

1. The University's business critical applications 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 client departments. All personnel involved in managing business systems shall be given appropriate training in information security issues.
2. confidentiality, integrity and availability of information systems should form the basis of decisions on the scheduling of upgrades. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.
3. Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls.
4. Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to critical business software. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment.
5. Modifications to vendor-supplied software shall be discouraged, only strictly controlled essential changes shall be permitted. The development of interfacing software shall only be undertaken in a planned and controlled manner.
6. All interfaces between critical business applications and other systems shall be