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 additional terms used in this document are provided in the overarching policy, Information Technology security.

Encryption: The University considers an appropriate level of encryption to be the standards specified in the Australian Government Information Security Manual.

Information asset: any set of information or part of the information infrastructure critical to the functioning of the University, with a designated system owner.

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. It is recommended that University data is backed up and primarily stored on University provided storage infrastructure. Data owners that choose to store University data elsewhere are responsible for maintaining appropriate backups.
3. The University recognises three broad categories of data held within its systems:
   a. public data
   b. sensitive data (formerly referred to as internal data)
   c. highly sensitive data (formerly referred to as confidential data)
4. Responsibility for the classification of data rests with the system owner.
5. Data users must comply with all relevant non-disclosure agreements, copyright restrictions, confidentiality agreements and ANU disclosure rules.
6. All systems, regardless of their classification, must include the following measures:
   a. access control
   b. asset management
   c. communication and operations management.

Public data

7. Public data is defined as that which would have an insignificant impact on the University if breached.

8. Public data is available to all members of the University community and all individuals and entities outside ANU. Disclosure of public data is generally unrestricted, providing the disclosure does not violate non-disclosure agreements.

9. Encryption is permitted but not required for the transmission of public data.

10. Examples of public data include:
    a. publicly posted press releases
    b. published research data
    c. publicly available marketing materials
    d. publicly posted job announcements.

Sensitive data

11. Sensitive data is defined as that which would have a low or medium impact on the University if breached.

12. Sensitive data is restricted on a need to know basis, and may only be accessed, transmitted, modified, or stored for a legitimate academic, research or business purpose.

13. Encryption is recommended but not required for the transmission of sensitive data.

14. Sensitive data is:
    a. protected to prevent loss, theft, malicious activity, unauthorised access and/or unauthorised disclosure
    b. protected by confidentiality agreements before access is permitted
    c. the default classification for data if a classification level has not been explicitly defined.
15. Hard copies of sensitive data must be stored in a closed container (filing cabinet, closed office, secure area etc.). Sensitive data in electronic format must be stored on a system that requires user authentication.

16. Examples of sensitive 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.

Highly sensitive data

17. Highly sensitive data is defined as that which would have a high impact on the University if breached.

18. Highly sensitive data is restricted on a need to know basis, and may only be accessed, transmitted, modified, or stored for legitimate academic, research or business purposes.

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

20. Highly sensitive data is protected by statutes, regulations, policies and contractual obligations.

21. When storing and transmitting highly sensitive data, the following measures must be undertaken:
   a. hard copies must be stored in a locked drawer, cabinet, room or area where access is controlled or has sufficient access control measures
   b. electronic copies must be stored on a system that requires ANU-based user authentication
   c. in the event that it must be recorded to an external data storage device, such as a flash drive, all data must be encrypted
   d. electronic copies must be encrypted when transferring to an external entity
   e. must not be posted to a public website
   f. must not be sent to an external email account
   g. must not be stored on non ANU-managed storage.

22. The Information Technology Services (ITS) Cyber and Digital Security Team
must be notified if data classified as highly sensitive is lost, disclosed to an unauthorised party, 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.

23. Examples of highly sensitive data include:
   a. medical records and clinical trial data
   b. safety data
   c. personnel and/or payroll records
   d. student records
   e. data identified under the Australian government security classification system as confidential (refer to www.protectivesecurity.gov.au)
   f. data belonging to a third party that may contain personal or identifiable information
   g. contracts
   h. patent information.

**System owner responsibilities**

24. Physical and logical access to systems may be granted by the system owner if access is appropriately controlled, and formal procedures are implemented to permit access to the system.

25. The allocation and use of system privileges must be restricted and controlled.

26. 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.

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

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

29. 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.

30. 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.

**User responsibilities**

31. The allocation, management, and use of passwords and other forms of authentication must be controlled and in accordance with the *Passwords procedure*.

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

33. Portable computing devices owned by the University, or that contain non-public University information, must be physically secured when unattended by either: locked drawer, cabinet or room, or with a cable-lock system.