Procedure: Authentication for access to University resources

Purpose

This procedure establishes the minimum standards for authentication for access to University systems (email, file storage, software, etc.) and services to authorised users within the University community.

Definitions

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

Authentication: the act of verifying the identity of a user, process or device as a prerequisite to allowing access to resources in an information system. Includes authentication measures such as passwords, passphrases and multifactor authentication.

Multifactor Authentication: a security measure that requires two or more proofs of identity to allow a user to authenticate. Multifactor authentication typically requires a combination of something the user knows (PIN, secret question), something they have (phone, card, token) or something they are (fingerprint or other biometric).

Passphrase: a sequence of words used for authentication (e.g. pineapple Imagine 99).

Password: a sequence of characters or words used for authentication (e.g. ^Mhall.ifwwa*99btls). The use of the term password(s) also includes passphrase(s). The use of the term password(s) in this procedure does not include Personal Identification Numbers (PINs).

Personal Identification Number (PIN): a sequence of numbers used for authentication.

Standard users: users who do not have privileged or elevated access to University systems, as defined in the Information technology account management and access procedure.

Procedure

1. ANU is committed to ensuring appropriate security for all systems, technology, data, equipment, and processes within its ownership and control.

2. The University provides access to:

a. authorised users within the University community; and

b. network connecting devices authorised for connection, and that have been allocated an IP address within the University's IP Address range.

University responsibilities

3. The University is responsible for:

a. providing and maintaining access to systems and resources for authorised users;

b. suspending any part of an authorised user's access as a result of a security concern or policy breach, resulting from penalties or disciplinary action; and

c. maintaining and amending minimum authentication standards as appropriate, to reflect current information security protocols.

User responsibilities

4. Users:

a. do not disclose or share their authentication details to anyone else under any circumstances;

b. do not allow any other individual access to a service or resource authenticated with their credentials;

c. do not reuse authentication details used for University systems on any other system or service;

d. comply with published account management and authentication security standards for the system/service that they are accessing; and

e. report suspected security incidents such as the compromise of authentication details by emailing it.security@anu.edu.au in accordance with the Information technology security policy. Further information is available at https://services.anu.edu.au/information-technology/it-security/reporting-an-it-security-incident.

f. If a user wishes to record and store authentication details, the following measures are undertaken:

i. records in electronic format are stored on a secure system such as a password/credentials manager or password vault; and

ii. records in hard copy are stored in a highly secure location such as a locked safe, security container or other secure area with sufficient auditable physical access control measures.

5. Group or shared passwords are not used unless no reasonable alternative is available. Where group or shared passwords are used, this is signed off by the owner of the account and/ or the relevant delegate and registered with the ANU Information Security Office at it.security@anu.edu.au. The owner of the account is responsible for any misuse of the account. Group passwords are:
    a. only disclosed to individuals who have been authorised to access a particular electronic resource or service as part of that group; and
    b. changed whenever a member of the group leaves the group.

System owner responsibilities

6. System owners enforce the minimum authentication standards set out in this document when allowing user access to the systems under their ownership.
7. Owners of systems containing sensitive or highly sensitive data as defined in the Infrastructure security classification standard will:
    a. ensure that authentication requirements are in line with the relevant enterprise systems tier as per the Enterprise systems management standard; and
    b. publish any change in authentication requirements to users of that system directly at the time the account is issued and at least annually thereafter.

Minimum authentication standards

8. Access to University systems and services is only given to users with secure access via a password and/or multifactor authentication. Information on best practice regarding passwords and authentication is available on the ANU Cyber Sense website at https://cybersense.anu.edu.au/faq.
9. Standard user passwords meet the following requirements:
    a. are a minimum of 17 characters; or
    b. are a minimum of 10 characters and include at least one character from each of at least three of the following groups:
        * lowercase characters (a - z)
        * uppercase characters (A – Z)
        * digits (0 - 9)
        * punctuation and special characters ($, !, %, ^, (,), {, }, [,], ;, :, <, >, ?)
        * unicode characters; and
    c. do not consist of:

- the account name in any form (as-is, reversed, capitalised, doubled, etc.);
- the user's first or last name in any form;
- simple patterns of letters on keyboards; or
- any well-known or publicly posted identifiable information.

10. Any and all exceptions to the minimum authentication standards at clauses 8 and 9 are registered by the system owner with ANU Information Security Office by emailing it.security@anu.edu.au with sign off by the relevant delegate.

Initial and reset authentication generation

11. All initial and assisted reset passwords are generated randomly and are only recorded upon initial generation. Only one copy is made and this is provided directly to the owner of the password after suitable proof of identity is provided as per clause 13. User passwords are not disclosed to anyone other than the password owner under any circumstances.

12. Requests for user authentication resets or single-use authentications require suitable proof of identity before being actioned. Suitable proof of identity for authentication includes:

a. photo ID;

b. supervisor identification; or

c. satisfactory challenge responses.

13. All authentication resets generate an auditable log indicating at a minimum the date, time, account name, and who conducted the reset.

14. Authentication resets conform to the same controls as set out for initial credential generation.

Document information

Title	Authentication for access to University resources
Document Type	Procedure
Document Number	ANUP_013008
Version	
Purpose	This procedure establishes the minimum standards for authentication for access to University systems (email, file storage, software, etc.) and services to authorised users within the University community.
Audience	Staff, Students, Alumni, Affiliates
Category	Administrative
Topic	Information Security
Subtopic	
Effective Date	27 Sep 2022
Review Date	27 Sep 2027
Responsible Officer	Chief Information Security Officer (ciso@anu.edu.au)
Approved By	Chief Operating Officer (COO@anu.edu.au)
Contact Area	Information Security Office (ciso@anu.edu.au)
Authority	1092601639 Information Infrastructure and Services Rule 2020 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 Crimes Act 1914 (Cth) Privacy Act 1988 Telecommunications Act 1997 Telecommunications Regulations 2021 1504249911
Printed On	14 Dec 2024