Standard: Infrastructure security classification

Purpose

To establish the infrastructure security classification standards and guidelines for University information infrastructure, information systems and assets.

Definitions

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

Standard

1. The University is committed to providing a secure yet open information infrastructure that protects the integrity of its information assets (data and other information), and confidentiality of information without compromising its availability. Systems hosting the University's information or data sets are required to be appropriately classified and secured.

2. The University recognises three broad categories of data held within its systems:
   a. Public data
   b. Internal data
   c. Confidential data

Public data

3. Public data may be open to the general public and is defined as information with no existing restrictions on access or usage. Public data, although subject to ANU disclosure rules, is available to all members of the ANU community and all individuals and entities outside ANU.

4. Examples of public data include:
   a. Publicly posted press releases
   b. Publicly available marketing materials
   c. Publicly posted job announcements
5. Disclosure of public data is unrestricted, providing the disclosure does not violate non-disclosure agreements.

Internal data

6. Due to proprietary, ethical, and privacy considerations, internal data is protected from unauthorised access, modification, transmission, storage, or other use. Internal data is information that is restricted to designated users who have a legitimate purpose for accessing data.

7. Examples of internal data may include:
   a. Employment data
   b. Business partner information (in the absence of more restrictive arrangements)
   c. Internal directories and organisational charts
   d. Planning documents
   e. Contracts.

8. Internal data is:
   a. protected to prevent loss, theft, unauthorised access and/or unauthorised disclosure
   b. protected by confidentiality agreements before access is permitted
   c. stored in a closed container (filing cabinet, closed office, secure area, etc.) when not in use
   d. assigned default classification level if one has not been explicitly defined.

Confidential data

9. Confidential data is protected by statutes, regulations, policies and contractual obligations. Confidential data is sensitive in nature and access is restricted. Disclosure is limited to individuals on a need-to-know basis.

10. Disclosure of confidential data to parties outside the University must be authorised by executive management, or covered by a binding confidentiality agreement.

11. ANU IT Cyber and Digital Security must be notified if data classified as confidential is lost, disclosed to an unauthorised party, or is suspected of being lost or disclosed, or if any unauthorised use of ANU information systems has taken place, or is suspected of taking place.

12. Examples of confidential data include:
a. Medical records and clinical trial data
b. Safety data
c. Personnel and/or payroll records
d. Student records
e. Data identified by government regulation as confidential 
f. Data belonging to a third party that may contain personal or identifiable information
g. Patent information.

13. When storing and transmitting confidential data the following measures must be undertaken:

a. in electronic format data must be protected with a minimum level of authentication to include strong passwords wherever possible
b. encryption methods must be used on mobile devices
c. physical confidential data must be stored in a locked drawer, cabinet, room or area where access is controlled or has sufficient access control measures
d. when transferring to an external entity, electronic data must be strongly encrypted
e. facsimile transferred data must only be sent to a previously established and used address, or one that has been verified as a secure location
f. confidential data must not be posted to a public website.

14. All systems, regardless of their classification, must include the following measures:

a. Access control
b. Asset management
c. Communication and operations management

Access control

15. Access to information infrastructure

a. Physical and logical access to systems may be granted if access is appropriately controlled, and formal procedures are implemented to permit access to the system.
b. The allocation and use of system privileges must be restricted and controlled.
c. A formal review of user privileges must be conducted on a regular basis to ensure that they remain appropriate. Accounts that are no longer required or appropriate must be closed or disabled.

d. When users leave the University, or change roles, access rights on systems must be reviewed and adjusted appropriately.

16. Mobile computing

a. Confidential University data must not be stored on portable computing devices. In the event that no alternative to local storage exists, all confidential University data must be appropriately encrypted.

b. University data must not be transmitted via wireless or to/from a portable computing device, unless approved wireless transmission protocols and approved encryptions are used.

c. Portable computing devices owned by the University, or that contain on–public University information, must be physically secured when unattended by either; locked drawer, cabinet or room, or with a cable–lock system.

17. Password and authentication management

a. The allocation, management, and use of passwords and other forms of authentication must be controlled.

b. System administration and account management passwords should not be stored in an unencrypted form.

18. Remote Access to Information Infrastructure

a. All remote access connections made to the information infrastructure must be made through approved University secure connections.

Asset management

19. Information assets, including hardware and software, must be recorded in an information asset register.

Communication and operation management

20. Capacity Management

a. System resources must be monitored, tuned, and projections made for future capacity requirements to ensure the required system performance.

b. For each new and ongoing activity, capacity requirements must be identified. System tuning and monitoring must be applied to ensure and improve the availability and efficiency of systems. Detective controls must
be put in place to indicate problems in due time, and projections of future capacity requirements take account of new business and system requirements, and current and projected trends in information processing capabilities.

21. Change Management
   a. Change Management systems must follow the documented change control procedures and guidelines to ensure that only authorised updates or changes are made.

22. Operating Procedures
   a. Operating procedures must be documented, maintained and made available to all users. Sensitive documentation must be protected, and access restricted on a need-to-know basis.