|  |  |
| --- | --- |
| **Position Title** | Senior IT Security Analyst |
| **Group/Portfolio** | Digital Solutions |
| **Classification** | HEW 8 |
| **Position Number** | 00061161 |
| **Reports To** | Senior Lead, Cyber Security |
| **Employment Type** | Fixed Term  |

## Position Purpose

Digital Solutions is a value-driven strategic IT partner focused on delivering leading digital experiences for our Students, Colleagues and Community. We work within a contemporary operating model and are modernising our technologies and ways of working to create value and build a digital future for Griffith.

Senior IT Security Analysts provide guidance and advice on the implementation and secure operation of software and network solutions to protect ICT infrastructure, systems, data and users from unauthorised access and manipulation. They are accountable for day-to-day cyber threat defence and response activities for security events and incidents and help drive continuous improvement to ensure the organisation's cyber resilience and maturity is increasing.

## 2.0 Eligibility Requirements

* + - The occupant of this position will hold relevant postgraduate qualifications or progress towards postgraduate qualifications and extensive relevant experience or an equivalent combination of relevant experience and/or education/training in cyber security.

## 3.0 Key Responsibilities

* + - **Information security.** Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security and recommends appropriate control improvements. Contributes to development of information security policy, standards and guidelines.
		- **Specialist advice.** Actively maintains recognised expert level knowledge in one or more identifiable specialisms. Provides definitive and expert advice in their specialist area(s). Oversees the provision of specialist advice by others, consolidates expertise from multiple sources, including third party experts, to provide coherent advice to further organisational objectives. Supports and promotes the development and sharing of specialist knowledge within the organisation.
		- **Security administration.** Monitors the application and compliance of security administration procedures and reviews information systems for actual or potential breaches in security. Ensures that all identified breaches in security are promptly and thoroughly investigated and that any system changes required to maintain security are implemented. Ensures that security records are accurate and complete and that request for support are dealt with according to set standards and procedures. Contributes to the creation and maintenance of policy, standards, procedures and documentation for security.
		- **Penetration testing.** Coordinates and manages planning of penetration tests, within a defined area of business activity. Delivers objective insights into the existence of vulnerabilities, the effectiveness of defences and mitigating controls - both those already in place and those planned for future implementation. Takes responsibility for integrity of testing activities and coordinates the execution of these activities. Provides authoritative advice and guidance on the planning and execution of vulnerability tests. Defines and communicates the test strategy. Manages all test processes and contributes to corporate security testing standards.
		- **Incident management.** Ensures that incidents are handled according to agreed procedures. Investigates escalated incidents to responsible service owners and seeks resolution. Facilitates recovery, following resolution of incidents. Ensures that resolved incidents are properly documented and closed. Analyses causes of incidents and informs service owners in order to minimise probability of recurrence and contribute to service improvement. Analyses metrics and reports on performance of incident management process.
		- **Relationship management.** Identifies the communications and relationship needs of stakeholder groups. Translates communications/stakeholder engagement strategies into specific activities and deliverables. Facilitates open communication and discussion between stakeholders, acting as a single point of contact by developing, maintaining and working to stakeholder engagement strategies and plans. Provides informed feedback to assess and promote understanding. Facilitates business decision-making processes. Captures and disseminates technical and business information.
		- Supports compliance with relevant legislation and University policies and procedures, including equity and health & safety and exhibit good practice in relation to same.
		- Be a leading example of the principles and values embodied in the University’s Code of Conduct, and behave, act and communicate at all times to reflect fairness, ethics and professionalism.

## 4.0 Key Capabilities

* Griffith University identifies the attributes of resilience, flexibility, creativity, digital literacy and entrepreneurship as critical to our graduates’ success, in the rapidly changing future world of work. We have established a Griffith University Capability Development Framework to provide a common language of some of the non-technical organisation skills that will support our staff to thrive now and into the future. The Capability Development Framework will assist you to understand the current skill level of this position in the non-technical but critical skill domains that are increasingly important in a changing workplace context.

To read about some of the non-technical organisation skills for this position, please see the Leads Self section of our [Capability Development Framework](https://intranet.secure.griffith.edu.au/employment/learning-and-development/specialist-programs/capability-development-framework#framework).