Information Systems Planning Policy

1. New information systems, or enhancements to existing systems, must be authorised jointly by the manager(s) responsible for the information having taken competent technical advice. The business requirements of all authorised systems must specify requirements for security controls.
2. The implementation of new or upgraded software must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.
3. The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the Information Handling Policy, and a risk assessment undertaken to identify the probability and impact of security or availability failures.
4. Equipment supporting business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.
5. Equipment supporting business systems shall be given adequate protection from unauthorised access, environmental hazards and electrical power failures. Advice on suitable electrical, environmental, physical security, safety and communications infrastructure must be sought from Estates and Facilities and IT Services.
6. Access controls for all information and information systems are to be set at appropriate levels in accordance with the value and classification of the information assets being protected.
7. Access to operating system commands and application system functions is to be restricted to only those persons who are authorised to perform those systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.
8. Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the organisation's information security policies, access control standards and requirements for ongoing information security management.

approved by IFSG