Applications are invited from suitably qualified candidates for the following position:

Information Systems Services (ISS)
IT Security Engineer
3 Year Contract

Dublin City University www.dcu.ie is a research-intensive, globally-engaged, dynamic institution that is distinguished both by the quality and impact of its graduates and by its focus on the translation of knowledge into societal and economic benefit. Through its mission to transform lives and societies through education, research and innovation, DCU acts as an agent of social, cultural and economic progress. DCU is Ireland's fastest growing University, and now hosts more than 17,000 students across its three academic campuses: DCU Glasnevin Campus, DCU St Patrick's Campus and DCU All Hallows campus.

Information Systems Services (ISS)

The ISS Department is a central support unit responsible for providing a complete ICT service to the University's various schools, units, research centres and campus companies. In addition to working closely with all stakeholders across DCU to ensure quality service delivery, ISS is responsible for the University's extensive ICT infrastructure estate servicing our three academic campuses. ISS plays a key role in supporting the University in achieving the objectives set out in its Strategic Plan: *Talent, Discovery and Transformation 2017-2022*. For further information, please visit https://www.dcu.ie/iss/

Role Profile

The IT Security Engineer will report to the Deputy Director of ISS and work with the Senior IT Security Engineer, within the Engineering and Innovation Team, to monitor and manage the operation of security systems and best practice across the university's IT environment. The post-holder will participate in security related service management processes (security incident, change and problem management) and will participate in the planning, design, enforcement and review of security controls which protect the integrity of DCU digital assets.

Duties and Responsibilities

Duties and responsibilities include but are not limited to:

- Follow standard security control frameworks/guidelines to ensure consistent application of information security controls
- Recognise and identify potential threats and areas where existing cyber security procedures require change, or where new procedures need to be developed

- Analyse and evaluate network, subsystems, components, controls and security criteria for vulnerabilities and weaknesses
- Provide hands-on remediation of security vulnerabilities across a wide range of infrastructure and technologies
- Implement and manage network security components such as next generation firewalls, intrusion detection and prevention (IDS/IPS) systems
- Provide expertise in the technical design, implementation, testing and troubleshooting for security infrastructure components
- Ensure appropriate and proactive monitoring and event logging for the DCU IT Infrastructure
- Investigate and utilise new technologies, tools and techniques to enhance security capabilities and performance
- Perform security monitoring, vulnerability assessments and forensic log analysis to proactively detect security incidents and threats
- Plan for and perform periodic security audits to validate that the security posture satisfies DCU security requirements
- Lead cyber security aspects of IT disaster recovery and business continuity planning
- Provide subject matter expertise and support to all DCU stakeholders to ensure information security is appropriately considered and implemented
- Be responsible for the design and development of the university's cyber security awareness training programme
- Ensure appropriate incident handling procedures and security incident reporting is adhered to
- Undertake any other appropriate duties assigned by the Director of ISS or nominee.

Candidate Requirements

Essential

- At least 5 years' relevant experience working in a challenging IT environment
- A strong technical background with a clear and abiding interest in cyber security
- Significant hands on technical experience in enterprise level information security management
- A primary degree or equivalent (NFQ Level 7) in Information Technology, Computer Science or other relevant field
- Proven ability to implement proper system security controls, metrics and performance indicators for IT systems and service security.
- Strong working knowledge across a range of technologies including Active Directory, IdP, Windows/Linux servers, VPNs, encryption, two factor authentication, VMware, network infrastructure and storage
- Good customer focus
- Strong communication, presentation, interpersonal and problem-solving skills

Desirable

- Experience working with a security incident and event management (SIEM) solution

- Information security management qualifications such as CISSP or similar

Mandatory Training

The post holder will be required to undertake the following mandatory compliance training: GDPR, orientation, and compliance. Other training may need to be undertaken.