any contract that was offered to the software provider. The purpose of this clause aims for software maintenance claim if the software contains malicious programs; (h) To establish programs and quality assurance procedures for all developed software; and (i) Provide warnings regarding ICT security threats such as virus attacks.	
UM-060402 Mobile Code Protection	
Matters that need to be complied with are as follows: (a) The use of mobile code, which can threaten ICT security, is not allowed.	All
0605 Housekeeping	
Objective: Protecting the integrity of the information so that it can be accessed at any time.	
UM-060501 Back-up	
To ensure that the system can be rebuilt after a disaster, back-up copies must be created each time configurations change. The back-up copies shall be catalogued and stored off site. Matters that need to be complied with are as follows:	All

(a) Make a security back-up of all software systems and applications at least once or after obtaining the latest version; (b) Backup all data and information in accordance with operational needs. The back-up frequency depends on a criticality level of the information concerned; (c) Testing the back-up system and restore existing procedures periodically to ensure that it can function properly, reliably and effectively when used particularly in case of emergency; (d) Store at least three (3) generations of back-ups; and (e) Record and store the back-up copies are various secure locations.	
0606 Network Management	
Objective: Protect the information in the network and supporting infrastructure.	
UM-060601 Network Infrastructure Control	
Network infrastructure must be controlled and managed as well as possible to protect against threats to systems and applications across the network. Matters that need to be complied with are as follows:	Computer Manager, ICT System Administrator

(a) The responsibilities or the network operations and computer tasking should be segregated to minimize unauthorized access and modification;

(b) Network equipment shall be placed in a location having strong physical characteristics and free from hazards such as flooding, vibration and dust;

(c) Access to the network equipment should be controlled and restricted to authorized users only;

(d) All equipment must go through the process of a Factory Acceptance Check (FAC) during installation and configuration;

(e) A firewall should be installed between the internal network and systems involving university official's confidential information and should be configured and monitored by ICT Systems Administrator;

(f) All incoming and outgoing traffic through the firewall should be under the control of UM;

(g) All sniffer or network analyzer software is prohibited to be installed on the user's computer unless approved by ICTSO;

(h) Install Intrusion Detection System (IDS) software or Intrusion Prevention System (IPS) to detect any hack attempts and other activities that may threaten the UM system and information;

(i) Install Web Content Filtering on an Internet Gateway to restrict prohibited activities;

(j) Any network connection which is not under the control of UM is not allowed; (k) All users are allowed to use only UM networks. The use of modems is strictly prohibited; and (l) Facilities for wireless LAN need assurances on security control.	
0607 Media Management	
Objective: Protecting ICT assets from any disclosure, modification, removal or destruction and disruption of service activities.	
UM-060701 Delivery and Transfer	
Delivery or moving the media out of the office can only be performed with the approval from the Head of Department in advance.	All
UM-060702 Media Handling Procedures	
Media handling procedures to be followed are as follows: (a) Labeling all media according to the sensitivity of the information; (b) Limit and determine the access of media to authorized users only; (c) Limit the distribution of data or media to permitted purposes;	All

(d) Control and record the media maintenance activities to avoid any damages and unauthorized disclosure; (e) Store all media in safe locations; and (f) The media containing classified information to be deleted or destroyed must be disposed using the right and safe procedure.	All
UM-060703 System Documentation Security	
The matters that must be observed in ensuring the security of system documentation is as follows: (a) Ensure that the documentation storage system has security features; (b) Provide and enhance the security of the documentation system; and (c) Control and record all activities of access to existing documentation systems.	ICT System Administrator, ICTSO

0608 Information Exchange Management	
Objective: Ensuring the security of information and software exchange between UM and external agencies is guaranteed.	
UM-060801 Information Exchange	
Matters that need to be complied with are as follows: (a) Policies, procedures and controls of the formal exchange of information should be established to protect the exchange of information through the use of various types of communication facilities; (b) The agreement must be established for the exchange of information and software between UM and external agencies; (c) Media containing information should be protected from unauthorized access, misuse or damage during transfer out of UM; and (d) The information contained in the electronic mail should be well-protected.	All
UM-060802 Electronic Mail Management (E-mail)	
The use of e-mail at UM should be continuously monitored by E-mail Administrator to meet the ethical requirements of e-mail and the Internet which is written in the Development Administration Circular No. 1 of 2003 entitled	All

"Guidelines on the Procedure for Use of the Internet and Electronic Mail in agency-Government agencies "and any written law by which it comes into effect. Matters that need to be adhered to in handling electronic mail is as follows: (a) Only Accounts or electronic mail (e-mail) provided by UM can be used. The use of other individuals'' accounts or shared accounts is prohibited; (b) Each e-mail provided shall comply with the format specified by the UM; (c) Ensure that the subject and e-mail content is relevant and refers to the same subject matter being discussed before sending; (d) The delivery of official e-mail should use official e-mail account and ensure the e-mail address of the recipient is correct; (e) Users are advised to use attachments, if necessary, not exceeding ten megabytes (10MB) when sending email. File compression is recommended in order to reduce the size; (f) Users should avoid opening e-mail from an unknown or doubtful sender; (g) Users shall identify and verify the identity of person with whom they are communicating before proceeding to transmit information via e-mail;	All

(h) Each official e-mail sent or received shall be kept based on specified electronic file system management procedures; (i) An unimportant E-mail without archival value upon which action has been taken and no longer is needed can be removed; (j) Users shall ensure that the date and time of the computer system is accurate; (k) To take action and respond to e-mails quickly and take immediate action; (l) Users shall ensure that personal e-mail addresses (like yahoo.com, gmail.com, streamyx.com.my etc.) will not be used for official purposes; and (m) Users shall be responsible for updating and utilizing their own mailbox.	
0609 Electronic Commerce Services	
Objective: Control the sensitivity of the information and applications in service so that any risks such as misuse of information, information theft and unauthorized amendments are prevented.	
UM-060901 E-Commerce	

To encourage the growth of e-commerce as well as supporting the government's desire to popularize electronic service delivery, users should use the Internet. Matters that need to be complied with are as follows: (a) Information to be involved in e-commerce should be protected from fraudulent activity, contract dispute and disclosure as well as unauthorized modification; (b) The information involved in online transactions should be protected to prevent incomplete transmission, wrong destination, modification, disclosure, duplication or repetition of unauthorized messages; and (c) The integrity of information provided to the system that can be accessed by the public or other interested parties should be protected to prevent from any unapproved amendment.	All
UM-060902 General Information	
The matters that need to be observed to ensure the security of information is as follows: (a) Ensure the software, data and information are protected with an appropriate mechanism; (b) Ensure that the systems that are accessible to the public are tested beforehand; and (c) Ensure that all information to be displayed has been endorsed and approved before uploading to websites.	All

0610 Monitoring	
Objective: Ensure detection of unauthorized information processing.	
UM-061001 Auditing and ICT Forensics	
ICTSO must be responsible for recording and analyzing the following: (a) Any intrusion attempts into UM ICT systems; (b) Malicious code attacks, denial of service, spam, forgery (forgery, phishing), intrusion, threats and physical loss; (c) Modification of hardware features, software or any of the system components without the knowledge, direction or consent of any parties; (d) Activities for surfing, keeping or distribute obscene material, defamatory and propaganda; (e) Activities involving the establishment of unauthorized services; (f) The installation and utilization of software which burdens bandwidth of the network; (g) E-mail abuse activities; and (h) Unauthorized IP address conversion activities of other than as provided for by ICT System Administrators.	ICTSO

UM-061002 Audit Trail	
Every system must have an audit trail (audit trail). An audit trail records the activities that occur chronologically in the system to allow for screening and reconstruction in the event of any rearrangement or changes to the system. Audit trail shall contain the following information: (a) A record of every transaction; (b) The audit trail information contains the user's identity, the sources used, change information, dates and times of activities, networks and applications used; (c) The user access activity to the ICT system is either valid or otherwise; and (d) Details of abnormal system activity or activity that does not have security features. Audit trail must be kept for a period of time as proposed by Instruction of Information Technology and the National Archives Act. ICT Systems Administrator shall review the audit trail notes from time to time and to prepare a report if necessary. This will help to detect prior abnormal activity. Audit trails should also be protected from damage, loss, deletion, forgery and unauthorized modifications.	ICT Administrator

UM-061003 Log System	
ICT Systems Administrators shall perform the following: (a) Establish log system to record all daily activities of users; (b) Review the system log periodically to detect errors which may cause disruptions to the system and take immediate action to rectify those errors; and (c) In the event of other invalid activities such as information theft and hacking, ICT System Administrators shall report these events to ICTSO and CIO.	ICT System Administrator
UM-061004 Log Monitoring	
Matters that need to be complied with are as follows: (a) Audit Log which records all activities should be prepared and kept for an agreed period of time in order to assist in investigations and access control monitoring; (b) Procedures for monitoring use of information processing facilities should be established and the results should be monitored regularly; (c) The facilities for recording and log information should be protected from any modified and unauthorized access; (d) The administrative activities and system operations need to be recorded;	ICT Safety Section, PTM dan ICT System Administrators

(e) Fault, error and / or abuse must be recorded in logs, analyzed and appropriate action taken; and (f) The time related to information system processing in UM or the security domain should be consistent with an agreed point of time.	

ARTICLE 07

ACCESS CONTROL

0701 Access Control Policy

Objective:

Control access to information.

UM-070101 Access Control Requirements

Access to processes and information shall be controlled in accordance to security requirements and different job functions of users. It shall be recorded, updated and support existing user access control policies. Access control rules must be established, documented and reviewed based on the requirements of the services and security. Matters that need to be complied with are as follows: (a) Control access to ICT assets in accordance with the security requirements and the role of the user; (b) Control access to internal and external network services; (c) Security of information obtained using the facility or mobile devices; and (d) Control of information processing facilities.	PTM and ICTSO

0702 User Access Management	
Objective: Control user access to UM ICT assets.	
UM-070201 User Accounts	
Each user is responsible for the use of ICT systems. To identify users and their activities, the following shall be observed: (a) Only the account provided by UM can be used; (b) A user account must be unique and should reflect the user's identity; (c) A user account created for the first time will be given a minimum level of access which is to view and read only. Any change in the level of access shall obtain approval from the ICT system owner; (d) Ownership of a user account is not an absolute right and is subject to UM rules. Account may be withdrawn if the usage is found breaking the rules; (e) The use of another person's account or account that is shared is prohibited; and (f) ICT System Administrator can freeze and terminate the user's account on the following reasons:	All and ICT System Administrators

i. Users who are on long vacation during the time period exceeding two (2) weeks; ii. Change of job function assignments; iii. Switch to other agencies; iv. Retired; or v. Termination of employment.	
UM-070202 Access Rights	
Setting up and the usage of access rights must be given a strict control and supervision based on the scope of the task.	ICT System Administrators
UM-070203 Password Management	
Selection, use and management of passwords as the main gateway to access information and data in the system must comply with the best practices and procedures set by UM as follows: (a) In any situation, and the reasons, the password should be protected and cannot be shared with anyone else; (b) The user must change the password when the password is suspected leakage or compromised; (c) Length of the password must be at least twelve (12) characters with a combination of alphanumeric, numbers and special characters; (d) Passwords should be remembered and CANNOT be written, stored or disclosed in any way;	All and ICT System Administrators

(e) Windows password and screen saver shall be enabled especially on computers that are located in a share working area; (f) Passwords shall not be displayed during input, reports or other media and shall not be coded; (g) Enforce password change at the first logon or after login for the first time or after a password reset; (h) The password must be different from the user identification; (i) Set time limit for verification for two (2) minutes (according to the suitability of the system) and after the limit, the session is terminated; (j) Passwords shall be changed after 90 days or after an appropriate period of time; and (k) Avoid the use of a recently used password.	
UM-070204 Clear Desk and Clear Screen	
All information in any media form shall be stored properly and securely to avoid damage, theft or loss. Clear Desk and Clear Screen means not leaving sensitive materials exposed either on the table or on the display screen when users are not in place.	All

Matters that need to be complied with are as follows: (a) Utilize a screen saver password or logout when leaving the computer; (b) Keep sensitive materials in a drawer or a locked file cabinet; and (c) Ensure that all documents are taken immediately from the printer, scanner, fax machine and photocopier.	
0703 Network Access Control	
Objective: Prevent unauthorized access and unauthorized use of network services.	
UM-070301 Network Control	
Access controls to networked services shall be secured by: (a) Placing or installing the appropriate interface between UM network, network of other agencies and the public network; (b) Establish and enforce a mechanism for user authentication and the use of appropriate equipment that meet the suitability; and (c) Monitor and enforce user access control on the ICT network services.	ICT System Administrators and ICTSO

UM-070302 Internet Access	
Matters that need to be complied with are as follows: (a) The Internet usage at UM shall be continuously monitored by the Network Administrator to ensure its use for authorized purposes only. Prudence, indeed, will protect from malicious code, viruses, and substances that are not supposed to be in the UM network; (b) Content Filtering method shall be used to control the Internet access according to job functions and monitoring of compliance; (c) The use of packet shaper technology to regulate activity such as video conferencing, video streaming, chat and downloading is required to manage the use of bandwidth maximally and effectively; (d) Internet is for official use only. ICT Manager reserves the right to determine who can use the Internet or otherwise; (e) The website accessed must be related to job functions and limited to purposes that are permitted by the CIO / authorized officer; (f) The material obtained from the Internet shall be determined accuracy and authenticity. As a best practice, the Internet resources referred shall be specified;	Network Administrators ICT Managers All

(g) Official materials must be reviewed and validated by the Head of Division before being uploaded to the Internet; (h) The user shall download authorized material only such as registered software and protected under copyright; (i) Any material downloaded from the Internet shall be used for purposes permitted by UM; (j) Only officers who have permission are allowed to use public discussion as newsgroups and bulletin board. However, the content of public discussion shall obtain prior approval from the CIO subject to the policies and rules that have been set; (k) The use of modem for connection to the Internet is not allowed; and (l) The user is forbidden from performing the following activities: i. Upload, download, store and use unlicensed software and other applications such as electronic games, videos, songs that can affect the performance of Internet access; and ii. Prepare, upload, download and store texts, speeches or materials containing pornographic elements.	

0704 Operating System Access Control	
Objective: Prevent unauthorized access and unauthorized use of operating system.	
UM-070401 Operating System Access	
Operating system access controls are necessary to prevent any unauthorized access. Security features in the operating system shall be used to prevent access to the computer system resources. This feature is also necessary to: (a) Identify the identity, terminal or location for each user that is allowed; and (b) Record of successful and failed access. The methods used must be able to support the following criteria: (a) Verify that the user is authorized; (b) Establishing an audit trail of all users accessing the operating system, particularly with super user privilege; and (c) Generate a warning (alert) in the event of a security breach. Matters that need to be complied with are as follows: (a) To control access to the operating system using a secure logon procedure;	ICT System Administrators and ICTSO

(b) Establish an identification (ID) that is unique to each user and is used by the specific user only; (c) Limiting and controlling the use of the program; and (d) Limiting the connection period to a high-risk applications.	
UM-070402 Smart Cards	
Matters that need to be complied with are as follows: (a) Smart Cards shall be used to access the electronic system or access to designated areas; (b) Smart cards shall be kept in a safe place to prevent theft or use by any other unauthorized party; (c) Sharing of smart cards for any access is not allowed. Misuse smart card will be blocked; and (d) Any loss, damage and misuse attempts shall be reported to the Security Office, UM.	All

0705 Application and Information Access Control	
Objective: Prevent unauthorized access and unauthorized use of information contained in system applications.	
UM-070501 Application and Information Access	
Intended to protect system applications and existing information from any form of unauthorized access that can cause damage. To ensure that the access control of systems and applications are strong, the following shall be observed: (a) User shall only use information systems and applications that are permitted to them in accordance to access level and security of information that has been determined; (b) Each activity accessing information systems and user applications must be recorded (log system); (c) Restrict access to system and application to three (3) attempts only. If failed, the user's password or account shall be blocked; (d) Ensure control to network system is strong and complete with security features to prevent the unauthorized activity or access; and (e) Access to information systems and applications from remote distance is recommended. However, its use is restricted to authorized services only.	ICT System Administrator and ICTSO

0706 Mobile Devices and Teleworking	
Objective: Ensure information security while using mobile devices and teleworking facilities.	
UM-070601 Mobile Devices	
Matters that need to be complied with are as follows: (a) Record the use of mobile computing devices activity in and out to detect the loss or damage; and (b) A mobile computer must be stored and locked in a safe place when not in use.	All
UM-070602 Teleworking	
Matters that need to be complied with are as follows: (a) Protective action shall be taken to prevent the loss of equipment, information disclosure, unauthorized access and misuse of facilities.	All

ARTICLE 08

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

0801 Security in Developing Systems and Applications

Objective:

Ensure that the system either developed in-house or by third party has the characteristics of an appropriate ICT security.

UM-080101 Information System Security Requirements

Matters that need to be complied with are as follows: (a) The acquisition, development, improvement and maintenance of the system shall take account of security control to ensure that the system is free from error that can interfere with the processing and accuracy of information; (b) Security testing shall be conducted on system input to verify for authentication and integrity of data entered, on system processing to determine whether the program is running correctly and properly and; on system output to ensure that the data processed is accurate; (c) The application must contain verification check (validation) to prevent any damage due to information processing faulty or intentional conduct; and (d) All systems either developed in-house or otherwise must be tested in advance to ensure the system meets the expected security requirements before use.	System Owners, ICT System Administrators and ICTSO

UM-080102 Data Input and Output Validation	
Matters that need to be complied with are as follows: (a) Data input for the application must be verified to ensure that the data was entered correctly and appropriately; and (b) Data output from an application must be verified to ensure that the information produced is accurate.	System Owners and ICT System Administrators
0802 Cryptography Control	
Objective: Protect confidentiality, integrity and authenticity of the information through cryptographic controls.	
UM-080201 Encryption	
Users shall encrypt sensitive information or official secret information at all times.	All
UM-080202 Digital Signatures	
Use of digital signatures is required for all users, especially those who manage the transaction of official secret information electronically.	All
UM-080203 Public Key Infrastructure (PKI)	
Management of PKI must be done effectively and securely to protect the keys from being altered, destroyed and exposed during the validity period of the key.	All

0803 System File Security	
Objective: Ensure that system files are controlled and handled safely and securely.	
UM-080301 System File Controls	
Matters that need to be complied with are as follows: (a) Updates to the system files can only be done by the ICT system administrator or authorized officer in accordance with the prescribed procedures; (b) Source code or system programs that have been updated can only be implemented or applied after doing a proper test; (c) Control access to the source code or program code to avoid damage, unauthorized modifications, deletions, and theft; (d) Test data shall be selected with care, protected and controlled; and (e) Enable audit logs to record all updates activity for statistical purposes, recovery and security.	System Owners and ICT System Administrators

0804 Security in the Development and the Support Process	
Objective: Protect and ensure the security of information systems and applications.	
UM-080401 Change Control Procedures	
Matters that need to be complied with are as follows: (a) Changes or modifications to the information systems and applications shall be controlled, tested, recorded and verified before use; (b) Critical applications shall be reviewed and tested when there is a change to the operating system to ensure there is no adverse effect on the operation and security of the university. Individual or a particular group shall be responsible for monitoring improvements and corrections made by the vendor; (c) Control of changes and/or modifications to the software package and ensure that any changes are limited by necessity only; (d) Access to the application source code shall be limited to the permitted users; and (e) Prevent information leakage possibilities.	System Owners and ICT System Administrators
UM-080402 Outsourced Software Development	
Outsourced software development shall be supervised and monitored by the system owner.	PTM and

The source code for all applications and software are the property of UM.	ICT System Administrators
0805 Control of Technical System Vulnerabilities	
Objective: Ensure control of technical systems vulnerabilities is effective, systematic and consistent by taking appropriate measures to ensure effectiveness.	
UM-080501 Control of Technical Threats	
Control of technical threats (vulnerabilities) must be implemented on the operating system and the applications used. Matters that need to be complied with are as follows: (a) Acquiring information about technical vulnerability of information systems used on timely basis; (b) Assessing the level of vulnerability to identify the level of risk that may be encountered; and (c) Taking control measures to address such risks.	ICT System Administrators

ARTICLE 09

ICT SECURITY INCIDENT MANAGEMENT

0901 ICT Security Incident Reporting Mechanisms

Objective:

To ensure that incidents are handled quickly and effectively to minimize the impact of ICT security incidents.

UM-090101 Reporting Mechanism

ICT security incident means an adverse event occurring to an ICT asset or a threat of such an incident. It may be an act in violation of the ICT security policy either expressed or implied. ICT security incidents such as following must be reported to ICTSO and UMCERT immediately: (a) Information is missing, disclosed to the parties who are not authorized, or suspected lost or disclosed to the parties who are not authorized; (b) Any unauthorized use of information systems or suspected as such; (c) Password or access control mechanism is lost, stolen or exposed, or suspected lost, stolen or disclosed; (d) The occurrence of an unusual system event such as missing files, the system often fails and communications wrongly delivered; and	All

(e) Trial trespassing, fraud and incidents that are not expected. A summary of all process involved in ICT security incident dealings at UM is as seen in **Appendix 2**. ICT security incident reporting procedures are based on: (a) General Circular No. 1 of 2001 - Information and Communication Technology Security Incident Reporting Mechanism; and (b) General Circular No. 4 Year 2006 - Management of Information Technology and Communications Security Incident Handling for Public Sector.	
0902 ICT Security Incident Information Management	
Objective: Ensure a consistent and effective approach is applied in the information management of ICT security incident.	
UM-090201 ICT Security Incident Information Management Procedures	
Information about ICT security incidents handled shall be kept and analyzed for the purpose of planning, prevention and learning to control the frequency, damage and incident costs in the future. This information is also used to identify incidents that often occur or have a significant impact on UM. Evidence materials related to ICT security incidents shall be kept and maintained.	ICTSO

Controls that should be considered in information collection and management of incident handling are as follows: (a) Retain audit trail, backup regularly and protect the integrity of all evidence; (b) Keep copies of evidence and records of all copying activity information; (c) Prepare a contingency plan and activate business continuity plans; (d) Provide prompt recovery action; and (e) Inform or consult legal authorities if necessary.	

ARTICLE 10

BUSINESS CONTINUITY MANAGEMENT

1001 Business Continuity Policy

Objective:

Ensure that the service operations are not delayed and sustained service delivery to customers.

UM-100101 Business Continuity Plan

A Business Continuity Management (BCM) Plan should be developed to determine ensure a holistic approach is taken to maintain service continuity. This is to ensure that there is no disruption in the processes in the delivery of the organization services. This plan must be approved by the ICT Council. Following points should be noted: (a) Identify all responsibilities and emergency or recovery procedures; (b) Identify events that can disrupt the business processes along with the likelihood and the impact of such interruptions and the consequences on ICT security; (c) Implementing emergency procedures to allow recovery to be done as soon as possible or within the specified time frame;	ICT Managers

(d) Document/record the processes and procedures that have been agreed upon;

(e) Conduct training programs on emergency procedures for users;

(f) Making back-ups, and

(g) Testing and updating the plan at least once a year.

A BCM plan should be developed and should include the following:

(a) List of core activities that are considered as critical in order of priority;

(b) A list of UM personnel and vendors with contact details (fax, phone and e-mail). Backup list should also be provided as to replace personnel who are unable to attend to deal with incidents;

(c) A complete list of information that require backups and the location it is stored together with the information recovery instructions and related facilities;

(d) Alternative processing resources and location to replace the resources that have been paralyzed, and

(e) Agreements with service providers for priority service reconnection where possible.

A copy of the BCM should be kept in a separate location to avoid damage from the disaster at the main site. BCM plan should be tested at least once a year or whenever there is a change in the environment or business function to ensure its effectiveness. Periodic evaluation shall be performed to ensure that the plan is appropriate and able to fulfill its objective. Tests on the BCM plan must be scheduled to ensure that all members in the restoration and personnel involved know about the plan, responsibilities and their role when the plan is implemented. UM should ensure that copies of the BCM are constantly updated and protected as in the main location.	

ARTICLE 11 COMPLIANCE	
1101 Compliance and Legal Requirements	
Objective: Increase the level of ICT security to prevent a breach of the UM ICT Security Policy.	
UM-110101 Policy Compliance	
Every user in the UM must read, understand and comply with the ICT Security Policy and other law or other regulations that being enforced. All ICT assets at UM, including information stored in its property belong to the University. Heads of Department/authorized officers reserve the right to monitor users' activities to detect the illegal usage. Any use of ICT assets UM other than the meaning and intended purpose, will be considered a misuse of UM resources.	All
UM-110102 Compliance with Policies, Standards and Technical Requirements	
ICTSO shall ensure that all security procedures within their scope of work comply with the policies, standards and technical requirements.	ICTSO

Information systems should be checked regularly to comply with the ICT security standards.	
UM-110103 Audit Requirements Compliance	
Compliance to audit requirements is necessary to minimize threats and maximize the effectiveness of the information systems audit process. Audit requirements and inspection activities of any operational system must be planned and agreed to reduce the probability of a services provision disruption. Access to the information systems' audit tools should be maintained and monitored to ensure that it is not misused.	All
UM-110104 Legal Requirements	
The following are the legal requirements or other relevant regulations which must be observed by all users at UM: (a) Security Directive; (b) General Circular No. 3 of 2000 entitled " Government Information Technology Security Policy and Communications "; (c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002; (d) General Circular No. 1 of 2001 entitled "Security Incident Reporting Mechanism Information and Communication Technology (ICT);	All

(e) Public Administration Development Circular No. 1 year 2003 entitled "Guidelines on the Procedure of Internet and Electronic Mail Usage in Government Agencies";

(f) General Circular Number 6 Year 2005 - Security Risk Assessment Guidelines for Public Sector;

(g) General Circular No. 4 Year 2006 - Public Sector Information and Communication Technology (ICT) Security Incident Handling Management;

(h) National Secretary General Letter of Instruction - Steps To Strengthen Security Wireless Local Area Network in Government Agencies, dated October 20, 2006;

(i) MAMPU Director General Letter of Instruction - Measures Concerning the Use of Electronic Mail on Government Agencies, dated June 1, 2007;

(j) MAMPU Director General Letter of Instruction - Stabilization Measures for Implementation of Electronic Mail System In Government Agencies, dated 23 November 2007;

(k) General Circular No. 2 Year 2000 - The Role of Committees under IT Committee and Government Internet Committee (GITIC);

(l) Treasury Circular Letter (First Supplementary) No. 2/1995 - Procedure for Preparation, Assessment and Tender Acceptance;

(m) Treasury Circular Letter. No.3/1995 - Consultancy Services Acquisition Regulation; (n) Digital Signature Act 1997; (o) Official Secrets Act 1972; (p) Computer Crimes Act 1997; (q) Copyright (Amendment) Act, 1997; (r) Communications and Multimedia Act 1998; (s) General Orders; (t) The direction of the Treasury; (u) Information Technology Act 2007; (v) MAMPU Safety Guidelines 2004; (w) MAMPU ICT Standard Operating Procedure (SOP); (x) General Circular Number 3 year 2009 - Guidelines for the Public Sector Network and ICT System Security Level Evaluation, dated 17 November 2009, and (y) MAMPU Director General Letter of Instruction - Business Continuity Management for Public Sector Agencies, dated January 22, 2010.	
UM-110105 Policy Violation	
UM ICT Security Policy Violation is liable to disciplinary action.	All

GLOSSARY	
Antivirus	Software which scans for any possible viruses on the storage media such as diskettes, compact discs, magnetic tapes, optical disks, flash disks, CD ROMs, thumb drive for viruses.
ICT Asset	ICT equipment including hardware, software, services, data or information and people.
Backup	Process of document or information duplication.
Bandwidth	Size or amount of data that can be transferred through the communication control (for example between hard drives and computers) in the set time frame.
CIO	Chief Information Officer responsible for the ICT and information systems to support an organization direction.
Denial of service	Obstruction of services provision.
Downloading	The act of downloading any online resource.
Encryption	Encryption is a process of data obfuscation by the sender to be understood only by the intended recipients.
Firewall	System designed to prevent access by invalid users either to or from the internal network. Available in the form of hardware or software or a combination of both.
Forgery	Identity fraud and disguise which usually done during message transmission through e-mails, including abuse and identity theft, information theft/espionage, hoaxes.

GLOSSARY	
Hard disk	Used to store data and can be accessed faster.
Hub	Hub is a device that connects two or more workstations to form a star-shaped bus topology and broadcast the received data from a port to the other ports.
ICT	Information and Communication.
ICTSO	ICT Security Officer Officer responsible for the security of computer systems.
Internet	Worldwide network system, where users can access information from the server or another computer.
Internet Gateway	Is a point that acts as an entrance to another network. It properly guides traffic from individual traffic to multiple traffic while maintaining traffic order in the networks so that they remain separated.
Intrusion Detection System (IDS)	Software or hardware that detects unrelated, errors or harmful activities to the system. The nature of the IDS based on monitored data type, i.e. whether the data more as a host or a network.

GLOSSARY	
Intrusion Prevention System (IPS)	Computer security hardware that monitors network and/or activities taking place in the system to detect malicious software. Able to take action by restricting or blocking attacks or malicious code activities. For example: Network-based IPS will monitor all network traffic for any possible attack.
LAN	Local Area Network that connects computers.
Logout	Computer Log-out. Out of a computer system or application.
Malicious Code	Hardware or software that is loaded into the system for the purpose of unauthorized intrusion. It involves the attack of viruses, Trojan horses, worms, spyware and others.
MODEM	MOdulator DEModulator Devices that can convert digital bit stream to analog signals and vice versa. It is usually connected to the phone lines to provide Internet access made from the computer.
Outsource	Using outside service to perform certain ICT functions for certain period stated in the Letter of Agreement with the agreed fee.
Application Software	It refers to the software or package that is often used as spreadsheet and word processing or application system developed by an organization or department.

GLOSSARY	
Public-Key Infrastructure (PKI)	Public Key Infrastructure is a combination of software, encryption technologies and services that enable organizations to protect the security of communication and transactions over the Internet.
Router	Routers are used to send data between two networks with different network position. For example, the Internet performance.
Screen Saver	The images will be activated on the computer after it is not used within a certain timeframe.
Server	Computer server. Storage and service delivery hardware for network client requests.
Switches	Switch is a combination of hub and bridge that filter frame for network segmentation. Switches can improve network performance Carrier Sense Multiple Access / Collision Detection (CSMA / CD) which is a transmission protocol to reduce the collision.
Threat	Harassment and threats through various means such as personal motives e-mails and letters and for some reason.
UMCERT	University of Malaya Computer Emergency Response Team. Team set up to help UM manage ICT security incident handling in all departments.
Uninterruptible Power Supply (UPS)	Equipment used to provide continuous power supply from different sources in the absence of power supply to the connected equipment.
Video Conference	Media that receive and display multimedia information to users at the same time it is received by the sender.

GLOSSARY	
Video Streaming	Interactive communication technologies that allow two or more locations to interact via simultaneous two-way video display and audio.
Virus	Programs that are aimed at destroying data or system applications.
Wireless LAN	Web-connected computer without use of cables.

Appendix 1

COMPLIANCE DECLARATION

UM ICT SECURITY POLICY

Name (Capital Letters) : ……

Identity Card Number : ……

Position : ……

Department : ……

It is solemnly and sincerely declared that:-

1. I have read, understood and will comply with the provisions contained in the UM ICT Security Policy; and
2. If I breach any of the described provisions, then appropriate action can be taken against me.

Signature : .....

Date : .....

ICT Security Officer Confirmation

.....

(ICT Security Officer Name)

On behalf of the Chief Information Office of UM

Date: .....

Appendix 2

ICT SECURITY INCIDENT RESPONSE PROCEDURE

1) Detect ICT security incidents
   1.1. If the incident is detected through the monitoring process continue to step 2
   1.2. If reports received of incidents from user / system administrator or an outside agency such as GCERT / MyCERT / Abuse nets etc. continue to step 4

2) Conduct a preliminary investigation on the incident within one working day.

3) Identify the IP address of the hacker and take action.
   3.1. If it is not a UM IP address, report to the ISP and go to step 6.
   3.2. If it is a UM IP address, proceed to step 4

4) Forward the report of the incident to the system administrator / ICT representatives / concerned parties for cleaning / restoration.

5) Get feedback from ICT Representative / concerned parties about the status of the action taken.

6) Update ICT security incidents statistics report.