Personnel Security Policy and Standard

Section 1 - Executive Summary

(1) To protect the University's ICT resources and data from compromise, the University must ensure that the users of those resources and data can be trusted. This requires screening employees prior to employment and continually informing employees on the secure and appropriate use of University assets.

(2) Access to the University's ICT resources and data must also be managed to ensure only current employees have access, access is role-based, and to revoke access upon changes to employment.

(3) Terminated employees and employees changing positions must also be notified of their obligation to protect the information gained during their employment at the University.

Section 2 - Purpose

(4) This document articulates the personnel security controls that must be applied to the access and use of the University's ICT resources and data.

Section 3 - Scope

(5) This policy is applicable to all employees of the University. In the context of this document, an employee is anyone who is engaged by the University to provide a service to the University regardless of the job function, including:

a. full-time, part-time and casual staff;
b. contractors and third party users; and
c. volunteers.

Section 4 - Personnel Security Requirements

Prior to Employment

(6) Digital Technology Solutions (DTS) must assign a risk designation to all positions. The risk designation should reflect the position level, level of access to systems, and access to classified information.

(7) Human Resource Services must determine screening requirements for individuals filling positions.

(8) Screening criteria must reflect applicable federal and state laws, directives, policies, standards, and specific criteria established for the risk designations of assigned positions.

(9) Human Resource Services and/or the hiring business unit must screen individuals prior to offering employment at the University.

(10) The security responsibilities of each position must be documented in job descriptions and within the terms and

conditions of employment.

During Employment

(11) All employees must undergo an orientation process and be provided with access to security policies and procedures.

(12) All employees must acknowledge that they have read and understood the University's Information Technology Conditions of Use Policy.

(13) All employees must complete the University's Information Security Awareness Training within the first three (3) months of employment and annually thereafter.

(14) Managers and supervisors should provide briefings to employees on the secure and appropriate use of ICT resources and data prior to granting access.

Termination of Employment

(15) Each business unit must assign responsibilities for performing employee terminations.

(16) The Separations and Transfers Checklist must be completed for terminated employees.

(17) University property must be returned on the last day of employment. This includes but is not limited to laptops, identification cards and building passes.

(18) Access to all systems and data must be revoked on the last day of employment.

(19) Managers and supervisors must perform exit interviews to ensure terminated employees understand their responsibility to protect information gained during their employment at the University.

Changes to Roles

(20) Each business unit must review and confirm the ongoing need for logical and physical access to ICT resources and data when individuals are reassigned or transferred to other positions.

(21) Each business unit must ensure that access to ICT resources and data is revoked on the last day of that individual filling a position within their department.

Contractors and Vendors

(22) Contractors and vendors must immediately notify the University of any terminations or transfers of personnel who possess credentials, building passes, or have information system privileges.

Section 5 - Roles and Responsibilities

Responsibilities of all Employees

(23) All employees must:

a. participate in annual security awareness training;
b. read and action advice from the Information Security Team;
c. understand and abide by the University's Information Technology Conditions of Use Policy and their associated documents;

d. follow established processes and procedures to maintain system and information security;
e. consult managers and supervisors for guidance on security issues; and
f. consider security implications when making changes to ICT resources and information assets.

(24) All employees must pay attention to:

a. legislation and policy related to information security; and
b. University communications relating to information security.

(25) All employees must report:

a. actions or activities which could circumvent or impair security controls; and
b. actual and suspected security incidents.

Responsibilities of Management

(26) All managers must:

a. ensure information security requirements are included in job descriptions;
b. ensure required pre-employment checks are completed for all new employees;
c. prior to granting access to systems and resources, provide any necessary briefings;
d. when assigning work, ensure employees are aware of security requirements;
e. consult the Information Security Team for guidance on security issues;
f. understand and abide by the University's Information Technology Conditions of Use Policy and their associated documents;
g. support security awareness training and events;
h. if a security breach occurs, review and revise related operating procedures as needed; and
i. inform departing employees of their continued obligation to protect sensitive information gained during their employment at the University.

(27) All managers must establish:

a. procedures for orienting new employees;
b. procedures for reviewing system access for employees when roles or employment status changes occur; and
c. develop standard operating procedures for system use.

(28) All managers must monitor:

a. employees to ensure they support and follow security processes and practices.

(29) All managers must report:

a. actual or suspected breaches of information security by contacting the Information Security Team.

(30) All managers must reinforce with employees:

a. the importance of understanding policies, adhering to standards, and following approved processes for the protection of information; and
b. that everyone has a role in securing information resources.

Status and Details

Status	Current
Effective Date	8th December 2022
Review Date	8th December 2025
Approval Authority	Chief Information Officer
Approval Date	5th December 2022
Expiry Date	Not Applicable
Responsible Executive	Anthony Molinia Chief Digital & Information Officer +61 49138713
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.

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

"Information asset" - A body of information, knowledge or data that is organised as a single entity and has value to the University.

"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.

"Third party" - A person or group other than the University or any of the University's partner institutions.