Procedure: Information technology account management and access

Purpose

To establish the framework and procedures by which University information technology (IT) accounts are managed and secured, and set guidelines for the use of privileged access and elevated access accounts.

Definitions

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

Non-ANU entity: a separate legal entity to the University that has a presence within the University, and requires access to the Integrated Communication Network (ICN) and an allocation of the University's internet protocol (IP) addresses. Accounts created for this purpose are known as auxiliary accounts.

Privileged access: users of a system who have one or more of the following, and may include systems and database administrators:

- the ability to change key system configurations;
- the ability to change control parameters;
- access to audit and security monitoring information;
- the ability to circumvent security measures;
- access to data, files, and accounts used by other users, including backups and media; or
- special access for troubleshooting a system.

Elevated access: users within a business system or application who have additional access via roles or functionality, and who do not have privileged access. Elevated access users includes supervisors or reviewers.

Procedure

1. The University provides access to information infrastructure and services to authorised users.

2. Suspected or known security incidents are reported to the Information Technology Services (ITS) Cyber and Digital Security Team by emailing it.security@anu.edu.au and remediation will be coordinated from that office.

University responsibilities

3. The University is responsible for:

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

   b. authorising and providing non-ANU entities with network access and determining the form of the network access;

   c. suspending an authorised user's network access for breaches of policy, resulting from penalties or disciplinary action;

   d. where possible, informing users and auxiliary account holders when their devices are blocked from network access and outlining the actions to be undertaken before network access will be restored; and

   e. establishing and managing life cycles of user accounts for authorised users. De-activation and/or expiration of access will occur when an authorised user leaves or ceases association with the University; an account reaches its expiration date; or account closure is requested

System owner responsibilities

4. System owners are responsible for:

   a. security architecture, identifying and accessing architecture within the system that they manage;

   b. providing appropriate network access to authorised system users and business areas;

   c. ensuring all users are advised of and acknowledge all relevant ANU policies and related documentation are provided with adequate training and support on the use of information infrastructure;

   d. reviewing and updating privileged access and elevated access on a semi-annual basis;

   e. identifying and managing disaster recovery and business continuity requirements for the system; and

   f. ensuring that risk management, including risk assessment and mitigation, and change management processes, are undertaken with respect to the system.

5. System owners maintain a list of privileged and elevated account users for the system. They are responsible for:

a. implementing and maintaining a system access approval process. This process limits the access level of users to that required to undertake their duties;

b. ensuring that users with elevated or privileged access are provided with adequate training and support on the use of privileged accounts and the security of information assets;

c. ensuring that privileged accounts are kept to a minimum and only used for essential administrative tasks; and

d. ensuring that privileged accounts are controlled and accountable.

User responsibilities

6. Authorised users:

a. maintain the integrity of the network, system, and physical infrastructure;

b. do not negatively impact the usage and output of other system users;

c. maintain awareness of and compliance with all relevant ANU policies and related documentation, rules and standards governing IT and information assets;

d. complete all user training required by the system owner; and

e. comply with security and password requirements, as set out in the Passwords procedure

7. Users of privileged accounts:

a. ensure the security of the account and access, and report any identified risks to the system owner; and

b. only use their privileged account for administrative purposes, i.e. no web browsing or email access occurs while logged in with this access.

Document information

Title	Information technology account management and access
Document Type	Procedure
Document Number	ANUP_000709
Version	10
Purpose	To establish the framework and procedures by which University Information Technology (IT) accounts are managed and secured, and set guidelines for the use of privileged access and elevated access accounts.
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

	1504249906
Printed On	26 Jan 2022

Please ensure you have the latest version of this document from the Policy Library website before referencing this.