Procedure: Passwords

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.

Definitions

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

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:
   a. all authorised users within the University community
   b. all 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 passphrase(s).

University responsibilities

5. The University is responsible for:
   a. providing and maintaining authorised users with access to systems and resources
   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 imposed under the Information Infrastructure and Services Rules 2015.
User responsibilities

6. Users are responsible for observing and complying with all relevant policies and procedures.

7. User must not disclose their password to anyone else under any circumstances.

8. User must not allow any other individual access to a service or resource authenticated with their credentials.

System owner responsibilities

9. System owners of systems containing sensitive or highly sensitive data may heighten authentication requirements in line with the Enterprise systems management standard.

10. System owners of systems which require more stringent password management controls will publish those standards to users of that system directly at the time the account is issued and at least on an annual basis.

Minimum password standards

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

12. Standard user passwords must meet the following requirements:
   a. passwords must be minimum of 10 characters
   b. passwords must 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
   c. passwords shall 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.

13. Passwords used for University systems must not be reused for other
systems or services.

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

15. Users must not re-use passwords for systems where the accepted level of security is high.

**Initial and reset password generation**

16. All initial and assisted reset passwords must be generated randomly.

17. Requests for user password resets will require suitable proof of identity before being actioned. Suitable proof of identity for password resets may include:
   a. photo ID
   b. supervisor identification
   c. satisfactory challenge–responses.

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

19. Password resets must additionally conform to the same controls as set out for initial password generation.

**Systems using Identity Self Service portal**

20. The initial password will be valid for 14 days, after which it will expire. When issued with an initial password, users must change the issued password immediately by:
   a. logging into the Identity Self Service portal
   b. read and acknowledge the required ANU Policies
   c. setup security questions and answers

21. All passwords setup using the Identity Self Service portal will have a minimum age of 24 hours. A user will not be able to change their password again during this period, except via an assisted password reset.

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

23. All passwords setup using the Identity Self Service portal will have an expiry period of 365 days.

24. User must not use any of the previous 5 passwords when setting a new password.

25. An assisted password reset will provide the user with a temporary password
to be used only once to log in to the Identity Self Service portal. This password will be valid for 24 hours only, after which the password will expire.

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

Storage of passwords

27. User passwords must only be recorded upon initial generation. Only one copy may be made and this is to be provided directly to the owner of the password.

28. If a user wishes to record and store passwords, the following measures must be undertaken:
   a. records in hard copy must be stored in a locked drawer, cabinet, room or area where access is controlled or has sufficient access control measures
   b. records in electronic format must be stored on a system that requires user authentication.

Confidentiality of passwords

29. User passwords must not be disclosed to anyone other than the password owner under any circumstances.

30. Group passwords are discouraged. Where permitted, group passwords must only be disclosed to individuals who have been authorised to access a particular electronic resource or service as part of that group. Group passwords must be changed whenever a member of the group leaves the group or at least as often as a user password.

31. Passwords believed to have been compromised must be changed immediately and the matter must be 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 must also notify their supervisor.
<table>
<thead>
<tr>
<th>Document information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Passwords</td>
</tr>
<tr>
<td>Document Type</td>
<td>Procedure</td>
</tr>
<tr>
<td>Document Number</td>
<td>ANUP_013008</td>
</tr>
<tr>
<td>Version</td>
<td>3</td>
</tr>
<tr>
<td>Purpose</td>
<td>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.</td>
</tr>
<tr>
<td>Audience</td>
<td>Staff, Students, Alumni, Affiliates</td>
</tr>
<tr>
<td>Category</td>
<td>Administrative</td>
</tr>
<tr>
<td>Topic</td>
<td>Information Technology</td>
</tr>
<tr>
<td>Subtopic</td>
<td>Security</td>
</tr>
<tr>
<td>Effective Date</td>
<td>19 Jul 2018</td>
</tr>
<tr>
<td>Review Date</td>
<td>2 Jan 2019</td>
</tr>
<tr>
<td>Responsible Officer</td>
<td>Director, Information Technology Services (<a href="mailto:director.its@anu.edu.au">director.its@anu.edu.au</a>)</td>
</tr>
<tr>
<td>Approved By</td>
<td>Chief Operating Officer (<a href="mailto:chris.grange@anu.edu.au">chris.grange@anu.edu.au</a>)</td>
</tr>
<tr>
<td>Contact Area</td>
<td>Information Technology Services (<a href="mailto:policies.its@anu.edu.au">policies.its@anu.edu.au</a>)</td>
</tr>
</tbody>
</table>
| 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 |
Please ensure you have the latest version of this document from the Policy Library website before referencing this.