Information Security Access Control Policy

Section 1 - Executive Summary

(1) Digital assets owned, supplied or managed by the University and controlled entities include software, hardware, data, and networks. These digital assets are used by staff, students, affiliates, vendors, and members of the public.

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

(3) Most staff and students are standard users of digital assets, 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. This document provides controls for managing both standard and privileged access to digital assets.

(4) System Owners and Information Owners are responsible for determining access requirements for their digital assets and for ensuring that access is managed throughout the life of the digital asset 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 digital assets owned and/or managed by the University and controlled entities.

Section 4 - Audience

(7) This document should be read and understood by System Owners, Information Owners, System Administrators, technical staff, and any other staff responsible for managing access to digital assets.

(8) All persons accessing University digital assets 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.	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) Access to all digital assets must be managed as follows:

a. all decisions to grant, modify, or revoke a user's access to digital assets should be recorded in the service management tool that is available on the University intranet;
b. access records should be retained for the life of the digital asset and in line with the Records Governance Policy to ensure access decisions can be traced;
c. approval must be sought prior to granting, modifying, or revoking access as follows:
    i. for new students, approval must be sought from the Senior Deputy Vice-Chancellor (Academic) as part of the enrolment process;
    ii. for new staff, approval must be sought from the Hiring Manager as part of the recruitment process; and
    iii. for affiliates, approval must be sought from the authorised University staff member within the business unit or School. Affiliates requiring access to University digital assets must have an active University sponsor.
d. All users must acknowledge the University's Digital Technology Conditions of Use Policy prior to being granted access.
e. Access to digital assets must:
    i. be role-based. This means that users should only be given access to the digital assets they require to fulfil their role;
    ii. reflect the least privileges or permissions necessary to perform a role. Permissions may include the right to read, write, execute, or delete resources;
    iii. be based on a need-to-know. This includes access to data, information, and documents;
    iv. enforce the segregation of duties where there is a risk of fraud, errors, or conflicts of interest. Refer to Clause 77-78 for details;
    v. wherever possible, 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.

f. if a staff account is not accessed for 90 consecutive days, the account should be disabled on the 91st day.
g. All account provided to affiliates must include an expiration date that reflects the period of their relationship with the University.

Digital Access Reviews

(11) Digital Access Reviews ensure that security principles are adhered to, and that access which violates one or more of the principles is revoked or remediated. Security principles are detailed in the Digital Security Policy.

(12) Digital Access Reviews are an important governance tool used to provide auditable assurance that the University is exercising due diligence and care in the application of security principles and risk management.

(13) System Owners:

a. must ensure that access review procedures are completed within their required minimum review period as defined in Clause 15 and 16;
b. are required to produce and maintain access review procedures and documentation for the systems they are responsible and accountable. Specific requirements are listed in clause 17;
c. must record the authorisation, provision, and removal of access entitlements via the University's approved identity and access management tool;
d. may allocate the responsibility for functional completion of access reviews to designated security officers or subject matter experts; and
e. are responsible for producing reports to ensure access entitlement decisions and actions are readily available for audit.

(14) Failure to complete access reviews aligned with this standard places System Owners in non-compliance with the access control requirements, and subject to enforcement clauses in the Digital Security Policy.

(15) Access to systems must be regularly reviewed to ensure only persons with legitimate access requirements retain access and that security principles are adhered to. Minimum review periods are listed below:

a. Standard user access must be reviewed at least every 12 months.
b. Privileged user access must be reviewed at least every 3 months. This includes generic, shared, break glass, and root accounts.
c. Segregation of duties must be reviewed at least every 12 months.

(16) Access reviews must also be conducted immediately in the following scenarios:

a. User onboarding and offboarding, including access by third parties.
b. Changes in user role or responsibility.
c. Security breach or incident.
d. User misconduct.
e. Change in compliance legislation or regulation.
f. Changes to policy or governance settings.
g. Significant changes to infrastructure including growth, upgrades, and migrations.

(17) To support the repeatable nature and auditability of access reviews, System Owners should maintain the following knowledge resources:

a. List of systems/applications for which they are responsible.

b. Access review schedule information for each system, including the type and cadence of review.
c. A matrix of system roles and privileges.
d. Entitlement mapping documentation indicating relationships between system roles and identity provider security groups, or role/attribute-based access logic.
e. Toxic role combinations and fraud possibilities.
f. Procedures and workflows used to identify, evaluate, authorise, and remediate access entitlements.

Technical Access Controls

(18) The technical controls described in clauses 19-31 should be applied to all digital assets.

(19) Access to all digital assets must be attributable to an individual by assigning a unique identity. These unique identities cannot be shared or reused.

(20) Users must be authenticated using multifactor authentication (MFA) prior to being granted access to digital assets. A Security Exemption must be sought via the ITSM tool for systems that do not use MFA.

(21) If MFA cannot be used, users must be authenticated by a long passphrase that the meets length and complexity requirements in Clause 43.

(22) 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.

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

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

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

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

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

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

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

(30) 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.

(31) All access to digital assets 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

(32) Passphrases must be issued using secure means.

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

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

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

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

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

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

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

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

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

(42) 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 or biometric authentication.

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

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

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

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

(47) 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.

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

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

(50) 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

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

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

(53) 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.

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

(55) 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.

(56) 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.

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

Account Protection

(58) 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.

(59) Where possible, systems should generate logs and alerts on suspicious logins and be centrally monitored by the Cyber Security team.

Break-Glass Accounts

(60) 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.

(61) 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.

(62) 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.

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

Database Access

(64) 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.

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

(66) 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

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

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

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

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

Secure Shell (SSH) Keys

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

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

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

(74) 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.

(75) 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.

(76) 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

(77) 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.

(78) 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

(79) 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 Information Classification and Protection Policy or perform highly critical functions.

Status and Details

Status	Current
Effective Date	1st May 2025
Review Date	1st May 2028
Approval Authority	Chief Digital & Information Officer
Approval Date	28th April 2025
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.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Risk management" - The co-ordination of activities to optimise the management of potential opportunities and reduce the consequence or impact of adverse effects or events.

"Controlled entity" - Has the same meaning as in section 16A 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.

"Hiring Manager" - The staff member who is facilitating the recruitment on behalf of the School/Unit/Division/College. This is typically the supervisor of the vacant position. For sessional academic staff, this is typically the Head of School or their nominee.

"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.

"Digital asset" - Means all or any information technology solution(s) (regardless of whether they are physical or

software-based), and the facility(ies) that house them.