Procedure: Enterprise systems and applications security

Purpose
To define enterprise systems and applications and their secure use, and to establish the responsibilities of owners and users of enterprise systems and applications.

Definitions
Definitions of terms used in this document are provided in the overarching Policy (Information Technology Security Policy).

Procedure
1. Enterprise systems include applications and associated information that permit the integration of data with other enterprise systems through the use of appropriate common identifiers, for example ANU ID and/or visitor ID.
2. All enterprise systems must have a designated system owner responsible for the operation of the system.
3. System owners must ensure that procedures and processes are regularly updated to remain consistent with current ANU Information Technology (IT) security policies and procedures.
4. Enterprise applications must only be made available to authorised users.
5. All enterprise systems must be covered by:
   a. a security risk management plan
   b. a system security plan
   c. appropriate Standard Operating Procedures (SOPs).
6. Establishment of an enterprise system requires approval from the Director, Information Technology Services (Director, ITS) and the University Information and Communications Technology Governance Committee (UICT), and a fully-costed and approved business case including the following:
   a. Business Solutions Group (providing operational support for business
processes
b. System Support Group (providing operational support for systems)
c. ongoing process support and maintenance
d. planning for system change, testing and quality assurance
e. training and development
f. security
g. upgrades
h. monitoring and documentation.

7. Funding for the establishment of an enterprise system is through the ANU budget allocation process.

8. An enterprise application typically includes:
   a. part of the University’s integrated business environment, supporting core processes and key academic and administrative functions
   b. broad impact systems
   c. sole authoritative sources
   d. an assessment of risk that must be managed, and a focus for audit concern
   e. significant resources for implementation, maintenance and ongoing support.

University responsibilities

9. The University is responsible for:
   a. developing and maintaining overarching IT security frameworks and policy
   b. providing information and support to enable a strong IT security culture
   c. providing guidance on better practice approach on systems across the University.

10. The University responsibilities identified in this procedure are vested in Information Technology Services (ITS).

Enterprise application owner responsibilities

11. Service Division Directors and other areas with responsibility for enterprise systems and applications must ensure that:
   a. procedures and processes are in place for the operation and security of the enterprise system, and that such procedures and processes are consistent
with current information technology security policy and procedures

b. all enterprise applications are protected and accessed only by authorised users

c. adequate measures are taken to ensure that the application system is protected from unauthorised access by any utility, operating system or malicious software that is capable of overriding or bypassing application controls

d. adequate measures are taken to ensure that the application does not compromise other systems with which information resources are shared

e. appropriate steps are taken to ensure the integrity and security of all applications

f. that relevant applications and operating systems in each area remain the responsibility of that area

g. areas assess the risk of unauthorised access, disclosure and loss of data to their enterprise applications, and develop a relevant risk assessment and management plan

h. enterprise applications are included in appropriate backup and contingency plans for business continuity and disaster recovery.

12. Service Division Directors and other areas with responsibility for enterprise systems and applications must comply with the following:

   a. a process for user access to information and application functions must be implemented, documented, and reviewed on a regular basis

   b. user administration controls must be in place including formal procedures and processes for granting, removing, and modifying users

   c. formal change control procedures must be documented and enforced, and that a formal document change process, including risk assessment, and impacts of change, is implemented

   d. audit and monitoring activities must be logged and recorded, and that audit and monitoring logs include user activity, exceptions, and events including user ID, and date, time, and detail of event.

13. In the case of sensitive applications, Service Division Directors and other areas with responsibility for enterprise applications should consider that

   a. the application is run on a dedicated computer; or

   b. resources are only shared with trusted application systems.