REGENT'S
UNIVERSITY LONDON
CULTIVATING POSSIBILITY

ITS Security Analyst

At Regent's University London, we have a bold mission of reimagining education, and we're looking for talented and passionate people to help us do that. We're ambitious, collaborative and curious in how we approach our work, each other, and the education we give our students.

Nestled in the heart of royal Regent's Park, Regent's offers a premium experience for staff and students. We champion an environment that cultivates possibility for everyone in our community.

Job description

Position details

Job title:

ITS Security Analyst

Grade:

H

Department:

Information Technology Services

Line Manager Job Title:

Head of Cyber Security & Networks

Job purpose

The Security Analyst will play an important role in supporting the university's information security initiatives, focusing on developing a deeper understanding of policies, compliance, and security best practices.

Working closely with the broader cybersecurity and governance teams, this role is designed for someone eager to grow into the position, with opportunities to expand responsibilities over time.

The Security Analyst will assist in fostering a secure and compliant environment for the Regent's community by supporting learning and development around security policies, procedures, and practices. Their contributions will help strengthen both academic and administrative operations, ensuring continuous improvement in the university's cybersecurity posture.

The Regent's Way is a set of principles that guide our work and celebrate our unique offering – our strengths, our challenges and our commitment to continuous improvement.

Main responsibilities

1	**Day-to-Day Security Operations** Respond to incoming security alerts and inquiries from the IT Service Desk, third parties, and monitoring tools.
2	**Cybersecurity Incident Response** Manage and coordinate responses to cybersecurity incidents with internal teams, partners, and external entities.
3	**Cybersecurity Training and Awareness** Provide training, advice, and support to staff and students to raise cybersecurity awareness and address issues
4	**Compliance and Regulatory Guidance** Ensure cybersecurity practices align with legal, regulatory, and contractual requirements through policies, standards, and training
5	**Information Security Policy Management** Maintain and update the Information Security Policy suite in collaboration with the University's Governance team.
6	**Compliance Testing of Software and Products** Evaluate new and existing software/products for compliance with cybersecurity policies and standards, offering guidance to relevant teams
7	**Cybersecurity Risk Assessment** Assess software and product risks, maintain a cybersecurity risk register, and report key risks to the corporate risk register.
8	**Emerging Technologies and Threats Monitoring** Track new developments in cybersecurity technologies and threats, providing guidance on best practices
9	Actively seek to implement the University's health and safety policy and give due regard to the health and safety of themselves and others when carrying out duties.
10	Actively seek to implement the University's equal opportunities policy and promote equality of opportunity in relation to the duties of the post.
11	To undertake any other duties that may reasonably be requested appropriate to the grade and responsibilities of the post.

Person specification

Job requirements	Assessment criteria	
	(e)ssential	(d)esirable
Qualifications & training		
Educated to Degree Level (or Equivalent) in Computer Science**,** Cybersecurity**,** Information Technology or equivalent practical experience in the cybersecurity field	E	
At least 2-3 years of experience working in cybersecurity, with hands-on experience in security operations, incident response, network security, or systems administration.	E	
CompTIA Security+, CISSP qualification		D
Experience		
Cross-Functional Collaboration and Awareness Experience in managing or contributing to cybersecurity awareness platforms, creating educational content, and collaborating across teams to promote a culture of security awareness.		D
Cybersecurity Policy, Compliance, and Frameworks Experience in contributing to and maintaining an Information Security Policy suite, ensuring timely updates and proper publication, along with familiarity in monitoring and ensuring compliance with frameworks such as Cyber Essentials, ISO 27001, and others across teams.		D
Emerging Threats and Technologies Hands-on experience in analysing, advising on, and mitigating the impact of emerging technologies (e.g., AI, cloud platforms) and new cybersecurity threats or vulnerabilities, with a focus on adapting the Regents University cybersecurity posture accordingly.		D
Knowledge, skills & competencies		
Cybersecurity Expertise and Principles Solid understanding of core cybersecurity principles, including incident response, vulnerability management, threat intelligence, security policy development, and familiarity with regulations and compliance frameworks (e.g., GDPR, PCI-DSS, NCSE).	E	
Cybersecurity Tools and Technologies Proficiency with cybersecurity tools and platforms such as SIEM, vulnerability scanners, endpoint protection systems, firewalls, and other security technologies to effectively monitor, detect, and mitigate threats.		D
Communication and Collaboration Strong verbal and written communication skills to effectively engage with both technical and non-technical stakeholders, with the ability to draft clear, actionable cybersecurity messaging, especially in response to incidents or emerging threats	E	
Training and Development Ability to oversee and contribute to cybersecurity training initiatives, ensuring the staff and student bodies are continuously educated on evolving cybersecurity threats	E	

Advisory Skills Expertise in advising on the cybersecurity implications of new IT products and services, assisting product owners in achieving compliance and security best practices, as well as providing subject matter expertise on the cybersecurity aspects of emerging technologies like AI.	E	
Risk Management and Assessment Understanding of cybersecurity risk management and how to assess and mitigate risks arising from new technologies and operational practices	E	
General attributes & personal qualities		
Problem-Solving and Analytical Thinking Strong problem-solving skills for managing complex security incidents, assessing risks, and implementing solutions.	E	
Detail-Oriented High attention to detail when reviewing cybersecurity policies, compliance audits, or incident reports, ensuring accuracy and thoroughness	E	
Adaptability Ability to adapt to evolving threats, technologies, and organisational needs, staying up to date with emerging cybersecurity trends and challenges.	E	
Proactive and Self-Motivated A proactive individual with a strong sense of ownership and accountability, able to identify potential risks and address them before they become incidents. Demonstrates a passion for continuous learning and staying up to date with the ever-evolving cybersecurity landscape.	E	