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 policy, Information Technology security.

Non-ANU entity: a separate legal entity to the University that has a presence within the University boundary, and requires as a minimum, access to the ICN and an allocation of the University’s internet protocol (IP) addresses.

Procedure
1. The University provides access to information infrastructure and services to authorised users within the University community.
2. Suspected or known security incidents must be 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. suspending an authorised user’s network access for breaches of policy, resulting from penalties or disciplinary action imposed under the Information Infrastructure and Services Rule 2015.
   c. where possible, informing users when their devices are blocked from network access and the actions they must undertake before network access will be restored.
d. authorising and providing non–ANU entities with network access and determining the form of the network access.

**System owner responsibilities**

4. System owners are responsible for:
   
a. security architecture, and identity and access architecture within the systems that they manage
   
b. providing appropriate network access to business areas under the control of the respective Budget Unit
   
c. providing and maintaining accounts for visitors
   
d. ensuring all users acknowledge and are advised of all relevant ANU policies and related documents, and are provided with adequate training and support on the use of information infrastructure
   
e. conducting semi–annual reviews of privileged access and elevated access to ensure that access is still required for the users to perform their role. The Manager, Cyber and Digital Security will initiate semi–annual review process and report outcomes to the Director, ITS
   
f. identifying and managing disaster recovery and business continuity requirements within their area
   
g. ensuring that risk management, including risk assessment and mitigation, and change management processes, are undertaken with respect to the information technology within their area.

**User responsibilities**

5. Authorised users are responsible for:
   
a. respecting the rights of other users and the integrity of the network, systems and physical infrastructure
   
b. maintaining awareness of and compliance with all relevant ANU policies and related documents, Rules and Standards governing IT and information assets, relevant laws, regulations, and contractual obligations
   
c. completing any user training required by the system owners
   
d. complying with security and password requirements set out in the

*Passwords procedure*. 
Privileged access and elevated access accounts

6. Privileged access users of a system are those who have one or more of the following, and may include systems and database administrators:
   a. the ability to change key system configurations
   b. the ability to change control parameters
   c. access to audit and security monitoring information
   d. the ability to circumvent security measures
   e. access to data, files, and accounts used by other users, including backups and media
   f. special access for troubleshooting a system.

7. Elevated access users are those within a business system or application who have additional access via roles or functionality, and who do not have privileged access. Elevated access users may include supervisors or reviewers.

8. Access to the University's computing resources, facilities and data is generally available to managers and administrative staff throughout the University. Standard access is provided initially to users by default; elevated access or privileged access is granted on the submission of an application form with delegate approval.

9. A list of privileged account users is maintained by each system owner.

10. System owners must ensure that:
    a. staff requesting access to a system have a genuine business requirement, verified by their manager
    b. staff are only given the privileges required to undertake their duties
    c. privileged accounts are controlled and accountable
    d. privileged accounts are kept to a minimum and only used for essential administrative tasks
    e. that users are provided with adequate training and support on the use of privileged accounts and the security of information assets.

11. Users of privileged accounts must ensure the security of the account and access, and that any risk is identified and reported.

12. Privileged and elevated access accounts must only be used for administrative purposes only, i.e. no web browsing or email access should occur while logged in with this access.
Deactivation and expiration of access

13. The University is responsible for establishing and managing life cycles of user accounts for authorised users.

14. Deactivation and/or expiration of access will occur when:
   a. a student or staff member leaves the University
   b. an auxiliary account holder is no longer associated with the University
   c. a user is found to have breached the ANU information technology policies and rules governing appropriate usage of University information technology resources
   d. an account is no longer required or has reached its expiration date as advised on the University Email or auxiliary account request form.