Information Systems Management Policy

1. The University's information systems shall be managed by suitably trained and qualified personnel to oversee their day to day running and to preserve security and integrity in collaboration with individual system owners. All personnel involved in systems management shall be given appropriate training in information security issues.
2. Access controls shall be maintained at appropriate levels for all systems by ongoing proactive management and any changes of access permissions must be authorised by the University manager responsible for the information system or application. A record of access permissions granted and revoked must be maintained.
3. Access to all information services shall use a log on process which is appropriately secure. Access to the organisation's business systems may also be limited by time of day or by the location of the initiating terminal or both. All access to information services shall be logged and the logs preserved for an appropriate period to enable identification of potential misuse of systems or information.
4. Inactive connections to the organisation's business systems shall shut down after a defined period of inactivity to prevent access by unauthorised persons.
5. Password management procedures shall be put into place to ensure the implementation of the requirement of the information security policies and to assist users in complying with best practice guidelines.
6. Access to commands and functions which might alter a system's normal operation shall be restricted to those persons who are authorised to perform systems administration or management functions. Use of such commands and functions should be logged and the logs preserved for an appropriate period.
7. 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. Changes must be appropriately tested, reviewed and authorised before moving the new or upgraded software to the live environment.
8. 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.
9. Security event logs, operational audit logs and error logs must be properly and periodically reviewed.
10. System clocks must be regularly synchronised between the University's various processing platforms.

11. All University systems shall be protected from virus and other malicious software infection using software and hardware products procured by the University for this purpose.
12. All University information systems shall run appropriately supported systems software, which must incorporate all relevant security updates, patches and hotfixes.

13. To ensure that data and software can be recovered following a media failure or computer disaster, backup copies of all essential data and software must be regularly taken. The backup requirements for each system or business application will vary and need to be defined and regularly reviewed in accordance with the Information Handling guidelines. Backup arrangements for individual systems must also meet the requirements of business continuity plans and backup data should be regularly tested, where practicable, to ensure that it can be relied upon for emergency use when necessary.

approved by IFSG