Information Security Human Resource Guidelines

Section 1 - Executive Summary

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

(2) All users interacting with information assets have a responsibility to ensure the security of those assets.

(3) The University must perform checks to ensure that each individual user is suitable to be given access to the University's ICT systems and the information held on these systems.

(4) Users must be trained, equipped and periodically reminded to use information securely.

(5) When employment ends with the University, respective user access must be suspended or removed from ICT systems.

(6) Where a user's role changes, the user's information access privileges must be reviewed and changed accordingly on a 'least privilege' basis.

Section 2 - Purpose

(7) The intent of this guideline is to govern the human resources aspect of information security for employees of the University.

Section 3 - Scope

(8) For the purpose of this guideline, an employee of the University is anyone who is engaged by the University to provide 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 - Guidelines

Prior to Employment

Objective: To develop a comprehensive process that includes identification of job roles and responsibilities, identify the appropriate candidate screening level for those roles and responsibilities, and to establish terms and conditions of employment.

(9) Prior to hiring or contracting staff or contractors, security roles and responsibilities should be clearly articulated in

job descriptions or well defined in terms and conditions of employment.

(10) For roles where handling of restricted or high-restricted information, or where access to sensitive ICT systems is required, careful attention should be paid to validation of references and the appropriate level of background checks.

During Employment

Objective: To ensure that employees are aware of and understand their information security roles and responsibilities; to ensure that they understand information security risks, and to ensure they have the necessary knowledge to mitigate those threats.

(11) All new employees should participate in new employee orientation and be provided with pertinent information including security policies and procedures, and the potential disciplinary process and actions for any security breaches.

(12) New employees must be required to acknowledge that they have read and understand the University's Information Technology Conditions of Use Policy.

(13) All managers and supervisors must emphasise the importance of information security to their employees.

(14) All employees must complete the University's Information Security Awareness Training within the first six (6) months of employment, which is available in Discover. The training should be completed again annually thereafter.

Termination and Change of Employment

Objective: To develop an orderly exit process to ensure that access to University systems is removed, and assets returned, in an expedited timeframe.

(15) Responsibilities for performing employee terminations must be clearly defined and assigned to ensure actions are taken within the prescribed timeframes.

(16) A checklist of actions to be taken and the person responsible for the execution of each action allows for quick identification of any missed steps. Please see Separations and Transfer checklist.

(17) Specifically, University assets must be returned on the termination of employment.

(18) Additionally, access to information assets must be removed at the termination of employment.

Section 5 - Roles and Responsibilities

Responsibilities of all Employees

(19) Things to do:

a. participate in security awareness training and events;
b. understand and abide by the University's Information Technology Conditions of Use Policy and Information Security Policy;
c. follow established processes and procedures to maintain system and information security;
d. consult managers and supervisors for guidance on security issues; and
e. consider security implications when making changes that involve information assets.

(20) Things to avoid:

a. not asking for clarification or direction when unsure about information security requirements.

(21) Things to pay attention to:

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

(22) Things to report:

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

Responsibilities of Management

(23) Things to do:

a. ensure information security requirements are included in job descriptions;
b. ensure required pre-employment checks are completed for all new employees;
c. when assigning work, ensure employees are aware of security requirements;
d. consult the Information Security Team for guidance on security issues;
e. understand and abide by the University's Information Technology Conditions of Use Policy and Information Security Policy;
f. support security awareness training and events; and
g. if a security breach occurs, review and revise related operating procedures as needed.

(24) Things to pay attention to:

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

(25) Things to establish procedures for:

a. orientation programs for new employees;
b. reviewing system access for employees when employment status changes occur; and
c. Standard Operating Procedures for system use.

(26) Things to monitor:

a. that employees support and follow security processes and practices.

(27) Things to report:

a. promptly contact Information Technology Services when actual or suspected breaches of privacy or information security occur.

(28) Things to reinforce with employees:

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

Status and Details

Status	Historic
Effective Date	17th June 2019
Review Date	17th June 2021
Approval Authority	Chief Information Officer
Approval Date	17th June 2019
Expiry Date	7th December 2022
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.

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

"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.

"Supervisor" - Staff members with direct supervisory responsibility for other staff within the workplace (a Supervisor may also be member of Senior Management, with duties as an Officer as defined in the Work Health and Safety Act 2011, or any replacing legislation).

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