Information Security Human Resource Guidelines

Section 1 - Guidelines

Executive Summary

(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) 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 the individual user is suitable for 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 there is a change in role for a user, the information access privileges must be reviewed and changed accordingly on a 'least privilege' basis.

Purpose

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

Scope

(8) For the purpose of this guideline, Employees 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.

Prior to Employment

Objective

(9) To develop a comprehensive process that includes identification of job roles and responsibilities, identify the corresponding candidate screening level for those roles and responsibilities and establish terms and conditions of employment.

(10) Prior to hiring or contracting employees or companies, security roles and responsibilities should be clearly articulated in job descriptions or well defined in terms and conditions of employment.

(11) For roles involving handling of restricted or high-restricted information or access to sensitive ICT systems careful attention should be paid to validation of references and the appropriate level of background checks as determined by the security roles and responsibilities of the position or contract.

(12) Consideration should be given that the receipt of affirmative references and the successful completion of a background check at a level commensurate with the position's roles and responsibilities be a condition of employment.

During Employment

Objective

(13) To ensure that employees are aware of and understand their roles and responsibilities; to ensure that they understand information security threats and; to ensure they have the necessary knowledge to mitigate those threats.

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

(15) New employees should be required to acknowledge that they read and understand the University's Information Technology Conditions of Use Policy. All managers and supervisors should be expected to emphasize the importance of information security to their employees.

(16) All employees must complete Information Security Awareness Training annually on basic information security practices and acknowledge their understanding of the institution's security policies and procedures.

Termination and Change of Employment

Objective

(17) To develop an orderly exit process to ensure that access is removed and assets returned in an expedited time frame.

(18) Responsibilities for performing employee terminations must be clearly defined and assigned to ensure actions are taken as quickly as possible. A checklist listing actions to be taken and the person responsible for the execution of that action allows for quick identification of any missed steps.

(19) Specifically, there should be a process that validates that all institution's assets are returned at termination.

(20) Additionally, there should be a process that ensures access to information assets are removed at the time of termination.

Section 2 - Roles and Responsibilities

Responsibilities of all Employees

(21) Things to do:

a. Participate in security and privacy awareness training and events.
b. Understand and abide by the Conditions of Use Policy and Information Security Policy.
c. Follow established processes and policies to maintain security and privacy.
d. Consult Managers or Team Leaders for guidance on security or privacy issues.
e. When assigning work, ensure staff are aware of security requirements.
f. Consider security implication when making changes which involve information resources.

(22) Things to avoid:

a. Not asking for clarification or direction when unsure about information security, privacy and records management requirements.

(23) Things to pay attention to:

a. Security is everyone's responsibility
b. Security and privacy requirements in job descriptions.

(24) Things to report:

a. Actions or activities which could circumvent or impair security processes.
b. Actual and suspected security incident and events as required by the Information Security Incident Management Guidelines.

Responsibilities of Management

(25) Things to do:

a. Ensure information security requirements are included in job descriptions.
b. Consult the IT services, IT Security Team for guidance on security issues.
c. Understand and abide by the University Conditions of Use Policy.
d. Support security awareness and privacy awareness training and events.
e. Ensure required pre-employment checks are completed for all new staff.
f. Ensure staff are aware of security, privacy and records management requirements.
g. When a security or privacy breach has occurred, review and revise related operating procedures as needed.

(26) Things to pay attention to:

a. Legislation and policy related to privacy, security and records management

(27) Things to establish procedures for:

a. Orientation programs for new staff
b. Reviewing access rights of staff when employment status changes occur

(28) Things to monitor:

a. That staff support and follow security, privacy and records management processes.

(29) Things to report:

a. Promptly contact IT services when actual or suspected breaches of privacy or information security occur.

(30) Things to reinforce with staff:

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	31st March 2017
Review Date	1st July 2018
Approval Authority	Chief Information Officer
Approval Date	30th May 2018
Expiry Date	16th June 2019
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.

"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.

"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).

"Term" - When referring to an academic period, term means a period of time aligned to an academic year for the delivery of a course in which students enrol and for which they are usually charged fees for example semesters, trimesters, summer, winter or full-year term. The academic year for a term is determined by the academic year in which the course commences, not concludes. For all other uses of this term, the generic definition applies.

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