Information Systems Operations Policy

1. Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security, environmental protection and access control. Staff with authorisation to enter such areas are to be provided with information on the potential security risks and the measures used to control them.
2. The procedures for the operation and administration of the University's business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained.
3. Duties and areas of responsibility shall be appropriately segregated to reduce the risk and consequential impact of information security incidents that might result in significant damage to the University.
4. Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the University's business operations and information processing systems. Mechanisms shall be in place to monitor and learn from those incidents.
5. 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.
6. Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have managerial approval.
7. Development and testing facilities for business critical systems shall be separated from operational facilities and the migration of software from development to operational status shall be subject to formal change control procedures.
8. 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.
9. Procedures shall be established to control the development or implementation of all operational software. All systems developed for or within the University must follow a formalised development process.
10. The security risks to the information assets of business system development projects shall be assessed and access to those assets shall be controlled appropriately.

approved by IFSG