**Australian National University**

# Position Description

| College/Division: | Services Portfolio |
|---|---|
| Faculty/School/Centre: | Chief Information Security Office |
| Department/Unit: | Cyber Engineering |
| Position Title: | Junior Information Security Engineer |
| Classification: | ANU Officer 5/6 (Information Technology) |
| Position No: | 41637 |
| Responsible to: | Manager, Cyber Engineering |
| Number of positions that report to this role: | 0 |
| Delegation(s) Assigned: | 0 |

## PURPOSE STATEMENT:

The ANU embraces global connectivity, cooperation and the sharing of ground-breaking research, but it also finds itself operating in and navigating through an increasingly complex and intricate threat landscape. The Information Security Office plays a critical role in leading and operating the ANU's capabilities for the protection of the information and information and communication technology systems within the digital and non-digital information eco-systems.

A Junior Information Security Engineer is accountable for performing and achieving cyber and information security tasks within an integrated and multidisciplinary workforce to assist in fulfilling the Information Security Office's mission areas.

## KEY ACCOUNTABILITY AREAS:

### Position Dimension & Relationships:

Under the direction of an Information Security Engineer or Senior Information Security Engineer, and more broadly under the Manager, Cyber Engineering, and in coordination with a range of stakeholders internally and externally the Junior Information Security Engineer is at the forefront of protecting and fortifying ANU information and cyber infrastructure. The Junior Information Security Engineer contributes to the development, implementation and operation of a range of system and network assets within the ANU Information Infrastructure.

This role requires a technical background and a proactive approach to addressing complex security challenges.

The role involves maintaining strong relationships with a network of diverse stakeholders both internally and externally, and liaising on a range of complex and sensitive information and cyber security issues and working towards team outcomes.

### Role Statement:

Outline principal tasks and/or duties in no more than 8 – 10 points.

- Assist with the deployment and management of a diverse set of cybersecurity tools and technologies to address sophisticated information and cyber threats effectively.
- Assist in the analysis and review of cyber and information security activities and data to proactively identify and mitigate security vulnerabilities.
- Assist in the audit and review processes of ANU information systems to ensure compliance with security regulations and best practices.
- Assist with the Communication of complex cybersecurity concepts in a clear and understandable manner through presentations, consultations, and reports for both technical and non-technical audiences.
- Provide guidance and assistance to stakeholders on cybersecurity matters, and assist in reviewing and reporting on adherence to established policies and standards. Participate in a collaborative team

environment by encouraging knowledge sharing, skill development, and positive contributions to team and group outcomes.

- Stay updated on emerging cybersecurity trends and technological advancements to maintain a cutting-edge understanding of the field.
- Undertake other duties as required from time to time consistent with the classification level of the position and aligned with the mission of the Information Security Office.
- Comply with all ANU policies and procedures, and in particular those relating to work health and safety and equal opportunity

## SELECTION CRITERIA:

1. Possess a degree qualification or be progressing towards one in computer science, computer engineering, information technology, cyber security, data science, or a relevant field. Alternatively, demonstrate an equivalent combination of experience and education/training.
2. Practical experience in at least one of the following IT areas: information security, system administration (Windows/Linux/MacOS), network administration, cyber security monitoring, incident response.
3. Possess knowledge, familiarity, experience, or industry qualifications in one or more of the following areas: cyber security, information systems auditing, python, PowerShell or other scripting languages, SQL, endpoint detection and response (EDR) platforms, security incident and event management (SIEM) platforms, security orchestration, automation, and response (SOAR) platforms, intrusion detection and prevention systems (IDS/IPS).
4. Demonstrate strong written and verbal communication abilities, including the capacity to effectively collaborate with diverse technical and business experts, conveying complex technical and analytical information clearly.
5. Exhibit a strong commitment to teamwork and collaboration, contributing to a positive and cooperative work environment.
6. Possess a high-level understanding of equal opportunity principles and a strong commitment to applying equal opportunity policies within a university context.
7. Hold an existing NV1 or NV2 Government security clearance or be willing to undergo the security clearance vetting process, with a willingness to disclose all relevant and required information for obtaining and maintaining a security clearance.

*ANU Officer Levels 5 and 6 are broadbanded in this stream. It is expected that at the higher levels within the broadband occupants, through experience, will have developed skills and expertise enabling them to more independently perform the full range of duties at a higher level, and that more time will be spent on the more complex functions of the position.*

*The ANU conducts background checks on potential employees, and employment in this position is conditional on satisfactory results in accordance with the [Background Checking](#) Procedure which sets out the types of checks required by each type of position.*

| Supervisor/Delegate Name: | Laura Borham | Date: | August 2024 |
|---|---|---|---|

**References:**
[Professional Staff Classification Descriptors](#)

# Australian National University
# Pre-Employment Work Environment Report

## Position Details

| College/Div/Centre | Chief Information Security Office | Dept/School/Section | Cyber Engineering |
|---|---|---|---|
| Position Title | Junior Information Security Engineer | Classification | ANUO 5/6 (IT) |
| Position No. | 41637 | Reference No. | |

In accordance with the Work Health and Safety Act 2011 (Cth) the University has a primary duty of care, so far as reasonably practicable, to ensure the health and safety of all staff while they are at work in the University.

- This form must be completed by the supervisor of the advertised position and appended to the back of the Position Description.

- This form is used to advise potential applicants of work environment and health and safety hazards prior to application.

- Once an applicant has been selected for the position they must familiarise themselves with the University WHS Management System via Handbook guidance https://services.anu.edu.au/human-resources/health-safety/whs-management-system-handbook

- The hazards identified below are of generic nature in relation to the position. It is not correlated directly to training required for the specific staff to be engaged. Identification of individual WHS training needs must be in accordance with WHS Local Training Plan and through the WHS induction programs and Performance Development Review Process.

- 'Regular' hazards identified below must be listed as 'Essential' in the Selection Criteria - see ' Employment Medical Procedures' at http://info.anu.edu.au/Policies/_DHR/Procedures/Employment_Medical_Procedures.asp

## Potential Hazards

- Please indicate whether the duties associated with appointment will result in exposure to any of the following potential hazards, either as a **regular** or **occasional** part of the duties.

| TASK | regular | occasional | TASK | regular | occasional |
|---|---|---|---|---|---|
| key boarding | ☒ | ☐ | laboratory work | ☐ | ☐ |
| lifting, manual handling | ☐ | ☒ | work at heights | ☐ | ☐ |
| repetitive manual tasks | ☐ | ☐ | work in confined spaces | ☐ | ☐ |
| Organizing events | ☐ | ☐ | noise / vibration | ☐ | ☐ |
| fieldwork & travel | ☐ | ☒ | electricity | ☐ | ☐ |
| driving a vehicle | ☐ | ☐ | | | |
| **NON-IONIZING RADIATION** | | | **IONIZING RADIATION** | | |
| solar | ☐ | ☐ | gamma, x-rays | ☐ | ☐ |
| ultraviolet | ☐ | ☐ | beta particles | ☐ | ☐ |
| infra red | ☐ | ☐ | nuclear particles | ☐ | ☐ |
| laser | ☐ | ☐ | | | |
| radio frequency | ☐ | ☐ | | | |
| **CHEMICALS** | | | **BIOLOGICAL MATERIALS** | | |
| hazardous substances | ☐ | ☐ | microbiological materials | ☐ | ☐ |
| allergens | ☐ | ☐ | potential biological allergens | ☐ | ☐ |
| cytotoxics | ☐ | ☐ | laboratory animals or insects | ☐ | ☐ |
| mutagens/teratogens/ carcinogens | ☐ | ☐ | clinical specimens, including blood | ☐ | ☐ |
| pesticides / herbicides | ☐ | ☐ | genetically-manipulated specimens | ☐ | ☐ |
| | | | immunisations | ☐ | ☐ |

| OTHER POTENTIAL HAZARDS (please specify): | | | |
|---|---|---|---|
| Supervisor/Delegate: | *Laura Borham* | Date: | *August 2024* |