Standard: Infrastructure security classification

Purpose

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

Definitions

Definitions of additional terms used in this document are provided in the overarching Information technology security policy.

Encryption: A cryptographic function used to ensure the confidentiality of data. The University considers an appropriate level of encryption to be the standards specified in the Australian Government Information Security Manual. See section “ASD Approved Cryptographic Algorithms”.

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); and

    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 comply with all relevant non-disclosure agreements, copyright restrictions, confidentiality agreements and ANU disclosure rules.

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

   a. access control;

   b. asset management; and

   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; and

   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; and

   c. the default classification for data if a classification level has not been explicitly defined.

15. Hard copies of sensitive data are stored in a closed container (filing cabinet, closed office, secure area etc). Sensitive data in electronic format is stored on a system that requires user authentication.

16. Examples of sensitive data include:

a. employment data;

b. business partner information (in the absence of more restrictive arrangements);

c. internal directories and organisational charts; and

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 is only accessed, transmitted, modified, or stored for legitimate academic, research or business purposes.

19. Disclosure of highly sensitive data to parties outside the University is 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 are undertaken:

a. hard copies are stored in a locked drawer, cabinet, room or area where access is controlled or has sufficient access control measures;

b. electronic copies are stored on a system that requires ANU-based user authentication;

c. in the event that it is recorded to an external data storage device, such as a flash drive, all data is encrypted;

d. electronic copies are encrypted when transferring to an external entity;

e. not posted to a public website;

f. not sent to an external email account; and

g. not stored on non ANU-managed storage.

22. The Information Technology Services (ITS) Cyber and Digital Security Team is 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; and

h. patent information.

System owner responsibilities

24. Physical and logical access to systems is 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 is restricted and controlled.

26. A formal review of user privileges is conducted on a regular basis to ensure that they remain appropriate. Accounts that are no longer required or appropriate are closed or disabled.

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

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

29. For each new and ongoing activity, capacity requirements are identified. System tuning and monitoring are applied to ensure and improve the availability and efficiency of systems. Detective controls are 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 are documented, maintained and made available to all users. Sensitive documentation is 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 is controlled in accordance with the Passwords procedure.

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

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

Document information

Title	Infrastructure security classification
Document Type	Standard
Document Number	ANUP_000753
Version	10
Purpose	To establish the infrastructure security classification standards and guidelines for University information infrastructure, information systems and assets.
Audience	Staff, Students, Alumni, Affiliates
Category	Administrative
Topic	Information Technology
Subtopic	Security
Effective Date	2 Apr 2019
Review Date	5 Apr 2022
Responsible Officer	Director, Information Technology Services (director.its@anu.edu.au)
Approved By	Vice-Chancellor (eo.vc@anu.edu.au)
Contact Area	Information Technology Services (policies.its@anu.edu.au)
Authority	Information Infrastructure and Services Statute 2012 Information Infrastructure and Services Rule 2015 AS ISO/IEC 27002:2015 Australian National University Act 1991 Australian Government Protective Security Policy Framework Public Governance, Performance and Accountability Act 2013 Public Governance, Performance and Accountability Rule 2014 Australian Government Department of Finance and Deregulation Finance Circular No. 2009/08 Crimes Act 1914 (Cth) Privacy Act 1988 Telecommunications Act 1997 Telecommunications Regulations 2001 1504249909
Printed On	26 Jan 2022