Information Security Access Control Procedure

Section 1 - Procedure

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 procedure is to establish the University's obligation to ensure that user access is based upon authorisation and that unauthorised access to systems and services is prevented.

Scope

(3) It is the responsibility of all Information owners and System Owners to determine appropriate controls, rules, 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 - Requirements

User Registration

(5) Through formal procedures, ensure that access control rules are reflected in the user registration process. The following control objectives must be covered in the design of these procedures:

a. allocation of unique user identities;
b. All University accounts must be accountable to an individual (e.g. no shared or generic accounts).
c. obtaining System Owner's or Information owner's authority prior to access;
d. preserving segregation of duties;
e. user’s acknowledgement of the rules regarding acceptable use;
f. no reissuing of user identities to new users.

(6) All third parties requiring access to University information assets must have an active University Sponsor. These accounts must include an accurate expiration date no greater than 1 year from the date the access is granted.

User Access Provisioning

(7) The minimum standards for access privileges are to be achieved through the user of the Role-Based Access control (RBAC) model. RBAC is an access control mechanism that permits system administrators to allow or disallow other

user's access to objects under their control. Users can be easily reassigned from one role to another. 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 greatly simplifies management of privileges and permissions.

(8) The following RBAC implementation standards apply:

a. A user can only access to an object (i.e dataset) based on an assigned role.
b. Roles are to be defined based on job functions.
c. Permissions are to be defined based on role authority and responsibilities within a job function.
d. Operations on an object are invoked based on the role permissions.
e. The object is only to be concerned with the user's role and not the user.
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 account is assigned to a role that allows it to perform only what is required for that role.
i. No single role is given more permission than the same role for another user.

Privilege Management

(9) 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. Separation 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.

(10) The need to know is enforced through the account authorisation process and establishment. The least privileges and separation 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.

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

Review of User Access

(12) University information asset and IT asset owners must review user access rights on a regular bass 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

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

Passwords

(14) 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.

(15) 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 by for all systems and applications to which users are being granted access.

Password Requirements

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

a. Passwords must be changed every 365 days for all users.
b. Passwords must be between 8 and 16 characters (inclusive) in length.
c. Passwords must include at least one uppercase and one lowercase letter, one number, and one special character (i.e %,!,* or similar).
d. Passwords must not contain any user ID, student ID, or any part of the user's name.
e. Passwords that are the same or substantially similar to the last 10 passwords that have been used earlier must not be used.

Password Protection

(17) 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 Account Lockout Counter After: 15 minutes.
d. Minimum Password Age: 1 day.
e. If a staff account is not accessed for 90 consecutive days, the account must be disabled on the 91st day.

(18) In the event that a password has been shared with IT Services for troubleshooting scenarios, the password must be immediately changed after this work is complete.

(19) 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

(20) 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 Account Passwords

(21) This applies to all privileged accounts created for University owned or managed systems, including but not limited to:

a. Domain Admin Accounts

b. Server Administrator Accounts
c. Application Administrator Accounts
d. Database Administrator Accounts
e. Network Devices management and monitoring accounts
f. Service accounts
g. Local Administrator Accounts
h. Super user accounts
i. SNMP community name strings
j. Contractors, vendors and other third parties managing University ICT services and systems.

Administrative User Password Requirements

(22) Privileged user access to any of the University's ICT domains, services and systems must be authenticated using at least single factor authentication. Where multi-factor authentication is available, privileged user access must use two factor authentication. Administrators must only use privileged credentials when performing tasks that specifically require those privileges. While performing normal activities, administrators must use a separate, unprivileged account.

a. Password length – the password must be between 10 and 20 characters long (inclusive).
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 ID or any part of the account owner's name.
d. Password history – passwords that are identical or substantially similar to passwords that have been previously used must not be re-used.
e. Password expiry – passwords must be changed every 90 days or immediately when a staff member with privileged access leaves.
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).
k. Default passwords of any system, network resources, application or database etc., must be changed either during the installation process or immediately thereafter.

Specialty Devices

(23) 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 Network Infrastructure Passwords & SNMP Community Name Requirements

(24) 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.

(25) Service accounts specifically created for services / applications must be used only for system services. Using a standard user account to run system services is prohibited. End users and administrators are not permitted to remotely or interactively log in using service account credentials except as required for supporting the specific

service. Systems and devices must be configured to prevent remote login using service accounts wherever technically feasible.

a. Password and Community Name Length – Must be a minimum of 15 characters long (inclusive).
b. Password and 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 Community Name Attributes – Must not contain a user ID or any part of a nma.e
d. Password and 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 organisation who would know the password, e.g. Networking devices local administrative account passwords.
f. Interactive Login – Service accounts must not allow interactive login to systems.

Password Management Software

(26) 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.

(27) 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.

(28) Use of Cloud based Password Management Tools is forbidden unless multifactor authentication is used.

Status and Details

Status	Historic
Effective Date	31st March 2017
Review Date	1st July 2018
Approval Authority	Chief Information Officer
Approval Date	24th May 2018
Expiry Date	17th June 2019
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.

"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.

"Establishment" - When referring to an Award offered by the University, establishment means the process of approving an award that the University has decided to offer. For all other uses of this term, the generic definition applies.

"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.

"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.