Information Security Access Control Standard

Section 1 - Executive Summary

(1) The University's ICT resources including software, hardware, data, and networks are used by staff, students, affiliates, vendors, and members of the public.

(2) Access management ensures only those with a legitimate need can access our ICT resources. Access management also prevents unauthorised viewing, modification and deletion of data and systems.

(3) Most staff and students are standard users of ICT resources, and their access is centrally managed. Some staff and students have privileged access, which allows them to perform actions that have a greater impact. Additional controls are required to protect privileged accounts from compromise. This document provides controls for managing both standard and privileged access.

(4) System Owners and Information Owners are responsible for determining access requirements for their ICT resources and for ensuring that access is managed throughout the life of the ICT Resource in accordance with this document.

Section 2 - Purpose

(5) This document provides the University's standard for access controls including account creation, authentication, authorisation, credential management, and monitoring.

Section 3 - Scope

(6) This document applies to all ICT resources owned and/or managed by the University.

Section 4 - Audience

(7) The primary audience for this document is System Owners, Information Owners, System Administrators, technical staff, and any other staff responsible for managing access to ICT resources.

(8) All persons accessing University ICT resources should be aware of this document and implement the access controls for which they are responsible.

Section 5 - Requirements

Types of Accounts

(9) Table 1 describes account types and their use.

Type of Account	Description	Example
Standard user	Unique University-issued account assigned to staff and students to access University networks and resources. These accounts have standard permissions.	UniID, three letters and three number combination.
Privileged user (personal account)	Unique University-issued privileged account assigned to staff who perform system administration activities. This does not included non-IT staff who may be administrator of an application in their area.	Database, server, cloud, and domain administrator.
Local administrator	Privileged account that is created by default when an operating system is installed. The account sits outside the domain and has full control of the files, directories, services, and resources on the load device.	Default local user account on operating systems.
Service account or application account	An account used to run services and applications such as a file server, web server, e-mail server, etc., or used by applications to access databases and operating systems.	Init or inetd on Linux and Unix; LocalSystem, NetworkService on Windows; cloud service account.
Generic/shared administrative account	Generic privileged account that exists on most devices and software by default. These accounts holder 'super user' privileges and are often shared among University IT support staff.	Windows administrator, local admin, UNIX root, Orale SYS, AWS Root account, Azure Global admin
Break glass account	Generic administrative account used for emergencies. These accounts usually provide the highest level of privilege. This account is only used for emergencies or to fix urgent problems.	Like generic/shared accounts.

Access Management

(10) Clauses 11 to 17 outline the access management controls for access management that should be applied to all ICT resources.

(11) All decisions to grant, modify, or revoke a user's access to ICT resources should be recorded in the IT service management (ITSM) tool that is available on the University intranet.

(12) Access records should be retained for the life of the ICT Resource and in line with the Records Governance Policy to ensure access decisions can be traced.

(13) Approval must be sought prior to granting, modifying, or revoking access as follows:

a. for new students, approval must be sought from the Deputy Vice-Chancellor (Academic) as part of the enrolment process;
b. for new staff, approval must be sought from the Hiring Manager as part of the recruitment process; and
c. for affiliates, approval must be sought from the authorised University staff member within the business unit or School. Affiliates requiring access to University ICT resources must have an active University sponsor.

(14) All users must acknowledge the University's Information Technology Conditions of Use Policy prior to being granted access.

(15) Access to ICT resources must:

a. be role-based. This means that users should only be given access to the ICT resources they require to fulfil their role;
b. reflect the least privileges or permissions necessary to perform a role. Permissions may include the right to read, write, execute, or delete resources;

c. be based on a need-to-know. This includes access to data, information, and documents;
d. enforce the segregation of duties where there is a risk of fraud, errors, or conflicts of interest. Refer to Clause 78-79 for details;
e. be regularly reviewed by Information Owners and/or System Owners in the following cycles to ensure only persons with legitimate access requirements retain access:
    i. standard user access must be reviewed at least every 12 months;
    ii. privileged user access must be reviewed every 6 months. This includes generic, shared and root accounts; and
    iii. segregation of duties must be reviewed at least every 12 months;
f. be revoked on the day they are no longer required. This applies to terminated employees, transfers to other areas, and changes to roles and responsibilities.

(16) If a staff account is not accessed for 365 consecutive days, the account should be disabled on the 366th day.

(17) All accounts provided to affiliates must include an expiration date that reflects the period of their relationship with the University.

Technical Controls

(18) Clauses 19 to 32 outline the technical controls that should be applied to all ICT resources.

(19) Access to all ICT resources must be attributable to an individual by assigning a unique identity.

(20) Unique identities cannot be reused.

(21) Users must be authenticated using multifactor authentication (MFA) prior to being granted access ICT resources. A Security Exemption must be sought via the ITSM tool for systems that do not require MFA.

(22) If MFA cannot be used, users must be authenticated by a long passphrase that the meets length and complexity requirements in Clause 45.

(23) Where systems cannot support MFA, passphrases must be changed at least once every 365 days. If passphrase expiration cannot be enforced by the system, users must manually change their passphrase using the University's passphrase reset procedure.

(24) Default, generic and shared accounts should not be used except for break-glass scenarios or cloud tenant administration.

(25) Default and generic accounts should be renamed and disabled/removed (except for break-glass and cloud tenant administration).

(26) The use of generic and shared accounts for break-glass scenarios and cloud tenant administration, must be attributable to an individual.

(27) A separate privileged user account must be created for system administration.

(28) Non-privileged activities must be performed using a standard user account.

(29) Standard user accounts must not be used to run system services.

(30) Service accounts must not be shared between applications or services, i.e., a separate account must be created for each application and service.

(31) Standard users and administrators are not permitted to interactively log-in using service account credentials, except, as required to support or troubleshoot the specific service.

(32) All access to ICT resources must be logged and sent to the Security Operations Centre (SOC) for monitoring and analysis. Digital Technology Solutions (DTS) should be engaged to facilitate the configuration and sending of logs to the SOC.

Passphrases, Passcodes, and Multi-Factor Authentication

(33) Passphrases must be issued using secure means.

(34) First-use passphrases must be randomly generated.

(35) Passphrases must be changed by a user upon first login.

(36) Default passphrases on all systems, network resources, applications and databases must be immediately changed to a unique passphrase.

(37) Unique passphrases must be used for each system.

(38) Passphrases must not be shared i.e., known to more than one individual.

(39) User identities must be verified prior to resetting passphrases.

(40) The minimum age for passphrases should be 1 day or greater.

(41) Passphrases used for single-factor authentication must be a list of random words, with a minimum length of 14 characters.

(42) Passphrases should not contain any identification information or be the same as the last 10 passphrases.

(43) MFA should require the use of a passphrase and a universal 2nd Factor security key, software based one-time passphrase token, physical one-time token, biometric authentication, or SMS.

(44) Passphrases implemented as part of MFA must be at least 10 characters in length.

(45) Passphrases for generic, default, shared, local administrator and service accounts must be at least 20 characters in length.

(46) Passcodes for mobile phones must be at least 4 digits, or a biometric authentication with a passcode as a backup if the biometric fails.

(47) Passphrases and passcodes must not be written down or stored in plain text.

(48) If passphrase management software is used, the passphrase to access this software should be unique and meet the requirements of a local administrator/service account passphrase.

(49) Cloud-based passphrase management software should be used with MFA.

(50) If a passphrase has been shared with DTS for troubleshooting, the passphrase must be changed once the work is complete.

(51) If an account or passphrase is suspected to have been compromised, the incident must be reported to the 17000 IT Service Desk and the passphrase must be changed immediately.

Credential Protection

(52) Credentials (i.e., the combination of username and passphrase) must be kept separate from the systems that they are used to authenticate to.

(53) Credentials must be obscured as they are entered into systems to protect credentials from compromise.

(54) Credentials stored on systems must be protected by a passphrase manager, a hardware security module, or by adopting methods such as salting, hashing, and stretching them before storage.

(55) Windows Defender Credential Guard and Windows Defender Remote Credential Guard should be enabled where available to provide additional protection for credentials.

(56) Privileged user accounts in Windows should be placed in a Protected Users security group where available. This security group will apply non-configurable protections to privileged user's credentials.

(57) Service accounts for Windows servers should be created as group Managed Service Accounts. This feature provides automated credential management and ensures service account credentials are long, unique, unpredictable, and managed.

(58) Cached credentials should be limited to one previous logon to prevent the retrieval of cached credentials by an adversary.

Account Protection

(59) The following controls should be implemented for University accounts:

a. Account lockout threshold: 5 invalid logon attempts;
b. Account lockout duration: 15 minutes; and
c. Reset account lockout counter after: 15 minutes.

(60) Email alerts should be sent to users when a login is detected from a new device.

Break-Glass Accounts

(61) Passphrases for break-glass accounts should be machine-generated and held in the University's approved privileged access management (PAM) platform to ensure they are available to system administrators. DTS should be engaged for PAM use.

(62) A break-glass procedure must be created by the System Owner or Information Owner to define the roles, responsibilities, and process for using break glass accounts.

(63) If a break-glass account is used, access to the account must be:

a. limited to the minimum amount of time necessary;
b. associated to a change, problem, or incident number/ticket;
c. recorded by the specific database, system, or application; and
d. logged in an auditable record (which identifies the individual user who used the account), such as within the PAM platform.

(64) Passwords for break-glass accounts must be changed immediately after each time they are used.

Database Access

(65) User access, user queries, and user actions on databases should occur only through programmatic methods. Programmatic access refers to the use of a programming language to access a database, which provides more security than direct/manual access.

(66) Only database administrators should be able to directly access or query databases.

(67) Application IDs for database applications should only be used by the applications (and not by individual users or other non-application processes).

Simple Network Management Protocol (SNMP) Community Name Requirements

(68) SNMP version 1 should not be used to monitor network devices as the protocol versions are insecure.

(69) Default SNMP community strings on network devices should be changed and write access disabled.

(70) SNMP community strings must meet the requirements of a local administrator/service account password.

(71) SNMP community strings should be changed when someone leaves the University who would know or had used the password.

Secure Shell (SSH) Keys

(72) SSH version 1 should be disabled. Only SSH version 2 should be used.

(73) Public key-based authentication should be used for SSH connections.

(74) SSH private keys should be protected with a password or key encrypting key.

(75) When SSH-agent or similar key caching programs are used, the program should be limited to workstations and servers with screen locks and key caches should expire within 4 hours of inactivity.

(76) SSH daemon should be configured to:

a. only listen on the required interfaces;
b. have a login grace time of no more than 60 seconds;
c. host-based authentication should be disabled;
d. rhost-based authentication should be disabled;
e. the ability to login directly as root should be disabled;
f. empty passphrases should be disabled;
g. connection forwarding should be disabled;
h. gateway ports should be disabled; and
i. X11 forwarding should be disabled.

(77) When using logins without a password for SSH connections, the following should be disabled:

a. access from IP addresses that do not require access;
b. port forwarding;
c. agent credential forwarding;
d. X11 display remoting; and
e. console access.

Segregation of Duties

(78) System Owners and Information Owners are responsible for defining segregation of duties requirements and regularly reviewing the implementation of those requirements. In general, a person should not be both the requestor and approver of an action; a person should not be able to ‘mark their own work’; and a person should not perform actions that may present conflict of interest or enable fraud, e.g., making payments and reconciling bank statements. Additionally, no one person should be able to initiate a transaction, request and approve a transaction, record a transaction, reconcile balances, handle assets and review reports.

(79) The following controls should be implemented to restrict administrative and privileged accounts:

a. limit the role of System Administrator to the fewest number of individuals necessary to achieve adequate service;
b. implement granular permissions for the performance of privileged tasks;
c. separate System Administrator accounts from regular user accounts;
d. separate System Administrator functions from audit and logging functions. System Administrators must not have the ability to modify or de-activate logs of their own activities.

Exemption for Specialty Devices

(80) Due to the wide variety of specialty devices and their frequently limited capabilities, particularly regarding passphrase management, specialty devices such as fax machines, printers, physical access control equipment, copy machines, specialty lab equipment, phones, etc. are not subject to these requirements unless those devices are used to store or protect Highly Restricted information as defined by the University's Data Classification and Handling Policy and Standard or perform highly critical functions.

Status and Details

Status	Current
Effective Date	30th March 2023
Review Date	30th March 2026
Approval Authority	Chief Information Officer
Approval Date	20th March 2023
Expiry Date	Not Applicable
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Information Security Team

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"ICT resources" - All information and communication technology resources and facilities.

"Information Owner" - A senior business, college or unit manager whom the University has authorised to collect, create, retain and maintain information within their assigned area of control.

"School" - An organisational unit forming part of a College or Division, responsible for offering a particular course.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"System Owner" - An authorised individual who has been allocated responsibility by the University and is held accountable for an ICT resource.

"Affiliate" - A person or organisation legally obligated to, or informally associated with the University. Categories of affiliates are outlined on the University website.

"System Administrator" - An individual responsible for the installation and maintenance of an information system, providing effective information system utilisation, adequate security parameters, and sound implementation of established Information Security policy and procedures.