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 accounts.

Definitions
Definitions of terms used in this document are provided in the overarching Policy (Information Technology Security Policy).

Procedure
1. In alignment with the University’s strategic plans, the University will provide access to information infrastructure and services to all members of the University community, enabling the continued excellence and performance in education, teaching and learning, and research.
2. The University provides access to:
   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 University Cyber and Digital Security and remediation is coordinated from that office.

University Responsibilities
4. The University is responsible for:
   a. providing and maintaining authorised users with access
   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 Rules 2015
   c. instructing any authorised users identified responsible for network
connecting devices which have been blocked from network access and the obligations they must undertake before network access is restored
d. authorising and providing non–ANU Entities with network access and determining the form of the network access
e. ensuring all network access adheres to the obligations of the University’s Access Agreement

5. University responsibilities under this procedure are vested in Information Technology Services.

Owner Responsibilities

6. 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. provision and ongoing management of user accounts for visitors
   d. ensuring authorised users acknowledge and abide by all relevant ANU policies and related documents
   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. ensuring users are provided with adequate training and support on the use of information infrastructure and the security of information assets
   g. identifying and managing disaster recovery and business continuity requirements within their area
   h. ensure 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

7. Authorised Users are responsible for:
   a. respecting the rights of other users and the integrity of the network, systems and physical infrastructure
   b. observing and complying with all relevant policies, laws, regulations, and
contractual obligations

c. not connecting unauthorised network devices to the University’s network
d. complying with security and password requirements set out in the Password Procedure
e. maintaining an appropriate level of awareness and compliance with University policies, procedures, Rules and Standards governing IT and information assets, and completing any user training required by the system owners.

Privileged Access and Elevated Access Accounts

8. Privileged Access users are users of a system/s with 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.

9. Elevated Access users are users within a business system or application who have additional access via roles or functionality, who do not have Privileged Access. Elevated Access users may include supervisors or reviewers.

10. Access to the University’s computing resources, facilities and data is generally available to managers and administrative staff throughout the University. Least privilege 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.

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

12. Use of privileged accounts

   a. Staff requiring access to a system must have a genuine business requirement, verified by their manager, to access the system.

   b. Staff must only be given the privileges required to undertake their duties. Providing staff with privileged access when there is no requirement can pose a significant risk to the integrity of the system.
c. Privileged accounts can potentially allow access to the entire system and strong authentication must be used, especially if the account provides access to financial, confidential, or otherwise sensitive information or data.

13. Control of privileged accounts
   a. Privileged accounts must be controlled and accountable.
   b. Privileged accounts must be kept to a minimum and only used for essential administrative tasks.

14. Supervisors of privileged accounts must ensure users are provided with adequate training and support on the use of privileged accounts and the security of information assets.

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

16. Users of privileged accounts must apply change management processes.

17. Users of privileged accounts are responsible for maintaining an appropriate level of awareness and compliance with University policies, procedures, Statutes, Rules, and Standards governing access, information infrastructure, and elevated password requirements.

Deactivation and Expiration of Access

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

19. Deactivation and/or expiration of access will occur when:
   c. a student or staff member leaves the University
   d. an auxiliary account is no longer associated with the University
   e. a user is found to have breached the ANU information technology policies and Rules governing appropriate usage of University information technology resources
   f. an account is no longer required/has reached its expiration date as advised on the University Email Account/Auxiliary Account Request Form.