Information Security Access Control Manual

Section 1 - Introduction

(1) The University of Newcastle is committed to and is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems.

(2) The purpose of this manual is to define the minimum standards required to ensure that user access is based upon authentication and authorisation, and that unauthorised access to systems and services is prevented.

(3) It is the responsibility of all Information Owners and System Owners to determine appropriate access controls, access rights and restrictions for their information and information systems. They must assure that access is provided only to authorised users and that unauthorised access is prevented.

(4) Furthermore, it is important for all University staff, students, affiliates, contractors, volunteers or visitors using University ICT resources to understand the need to ensure appropriate authorisation to any system or service provided by the University.

Section 2 - Scope

(5) The minimum standards outlined in this manual apply to all University ICT services and systems.

Section 3 - Audience

(6) These standards are primarily aimed at system administrators and technical staff, including Digital Technology Solutions staff, who are responsible for the management of access controls for University ICT services and systems. This includes third parties supporting University of Newcastle IT systems.

Section 4 - Requirements

User Registration

(7) A formal user registration and de-registration process should be implemented to enable assignment of access rights.

(8) The following control objectives must be covered in the design of user registration procedures:

a. the allocation of unique user identities;
b. all University accounts must be accountable to an individual (e.g. no shared or generic accounts).
c. obtaining appropriate authorisation prior account creation;
    i. for students, authorisation is provided by the DVC(A) as part of the enrolment process.
    ii. for staff, authorisation is provided by the hiring manager as part of the recruitment process.
    iii. for affiliates, authorisation is provided by an authorised University staff member within the unit or school.

d. preserving segregation of duties;
e. user acknowledgement of the policy regarding acceptable use, outlined in the Information Technology Conditions of Use Policy;
f. no reissuing of user identities to new users.

(9) All third parties requiring access to University information assets must have an active University sponsor. All user accounts provided to third parties must include an expiration date no greater than one (1) year from the date the access is granted.

User Access Provisioning

(10) Access privileges are to be assigned through the use of the Role-Based Access Control (RBAC) model.

(11) RBAC is an access control mechanism that permits system administrators to allow or disallow other user's access to objects under their control.

(12) The "role" in RBAC refers to a system of user roles, which are assigned to user groups and their users. Roles are assigned permissions, which define what a user can or can't do within a system or on an object. Roles can be particular to an application or may be defined more broadly as a job function or user type within the University, and may be a superset of more granular roles.

(13) Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed. This type of access simplifies management of privileges and permissions.

(14) The following RBAC implementation standards apply:

a. a user can only have access to an object (i.e dataset) based on an assigned role;
b. roles are to be defined based on a persona or job function. A persona is a profile that can be used to describe a type of user, e.g. student, staff, Researcher, guest;
c. permissions are defined based on role's authority, and responsibilities within a job function or of a persona;
d. operations on an object, such as view, edit or delete, are invoked based on permissions assigned to a role;
e. permissions configured on objects should only be based on roles, and not users;
f. roles are designed and implemented based on the principle of least privileged;
g. a role contains only the minimum amount of permissions required;
h. a user's account is assigned to a role that allows him or her to perform only what is required for that role.

Privilege Management

(15) All access privileges will adhere to the following principles:

a. Need to know – the legitimate requirement of a person to know, access, or possess sensitive information that is critical to the performance of the authorised job function.
b. Least Privilege – every user and program must operate using the least set of privileges necessary to complete the authorised job function.
c. Segregation of duties – the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.

(16) Need to know is enforced through the User Access Provisioning process.

(17) Least privilege and segregation of duties are achieved by:

a. limiting the role of system administrator to the fewest number of individuals necessary to achieve adequate service;
b. implementing fine grain access privileges for the performance of privilege tasks;
c. separating system administrator accounts from regular user accounts;
d. separating 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.

(18) In addition to various regular end-user roles, programmers, developers and testers will have separate roles with different privileges to system administrator roles.

Review of User Access

(19) University information asset and IT asset owners must review user access rights on a regular basis to ensure that role changes, such as promotion, demotion, transfer, and termination are correctly reflected in all information systems under their management.

Removal or Adjustment of Access Rights

(20) The access rights of all users to information and information processing facilities shall be removed upon termination of employment, contract or association with the University, or adjusted upon change.

Passwords

(21) Username and passwords are used to facilitate authorised access to University information assets. These credentials are intended to protect data from unauthorised access and ensure that only authorised users have access.

(22) All initial system and application passwords must be issued by University staff through a secure means. Once a password has been issued, full responsibility for that account and associated password is transferred to the user. On first login all initial passwords will need to be changed, this will be an automated enforcement mechanism configured for all systems and applications to which users are being granted access.

Password Requirements

(23) All passwords, including initial passwords, must be constructed and implemented according to the following rules:

a. passwords must be at least 10 characters in length;
b. passwords must include at least one uppercase and one lowercase letter, one number, and one special character (i.e %,!,* or similar). All American Standard Code for Information Interchange (ASCII) and Unicode characters should be made available for use in a password;
c. passwords must not contain any user identifier, student identifier, or any part of the user's name;
d. passwords that are the same as the last 10 passwords that have been used must not be re-used;
e. passwords must not contain common or banned words, i.e. those known to be commonly-used, expected, or compromised, e.g.:
    i. passwords obtained from previous breach corpuses, i.e. passwords known to be compromised; or
    ii. repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd').

Password Protection

(24) The following user account controls must be enforced for all systems:

a. account lockout threshold: 5 invalid logon attempts.
b. account lockout duration: 15 minutes.

c. reset count lockout counter after: 15 minutes.
d. minimum password age: 1 day.
e. if a staff account is not accessed for 365 consecutive days, the account should be disabled on the 366th day.
f. users must be forced to change their password if their credentials are known or suspected to be compromised.
g. email alerts should be sent to users when a login is detected from a new device.

(25) In the event that a password has been shared with Digital Technology Solutions for troubleshooting scenarios, the password must be immediately changed after this work is complete.

(26) In the event that an account or password is suspected to have been compromised, the incident must be reported to the 17000 IT Service Desk and the password must be changed immediately.

Mobile Device Passwords

(27) All smart devices containing University data (including email) must be secured with either:

a. a 4-digit PIN; or
b. a Biometric lock with a compliant backup password/PIN.

Privileged Accounts

(28) The following clauses apply to all privileged accounts created for University owned or managed systems, including but not limited to:

a. Privileged Personal Accounts - privileged accounts assigned to individual users (typically University IT Support Staff). Examples include the following privileged groups: DBA, Server Administrator, Tenant Admin, Domain Admins.
b. Generic/Shared Administrative Accounts - privileged accounts that exist in virtually every device or software application. These accounts hold “super user” privileges and are often shared among University IT Support staff. These accounts may be used by multiple users. Examples: Windows Administrator, UNIX root, Oracle SYS, SA.
c. Break Glass (Emergency) Accounts – break glass accounts are a type of Generic/Shared Administrative Account used by the University when elevated privileges are required for business continuity, disaster recovery, or to fix urgent problems.
d. Service Accounts – these are privileged accounts that provide a security context to a running service, daemon or process, such as a file server, web server, e-mail server, etc., or are used by applications to access databases and other applications.

(29) Privileged accounts provide a high degree of access to University ICT resources and therefore pose a significant risk if used in an unauthorised manner.

(30) As privileged accounts provide a significant level of control over University ICT resources, individuals with access to these accounts are expected to exercise a high degree of caution.

(31) All users with access to privileged accounts must maintain the confidentiality of any information that they have access to both during and after their employment with the University.

Privileged Account Password Requirements

(32) Privileged user access to any of the University's ICT domains, services and systems must be authenticated using multi-factor authentication (MFA) unless there is a system limitation that prevents its use. Privileged credentials must

only be used when performing tasks that specifically require those privileges. While performing normal activities, administrators must use a separate, unprivileged account.

(33) All privileged account passwords, including initial passwords, must be constructed and implemented according to the following rules:

a. password length – the password must be at least 14 characters long;
b. password complexity – the password must include one uppercase and one lowercase character, one number and one special character (i.e %,!,* or similar);
c. password attributes – the password must not contain a user identifier or any part of the account owner's name;
d. password history – passwords that are the same as the last 24 passwords that have been used must not be re-used;
e. password expiry – passwords must be changed immediately when a staff member who has accessed that password leaves their employment with the University;
f. minimum password age – 1 day;
g. account lockout threshold – 5 invalid logon attempts;
h. account lockout duration – 15 minutes;
i. reset account lockout counter after 15 minutes;
j. group or shared passwords are prohibited (unless an exception is approved). The only exceptions to this are
    i. 'break-glass' accounts, which must not be used for day-to-day support;
    ii. 'test' accounts, which may be shared during pre-production phases;
k. default passwords of any system, network resource, application or database etc., must be changed either during the installation process or immediately thereafter.

Break-Glass Accounts

(34) Passwords for break-glass accounts should be machine generated and held in the University's approved Privileged Account Management (PAM) platform to ensure they remain available to system administrators.

(35) A break-glass procedure defining the roles and responsibilities for use of break glass accounts should be created by each relevant System Owner or Information Owner.

(36) When a break-glass account is used, access to the privileged 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 'broke the glass'), such as within the PAM platform, for later review.

(37) After a break-glass procedure has been completed, the password for the break glass account must be changed.

Password Expiry and Multi-Factor Authentication (MFA)

(38) If a Uni-ID or privileged account is protected with MFA, then there is no requirement to expire the associated password.

(39) If a Uni-ID or privileged account is not protected with MFA, then the requirement for password expiry will be based on the data classification that a Uni-ID is authorised to access based on the roles that it has been assigned:

Data Classification available to Uni-ID or privileged account	Password Expiry
Highly-Restricted	Password must expire every 365 days
Restricted	Password should be changed every 365 days
X-in-confidence	No password expiry
Public	N/A – No authentication required

Specialty Devices

(40) Due to the wide variety of specialty devices and their frequently limited capabilities, particularly with regard to password 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 or perform highly critical functions.

Service Account and Simple Network Management Protocol (SNMP) Community Name Requirements

(41) The password length and complexity requirements for service accounts and SNMP community names are increased to allow for less frequent expiration. This ensures that key services are not disrupted due to regular change.

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

(43) Using a standard user account or Uni-ID to run system services is prohibited.

(44) End users and administrators are not permitted to remotely or interactively log in using service account credentials except as required to support or troubleshoot the specific service:

a. password and SNMP community name length – must be a minimum of 15 characters long;
b. password and SNMP community name complexity – must include at least one uppercase and one lowercase character, one number and one special character (i.e %,!,* or similar);
c. password and SNMP community name attributes – must not contain a user identifier or any part of a name;
d. password and SNMP community name reuse – must not be use passwords or community names that are identical or substantially similar to those that have been previously used;
e. password expiry – generally never, but the password must be changed when someone leaves the University who would know or had used the password.

Secure Shell (SSH) Keys

(45) SSH keys are a common way to connect to Unix\Linux based computers. Whilst they can provide a convenient and secure means of connection, the University does not currently have appropriate processes to ensure the security of their use across a user's lifecycle at the University, e.g. SSH keys may not be reliably disabled when a user leaves the University.

(46) As such, the use of SSH keys for authentication is prohibited.

Password Management Software

(47) Passwords must not be written down or stored in clear text, although password management software may be used. Special care should be taken to secure the password tool, as it will grant access to all passwords.

(48) The password manager tool must employ encryption at AES256 or SHA2 or stronger. The password used to access this application must also be very strong and unique, and meet the requirements of a Service Account Password.

(49) Use of cloud-based password management tools is forbidden unless MFA is used.

Status and Details

Status	Historic
Effective Date	18th June 2019
Review Date	18th June 2021
Approval Authority	Chief Information Officer
Approval Date	17th June 2019
Expiry Date	29th March 2023
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.

"Asset" - Any tangible or intangible item (or group of items) that the University owns or has a legal or other right to control and exploit to obtain financial or other economic benefits.

"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.

"Program" - When referring to learning, a program is a sequence of approved learning, usually leading to an Award. For all other uses of this term, the generic definition applies.

"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.