Draft Information Security Policy

Version	1.0
Draft Date	February 2014
Status	Draft
Approved By:	

Contents

1.0 POLICY STATEMENT

MUST shall uphold the principles of Information Security through the preservation of the confidentiality, Integrity and Availability of the university's information.

The University is committed to protect both its key data and information and to minimize the impact of any security incidents.

2.0 POLICY PRINCIPLES

2.1 Human Resource

- All employees must comply with the University's Information Security Policy. This requirement forms part of the conditions of employment and new employees will be notified of the policies when they sign into service at the university.
- Breaches of the University's Security Policy and/or associated procedures are potentially disciplinary issues, and may lead to action being taken in accordance with the University's disciplinary procedures.
- All Staff have a responsibility to ensure the security of information which they use or to which they have access. Staff must maintain the confidentiality of any information (both during and after their employment by the university) which comes into their possession in the course of their work and which is sensitive or confidential in nature.

2.2 Training and Awareness

- The Computing Services Unit shall provide all staff with information security awareness tools to enhance awareness and educate them regarding the range of threats, the appropriate safeguards and the need for reporting suspected problems.
- All users of users of new university systems shall be trained to ensure that their use is both efficient and does not compromise information security.

2.3 Staff Leaving the University

- By default staff IT accounts will be disabled immediately the staff member leaves the university, on notification by the Human Resource Department.
- Leaving staff are to be treated sensitively, particularly with regard to the termination of their access privileges.
- Leaving staff must return all information assets and equipment belonging to the university prior to departure, this may include computers, Laptops, Hard drives, Flash Disks

2.4 Personal Security of Information

Security roles and responsibilities will be included in job descriptions where appropriate. These will included any specific responsibilities for the protection of particular information, passwords to information or the execution of particular processes or activities such as data protection.

2.5 User Management

- The University shall maintain a directory of all users (staff and students) of its IT resources and systems.
- All users shall have a unique identifier (User name) for their personal and sole use to access university information services as appropriate. Personal user names must not be used by anyone else, and associated passwords shall not be shared with any other person for any reason. Shared accounts will only be allowed for special purposes, ans with restricted functionality. Such accounts will be disabled when deemed necessary.
- Password Management Procedures will be developed and maintained by the Computing Services Unit to ensure the implementation of the requirements of the Information Security Policy and to assist both staff and students in complying.
- Access Control Standards will be maintained for all information systems, at an appropriate level for each system, which minimizes information security risks yet allows the university's business activities to be carried out without undue hindrance.

2.6 Use of Computers

IT equipment and other physical resources, including hard copy data, must be safeguarded appropriately- especially when left unattended.

- Staff must take reasonable steps to ensure that data held electronically are not vulnerable to theft of inadvertent disclosure to unauthorized users. These include locking a computer if it is to be left unattended.
- The Computing Services Unit shall ensure the installation of protection software against malicious software and computer viruses.
- All computers must comply with the university's Data Backup Procedures to ensure that the risk of loss or damage to information is minimized.
- Staff is only permitted to load software onto University IT equipment with the full authorization and verification of the Computing Services Unit.

2.7 Asset Inventory

An inventory will be maintained of all the University's major information assets and the ownership of each asset shall be clearly stated.

2.8 Data Integrity

- System and Service owners must ensure compliance with the university's Data Backup procedures and Disaster Recovery Plan
- Day-to-day storage must ensure that current information is readily available to authorized users and that archives are both created and accessible in case of need.
- All information used by the university must be stored appropriately
- All hardcopy documents of a sensitive or confidential nature are to be shredded or similarly destroyed when no longer required.
- All university data system should maintain log records of whatever activities are to be carried out by users of the system.
- The Computing Services shall develop all log management policy for all university systems.

2.9 Communication by Email

- All official university email communication should be done using the University's official mailing system.
- Email should only be used for business purposed in a way which is consistent with other forms of business communication.
- Information received via email must be treated with care due to its inherent information security risks. File attachments will be scanned for possible viruses or other malicious code.

2.10 Encryption

A policy on encryption controls will be developed with procedures to provide

- appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory and contractual requirements.
- Confidential information and personal data shall only be taken for use away from the
- University in an encrypted form unless their confidentiality and security can otherwise be assured.

2.11 Network Management

- The University's network shall be maintained by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity. All network management staff shall be given relevant training in information security issues.
- The network must be designed and configured to deliver high performance and reliability to meet the University's needs, whilst providing a high degree of access control and a range of privilege restrictions.
- The network shall be segregated to create security zones, with routing and access controls operating between the zones, to reduce the possibility of internal or external users gaining unauthorised access to systems. Systems with particularly high security vulnerabilities shall be protected both from internal and external access. All other systems will be protected from external access by default.
- Appropriately configured firewalls shall be used to protect the network supporting the University's systems.
- Access to the resources on the network must be strictly controlled to prevent unauthorised access and access control procedures must provide adequate safeguards through robust identification and authentication techniques. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.
- The implementation of new or upgraded software or firmware must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all changes to critical systems or network components. All changes must be properly tested and authorised before moving to the live environment.
- The network infrastructure must be adequately configured and safeguarded against both physical attack and unauthorised intrusion.

2.12 Systems Operations

- All areas where sensitive or business critical information is processed shall be given an appropriate level of physical security and access control. All staff and third parties with authorisation to enter such areas are to be provided with information on the potential security risks, control measures to be taken, and the necessity of complying with the Information Security Policy.
- Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses the university's information systems. Mechanisms shall be in place to monitor and learn from those incidents.
- Procedures will be established for the reporting of software malfunctions and faults in the University's information systems. Faults and malfunctions shall be logged and monitored and timely corrective action taken.

2.13 Systems Management

- The University's systems shall be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with individual system owners. All systems management staff shal be given relevant training in information security issues.
  Access controls shall be maintained at appropriate levels for all systems. A record of access permissions granted must be maintained.
- Access to all information systems, except those which are publicly accessible, shall use a secure logging-on process, and may also be limited by time of day, location of workstation, or through an automatic time-out after a defined period of inactivity, where appropriate. Access to information systems may be logged and monitored to identify potential misuse of systems or information.
- Password management procedures shall meet the requirements of the Information Security Policy.
- Systems administration or management functions shall only be performed by authorised staff. Use of such commands should be logged and monitored where appropriate.
- The implementation of new or upgraded software must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all changes to systems. All changes must be properly tested and authorised by the system owner before moving to the live environment.

2.14 System Planning

- New information systems, or upgrades to existing systems, must be authorised Jointly by the (proposed) system user department and the the University ICT Committee.
- The System planning process shall follow the In-house software development procedures or Procurement of Software guidelines as provided by the Public Procurement and Disposal of Assets Authority (PPDA)
- This process must ensure that security requirements have been appropriately specified.

2.15 Information Access

Access of university information shall be limited to;

- Full-time, part-time and temporary staff employed by, or working for or on behalf of the University.
- Students studying at the university.
- Contractors and consultants working for or on behalf of the university.

2.16 Security of Third Party Access

Access to the university's information processing facilities by third parties will be controlled.
Third parties who require access to the university's information infrastructure will be bound by a contract that defines university security requirements.

2.17 Protection of Key Data and Information

Key data and information will be classified, protectively marked and only accessible to those privileged to access.

2.18 Disposal of Information Storage Media

The Computing Services unit shall ensure that all removable magnetic and optical media containing key data will be reused or disposed of through controlled and secure means when no longer required.