Australian National University

Position Description

College/Division:	Information Technology Services
Faculty/School/Centre:	
Department/Unit:	Cyber & Digital Security
Position Title:	Information Security Specialist
Classification:	ANU Officer Grade 8 (IT)
Position No:	TBA
Responsible to:	Manager, Cyber & Digital Security
Number of positions that report to this role:	0
Delegation(s) Assigned:	

ANU Officer Grade 8 (IT)

PURPOSE STATEMENT:

The IT Security Specialist assists in the management of the University's information security program, including responding to security incidents; undertaking risk assessment and management; advising on policies and procedures; and the development, implementation, and operation of security management systems.

KEY ACCOUNTABILITY AREAS:

Position Dimension & Relationships:

Under the broad direction of the Manager, Cyber & Digital Security, assist in the operation of the University's Information Security program.

Role Statement:

1. Work with senior technical staff across the University to plan, develop and maintain a secure University-wide information infrastructure.
2. Assist with the audit and assessment of university systems and processes to ensure ongoing security and compliance.
3. Assist in the oversight of the ANU information security strategy, including the coordination between security policy and business area security requirements.
4. Manage IT security incidents to ensure a consistent and coordinated University-wide response.
5. Assist with user education and maintenance of security documentation and publications.
6. Maintain specialist and technical knowledge across the Information Security sector and ensure appropriate processes and strategies are being implemented within the University.
7. Other duties as consistent with the classification of the level.

SELECTION CRITERIA:

1. Demonstrated ability to assist in the implementation of programs to protect large and complex environments against physical, network and system-level threats.
2. Proven ability to undertake IT security, risk and threat assessment audits of networks and systems, including the development of appropriate treatment plans.
3. Demonstrated experience in the development of technical, policy and awareness materials to ensure that business security requirements are addressed.
4. Demonstrated commitment to working effectively as a team member with the ability to work independently under minimal supervision, and to organise work priorities to meet competing deadlines.
5. Proven ability to develop and deliver training programs to support security knowledge and awareness.
6. Demonstrated high level interpersonal and communication skills, both written and oral, including the ability to liaise effectively with technical experts, business managers, users and service providers.
7. A demonstrated high-level understanding of equal opportunity principles and a commitment to the application of EO policies in a university context.

Delegate Signature:		**Date:**	
Printed Name:		**Position:**	

References:

General Staff Classification Descriptors

Academic Minimum Standards