JOB DESCRIPTION
Security Operations Centre Analyst
Vacancy Ref: A2042

Job Title: Security Operations Centre Analyst	**Present Grade:** 7
Department/College: Information Systems Services	
Directly responsible to: IT Security Manager	
Supervisory responsibility for: n/a	

Other Contacts:

Internal:
ISS Leadership Team (ISS-LT), University Strategic planning and Governance, IT Security Operations Group, University staff and students

External:
JANET Computer Security Incident response Team.

Main Functions:
The SOC analyst role will work closely with the IT Security Manager and IT system owners to maintain, monitor and respond to various notifications from monitoring systems to improve the IT security of the University. The role will also work with users across the university to respond to security issues and to identify and suggest improvements that can be made to technologies and processes.

Major Duties are to:

1. To monitor, maintain and protect University networks, systems and assets for malicious activity typically using technologies such as Security Incident and Event Management (SIEM) and IDS systems.
2. To carry out technical vulnerability assessments of IT systems to identifying potential vulnerabilities, make recommendations to control identified risks and work with those individuals to ensure they are implemented.
3. Under minimal guidance of the IT Security Manager, assist with IT security Audits throughout the University - identifying potentially insecure processes and systems.
4. To respond rapidly and effectively to IT security incidents, managing them in a professional manor, including performing forensics for evidence gathering and preservation.
5. To contribute towards information security guidance documentation and training.
6. Approach tasks with flexibility, proactivity and complete work to a high quality
7. To coordinate tasks as directed by the IT Security Manager to assist in the improvement of the security of the system.
8. To keep up to date with security trends, threats and control measures.
9. To manage other activities that may arise through evolution, growth or restructuring.
10. Maintenance of confidentiality of information; it will be necessary to comply with requirements related to the Data Protection Act.
11. At all times to carry out your responsibilities with due regard to the University's code on Equality and Diversity, University Health and Safety Codes of Practice and Child Protection Policy
12. Actively participate and contribute in regular and *ad-hoc* meetings and liaison with team, departmental and institutional colleagues as directed.
13. To maintain high levels of professional conduct, including but not limited to: cooperative engagement in tasks set; the exercising of initiative to suggest, through line managers, improvements to the service provided; and clear and professional styles of communication at all times.