Information Technology Security Policy

1. Policy Statement

The University has become increasingly dependent upon the availability and integrity of its computer based information and Information Technology (IT) based services for many aspects of teaching, learning, research and administration. This makes it is essential to enhance the reliability of IT systems and infrastructure which form the basis of these key services. The IT Security Policy is expected to guide the University and its stakeholders to manage IT in order to provide more reliable IT based services.

Objectives of the IT Security Policy are to:

- ensure that all the University's computer systems, information assets, and infrastructure will be protected from threats whether internal, external, deliberate or accidental
- ensure confidentiality and integrity of information, and availability of information without interruptions
- increase awareness and understanding of the requirements of IT security among both employees and students as well as any third party who access IT systems of the University

1.1 This set of policies has been approved by the University Council and forms part of the policies and procedures of the University. It is applicable to, and is to be communicated to, staff, students, and other parties who will have access to IT systems of the University

1.2 This Policy and associated guidance shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any changes in technology, the law, or University policy

1.3 Management and integrity of central computing servers, systems, core network switches, backup systems, and the overall network infrastructure interconnecting these systems is the responsibility of the ICT Centre

1.4 A member of staff or student shall never attempt to compromise the security of the internal systems of the University

1.5 All users have a responsibility to report promptly (to the ICT Centre) any incidents which may have an IT security implication for the University

1.6 Specialist advice on information security shall be made available throughout the University by the ICT Centre

1.7 Every effort shall be taken to safeguard user data and information of users residing in the University's IT system. However, the University is not liable for loss of such data and information

1.8 A formal complaint should be made to the Director/ICT Centre if users suspect that their personal information has been accessed without authorization. The ICT Centre should investigate such complaints and inform the outcome and report to the Vice Chancellor if the University's rules and regulations are found to be violated

2. Compliance

2.1 All faculties, departments, centres, units and administrative branches within the University are required to comply with this IT Security Policy. The responsibility for compliance lies with the appropriate Dean of the faculty, Head of the department, Head of unit/centre, Officer in charge of administrative branch

2.2 This IT Security Policy sets out the responsibilities of all staff, students and third parties, in relation to their use of ICT systems and information assets of the University. Any individual who accesses the University's systems and/or data agrees, in so doing, to comply with the IT Security Policy

2.3 Before any new critical system is introduced and connected to the network, a risk assessment process will be carried out in order to determine the appropriate level of security measures to be applied by the ICT Centre

2.4 All of the University's information systems will be operated and administered in accordance with relevant procedures, and the University may at any time monitor compliance with written authorization of the Vice-Chancellor, if there are reasonable grounds to believe that a violation of University policy has taken place

3. Employees of the University

3.1 All employees must comply with the University's IT Security Policy. This requirement forms part of the University's terms and conditions of employment, and new employees will be notified of the policies when they sign their contract with the University

3.2 Breaches of the University's IT 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

3.3 All staff members are to be provided with IT security awareness tools to enhance awareness and educate them regarding the range of threats, the appropriate safeguards, and the need for reporting suspected problems

3.4 The University is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise IT security

3.5 Training will be made available to the systems management staff where appropriate to support them in maintaining their knowledge of current threats and information/IT security techniques

3.6 By default, staff IT accounts will be disabled within 60 days after the staff member leaves the University, on notification by the Academic Establishment branch, unless a separate temporary agreement is in place

3.7 Leaving staff must return all information assets and equipment belonging to the University prior to departure, unless otherwise agreed with the faculty, department, centre/unit or administrative branch responsible for the asset

4. Students of the University

4.1 All students must comply with the University's IT Security Policy. This requirement forms part of the University's terms and conditions of registration of students, and new students will be notified of the policies when they register with the University

4.2 Breaches of the University's IT Security Policy and/or associated policies are potentially disciplinary issues, and may lead to action being taken in accordance with the University's disciplinary procedures

4.3 By default, student IT accounts will be disabled within 60 days after the student completes the degree or cancellation of registration, unless a separate temporary agreement is in place

5. Use of Computers and Access Control

5.1 Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all users' access rights match their authorizations

5.2 All users shall have a unique identifier (user ID) for their personal and sole use to access university information services as appropriate. Personal user IDs 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, and with restricted functionality. Such accounts will be disabled when deemed necessary by the ICT Centre in conjunction with the service owner

5.3 Password management procedures will be maintained to ensure the implementation of the requirements of the IT Security Policy and to assist both staff and students in complying with best practice guidelines

5.4 Access control standards will be maintained for all information systems at an appropriate level for each system, which minimizes IT security risks yet allows the University's activities to be carried out without undue hindrance

5.5 Access to all information systems must be authorized by the staff responsible for the system and a record must be maintained of such authorizations, including the appropriate access rights or privileges granted

5.6 Procedures will be maintained for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff changes their role, or staff or students leave the University

5.7 IT equipment and other physical resources must be safeguarded appropriately – especially when left unattended

5.8 Staff must take reasonable steps to ensure that data held electronically are not vulnerable to theft or inadvertent disclosure to unauthorized users. These include locking a workstation if it is to be left unattended

5.9 The ICT Centre will provide the means by which all users can download and install current versions of site-licensed virus protection software

5.10 The University installs protection against malicious software and computer viruses, where appropriate, on its computer systems. Users of these systems must not interfere with or prevent the operation of anti-virus protection. Care must be taken in this regard when transferring data to or from systems outside of the university network – including the transfer of data from home computers

5.11 Appropriate precautions must be taken by staff to ensure that the risk of loss or damage to information is minimized. These precautions must include adequate back up and contingency arrangements for individual, local and centrally run information systems

5.12 Care must be taken when transporting files on removable media (e.g. disks, CD- ROMs and USB flash drives) to ensure the safety of the media as well as information it contains

5.13 Staff are only allowed to install permitted software onto the University's IT equipment

5.14 Any computer equipment in general office environments should be secured behind locked doors or protected by user log-out and or password protected screensavers whenever it is left unattended; and outside of general office hours

5.15 Desktop machines in public areas should contain a device or mechanism for securing and protecting the main components and contents of the computer from theft

5.16 Any portable equipment (such as laptops, memory sticks, CDs, PDAs, etc.) should use a log-on or power-on password wherever possible. Any unattended portable equipment should be physically secure, for example locked in an office or a desk drawer. When being transported in a vehicle they should be hidden from view. Staff should avoid storing sensitive information on portable equipment whenever possible

5.17 Staff who store confidential information on university owned portable equipment must ensure that such data is thoroughly and securely cleansed from that equipment when they leave the University's employment

5.18 All third parties involving access to or use of the university's hardware, software or sensitive information must agree to follow the University's IT Security Policy

6. Information Handling

6.1 Information Assets and Relevant Systems

6.1.1 An inventory will be maintained of all the university's major information assets and the ownership of each asset will be clearly stated

6.1.2 Within the information inventory, each information asset will be classified according to sensitivity

6.1.3 When permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted

6.1.4 The University advocates a clear desk and screen policy particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorized persons

6.1.5 Backup of the University's information assets and the ability to recover them is an important priority. Respective 'owners' of systems are responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the business needs of the University. Backup media must be removable and stored in an area that is remote from the physical system that has been backed up. In the case of critical information systems where 24/7 service is required, consideration must be given to deploying fault tolerant equipment

6.1.6 All information used by the University must be stored appropriately

6.2 Communication by Telephone, WWW, Fax and Email

6.2.1 Email is not a completely secure medium. Users should be conscious of this and consider how emails might be used by others. It should be noted that emails can easily be taken out of context; once an email is sent, the user cannot control what the recipients might do with it; and that it is very easy to forward large amounts of information

6.2.2 Similarly, users should not necessarily trust what is received in an email - in particular, users must never respond to an email request to give a username or password

6.2.3 Email must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure confidentiality: that it is correctly addressed, intended recipients are authorized to receive it, and passwords are used to protect attached documents where required

6.2.4 Users should consider the security implications of any information they put on the University's Website, and the University reserves the right to remove any material which it deems inappropriate, illegal or offensive

6.2.5 Users should not in any way use any areas of the University Website for commercial purposes

6.2.6 Users shall not in any way use Web space to publish material which undermines IT security at the University. In particular, this covers making information available about how IT security is implemented at a practical level, or any known weaknesses

6.2.7 Email addresses and fax telephone numbers should be checked carefully prior to transmission, especially where the information content is confidential or sensitive, or where the disclosure of email addresses or other contact information to the recipients is a possibility. The attachment of data files to an email is only permitted after confirming the confidentiality classification of the information being sent and checking that the document will have been scanned for the possibility of a virus or other malicious code

6.2.8 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

6.2.9. Emailing to distribution lists of university and faculties will be restricted to the Vice Chancellor, respective deans and the Director/ICT Centre

6.3 Encryption

6.3.1 A policy on encryption controls will be developed with procedures to provide appropriate levels of protection to sensitive information

6.3.2 Procedures shall be established to ensure that authorized staff may gain access, when needed, to any important information being held in encrypted form

6.3.3 The confidentiality of information being transferred on portable media or across networks must be protected by the use of appropriate encryption techniques

6.3.4 Encryption shall be used whenever appropriate on all remote access connections to the University's network and resources

6.3.5 A procedure for the management of electronic keys, to control both the encryption and decryption of sensitive documents or digital signatures, must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements

7. Network Management

7.1 The University's network shall be maintained by suitably authorized 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 IT security issues

7.2 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

7.3 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 unauthorized 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

7.4 Access to the resources on the network must be strictly controlled to prevent unauthorized access and access control procedures must provide adequate safeguards through robust identification and authentication techniques

7.5 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 authorized before moving to the live environment

7.6 Faculties/ departments/ units/ centres/ administrative branches should refrain from creating their own Wi-Fi networks other than for research purposes without informing the ICT Centre. Any access points installed should be secure and able to authenticate individual users and ideally these points should be connected to the secure access controller maintained at the ICT Centre *(applicable only after implementation of the secure wireless network)*

7.7 Moves, changes and other reconfigurations of network access points will only be carried out by authorized staff *(applicable only after implementation of the secure wireless network)*

7.8 The network infrastructure must be adequately configured and safeguarded against both physical attack and unauthorized intrusion

7.9 Remote access to resources on the network will be made available only through authorized entry points, normally through the site firewall. Remote access to non-public resources will be subject to authentication and other security mechanisms

7.10 Assigning of IP addresses is a responsibility of the ICT Centre. IP addresses should only be changed by authorized staff and should not be changed without prior written notification to the ICT Centre

8. Systems Operation, Management and Development

8.1 Operations

8.1.1 The ICT Centre manages, maintains and operates a range of central computing servers, systems, core network switches, backup systems, and the overall network infrastructure interconnecting these systems

8.1.2 The ICT Centre shall maintain secure server room facilities with protected power arrangements and climate controlled environments with appropriate level of security

8.1.3 In order to provide a more secure and reliable service as well as to save resources, individual faculties, departments, centres/units and administrative branches are encouraged to utilize centralized systems to offer services such as Learning Management Systems, Websites, etc. where services could be offered as centralized services

8.1.4 In order to enhance the overall security of computing systems of the University, servers with real IPs which could be accessed from outside of the University are required to be kept inside a secure server room

8.1.5 Server rooms, offices and other areas where sensitive or critical information is processed shall be given an appropriate level of physical security and access control

8.1.6 Only authorized persons will be able to access areas where sensitive or critical information is processed or critical information assets are located

8.1.7 Duties and areas of responsibility shall be segregated where practical, and based upon a risk assessment, to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the University. Where possible this segregation of duties should be enforced by the system security

8.1.8 Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the University's systems and associated services, and computing and network facilities. Mechanisms shall be in place to monitor and learn from those incidents

8.1.9 Procedures shall be established for the reporting of software system malfunctions and faults in the University's computing and network facilities. Faults and malfunctions shall be logged and monitored and timely corrective action shall be taken

8.1.10 Development and testing facilities for critical systems shall be separated from operational facilities where economically feasible, and the migration of software from development to operational status shall be subject to formal change control procedures

8.1.11 Security risks to the information assets of all system deployment and development projects shall be assessed and access to those assets shall be controlled. This will include all aspects of integration with existing systems

8.1.12 A Disaster Recovery Plan shall be prepared, documented and tested for existing and new operational systems, at an appropriate level of detail commensurate with the complexity of the system and the assessed level of criticality for the business of the University. This documentation should encompass any recorded exceptions based on risks assessed and management approval given

8.1.13 Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place

8.1.14 Procedures shall be established to control the development and deployment of all operational systems. All systems developed for, and within, the University must follow a formalized development process

8.2 System Management

8.2.1 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 shall be given relevant training in information security issues

8.2.2 Access controls shall be maintained at appropriate levels for all systems by ongoing proactive management and any changes of access permissions must be authorized by the manager of the system or application. A record of access permissions granted must be maintained

8.2.3 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

8.2.4 Password management procedures shall meet the requirements of the IT Security Policy

8.2.5 Systems administration or management functions shall only be performed by authorized staff. Use of such commands should be logged and monitored where appropriate

8.2.6 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 authorized by the system owner before moving to the live environment

8.2.7 Capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available

8.2.8 Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff

8.2.9 System clocks must be regularly synchronized by authorized staff between the University's various processing platforms

8.3 System Planning

8.3.1 New information systems, or upgrades to existing systems, must be authorized within the University's governance structure. The authorization process must take account of security requirements

8.3.2 The information assets associated with any proposed new or updated systems must be identified, classified and recorded

8.3.3 Equipment supporting the University's systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained

8.3.4 Prior to acceptance, all new or upgraded systems shall be tested and the results documented to ensure that they comply with the University's IT Security Policy, access control standards and requirements for ongoing information security management

8.4 Software Management and Development

8.4.1 Software applications are to be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with nominated individual application owners. All staff involved in software development and management shall be given relevant training in information security issues

8.4.2 The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the University must always follow a formalized development process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls

8.4.3 Requirements specifications for new software or enhancement of existing software shall specify the required information security controls

8.4.4 Formal change control procedures, with audit trails, shall be used for all changes to software components of a critical system. All such changes must be risk assessed and authorized by the relevant Officer in Charge before being moved to the live environment

8.4.5 The implementation, use or modification of all software on the University's systems shall be controlled. All software shall be checked before implementation to protect against malicious code

9. Business Continuity

9.1 The University will continue to assess business continuity requirements and to identify appropriate areas for further action

9.2 A formal risk assessment exercise has been conducted to classify all systems according to their level of criticality to the University and to determine where business continuity planning is needed

9.3 A business continuity plan will be developed for each system or activity. The nature of the plan and the actions it contains will be commensurate with the criticality of the system or activity to which it relates

9.4 All business continuity plans will be periodically tested. The frequency of testing will be as defined for the appropriate criticality level and will include tests to verify whether management and staff are able to put the plan into operation

9.5 All relevant staff will receive appropriate training to be able to carry out their roles with respect to business continuity plans

9.6 Each business continuity plan will be regularly reviewed, and if necessary, updated. The frequency of reviews will be as defined for the appropriate criticality level

10. Procurement and management of ICT related systems

10.1 Users are advised to use recommended specifications and guidelines in purchasing general purpose IT equipment such as desktops, laptops, printers, photocopiers, etc. During the procurement process, users are encouraged to obtain the services of the ICT Centre in an advisory capacity.

10.3 Once equipment or systems are installed, either the ICT Centre or the respective user (in case of specialized equipment or systems) should certify that the work has been completed according to requirements

10.3 The ICT Centre should take 'ownership' of key ICT systems in the University to ensure these systems provide a reliable service