Procedure: Passwords

Purpose

The University provides access to information infrastructure and services to authorised users within the University community. Passwords are the primary means of authenticating user access to ANU information services and systems. This procedure establishes the minimum standards for University system passwords and/or passphrases, and outlines their correct use.

Definitions

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

Standard users: those 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 information technology, data, equipment, and processes within its domain of ownership and control.

2. The University provides access for all:

    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.

3. Suspected or known security incidents must be reported to the ITS Cyber and Digital Security Team by emailing it.security@anu.edu.au and remediation is coordinated from that office.

4. The use of the term password(s) in this document also includes passphrases(s).

University responsibilities

5. 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 password standards as appropriate, to reflect current IT security protocols.

User responsibilities

6. Users:

a. observe and comply with all relevant policies and procedures;

b. do not disclose their password to anyone else under any circumstances; and

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

7. Passwords used for University systems are not reused for other systems or services.

8. User passwords are changed in accordance with the published account management standards for the system/service that they are accessing.

9. Passwords believed to have been compromised are changed immediately and the matter is reported by the user to the ITS Cyber and Digital Security Team by emailing it.security@anu.edu.au, in accordance with the Information technology security policy. In this event staff members also notify their supervisor.

10. If a user wishes to record and store passwords, the following measures are undertaken:

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

b. records in electronic format are stored on a system that requires user authentication.

System owner responsibilities

11. System owners enforce the minimum password standards set out in this document when allowing user access to the systems under their ownership.

12. System owners of systems containing sensitive or highly sensitive data:

a. may heighten authentication requirements in line with the Enterprise systems management standard; and

b. publish heightened authentication requirements to users of that system directly at the time the account is issued and at least annually thereafter.

Minimum password standards

13. Standard user passwords meet the following requirements. Passwords:

    a. are a minimum of 10 characters;

    b. 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.

Initial and reset password generation

14. All initial and assisted reset passwords are generated randomly.

15. Requests for user password resets require suitable proof of identity before being actioned. Suitable proof of identity for password resets include:

    a. photo ID;

    b. supervisor identification; or

    c. satisfactory challenge-responses.

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

17. Password resets conform to the same controls as set out for initial password generation.

18. User passwords are only recorded upon initial generation. Only one copy is made and this is provided directly to the owner of the password.

19. User passwords are not disclosed to anyone other than the password owner under any circumstances.

20. Group passwords are discouraged. Where no alternative exists, group passwords can:

a. only be disclosed to individuals who have been authorised to access a particular electronic resource or service as part of that group.

a. be changed whenever a member of the group leaves the group or at least as often as a user password.

Identity self service portal

21. Some systems utilise the Identity Self Service Portal (ISSP) to generate and manage passwords. The following apply to passwords generated and managed in this manner.

22. The initial password is valid for 14 days, after which it will expire.

23. When issued with an initial password, users change the issued password immediately by:

a. logging into the Identity Self Service portal;

b. reading the required ANU policies; and

c. setting up security questions and answers.

24. All passwords created using the ISSP have a minimum lifespan of 24 hours. A user can not change their password again during this period, except via an assisted password reset.

25. All passwords created using the ISSP have an expiry period of 180 days.

26. Users receive an automatic email notification after a password reset has occurred.

27. Users cannot use any of the previous five passwords when setting a new password.

28. An assisted password reset provides the user with a temporary password to be used only once to log in to the ISSP. This password is valid for 24 hours only, after which the password will expire.

29. After a password has expired, users are still able to log into the Identity Self Service portal to reset their passwords.

Document information

Title	Passwords
Document Type	Procedure
Document Number	ANUP_013008
Version	5
Purpose	Passwords are the primary means of authenticating user access to ANU information services and systems. This procedure establishes the minimum standards for University system passwords and/or passphrases.
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	Chief Operating Officer (chris.grange@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 1998 Telecommunications Act 1997 Telecommunications Regulations 2001
	1504249911