REGENT'S
UNIVERSITY LONDON
CULTIVATING POSSIBILITY

Head of Information Security

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:

Head of Information Security

Grade:

J

Department:

Tech & Transformation

Line Manager Job Title:

Chief Information Officer

Job purpose

The Head of Information Security protects Regent's. The role owns the institution's security posture, risk and policy, and holds the rest of the organisation to account for compliance, setting expectations and outlining remediation. It leads a lean cyber function that owns direction and outsources execution, steering the outsourced SOC and SIEM. It leads through influence and relationships, reserving formal authority for the moments that need it.

The Head of Information Security delivers to compliance and governance: it co-chairs the Data Privacy and Information Security Group (DPISG), works closely with the Data Protection Officer, and is the sole IT security voice in governance forums.

The Head of Information Security delivers Professionalise Security: a single 360 security-first strategy that integrates cyber, privacy and continuity, and carries Regent's through the parent group's security tiers.

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	Own Regent's security posture and the 360 security-first strategy: deliver the multi-year cyber roadmap, define the security KPIs that measure it, and report progress and posture to executive governance.
2	Oversee and maintain the full suite of security policies and requirements, including the secure adoption of AI; publish, educate and drive adoption across the University.
3	To be responsible for the selection of, implementation, certification and ongoing compliance of recognised security frameworks and standards (currently Cyber Essentials Plus and PCI DSS), with sole authority to propose new frameworks for sign-off, holding the functions that operate the technical controls to account.
4	Co-chair the Data Privacy and Information Security Group (DPISG), act as the sole security voice in governance forums, and partner with the parent group (GGE) on security posture and progression through its tiers.
5	Lead the management of cyber risk across the departmental and organisational risk registers: set risk appetite and acceptance thresholds, escalate significant risk, and hold risk, application and process owners accountable through the cyber scorecard and monthly governance.
6	Provide strategic oversight of vulnerability management and the security testing programme, define response SLAs by severity, drive and audit adherence, with authority to test compliance against any standard the role sets.
7	Govern the outsourced SOC and SIEM and manage third-party and supply-chain security risk: detection and response performance, the contract and commercial relationship, and the security of vendors and SaaS.
8	Oversee identity and access governance: set and audit the access policy, including privileged access approval, with Technology Operations operating the platform and Service Operations handling standard transactions.
9	Lead data loss prevention and insider-threat controls, including the ownership of privacy and data protection through a security lens, coordinating with the University's data protection function.
10	Define and maintain the security standards that architecture must adhere to , and run the security review gate over designs, change and procurement, through pre-production sign-off or post-facto audit by standard.
11	Foster a security-first mindset across the University: define and lead mandatory security education for all staff and students, measure completion, and champion the behaviours that make security everyone's responsibility.

12	Coordinate cyber incident response within the ITSM framework owned by Service Operations, with decision-making authority to shut down systems for active operational security reasons, delegate to nominated team members and relevant parties.
13	Provide independent assurance over Technology Operations, Delivery, and all architecture and change, and oversee business continuity and disaster recovery readiness, holding business areas accountable through regular testing.
14	Day to day management and mentorship of the security team, including recruitment, objective setting, performance management, coaching and ensuring succession plans are in place for critical security skills, and mentor colleagues across the department to build security capability in every function.
15	Lead and develop the lean cyber function: own direction, outsource execution; own the security budget and cost centre, including procurement within the framework.
16	Maintain the relationship with the cyber risk insurance provider, overseeing renewals, attestations, policy compliance, incident notifications and claims management. Advise on the adequacy of cover against the institution's risk position, and maintain the security posture and evidence that keep cover attainable and affordable.
17	Contribute to building a vibrant campus community by taking real accountability, collaborating with colleagues across the university and constantly adding value. Foster an inclusive, sustainable and safe environment for all through our EDI, Health and Safety and B-Corp initiatives and policies.
18	To undertake any other duties that may reasonably be requested appropriate to the grade and responsibilities of the post.

Person specification

1. Position details

Job title: Head of Information Security
Grade: J
Department: Tech & Transformation
Line manager job title: Chief Information Officer

2. Person requirements

Job requirements	Assessment criteria	
	(e)ssential	(d)esirable
Qualifications & training		
Degree or equivalent professional experience in an IT or security discipline	E	
A recognised security certification such as CISSP or CISM		D
Certification or formal training in a recognised security framework such as ISO 27001 or NIST CSF		D
Experience		
Experience in managing security posture, risk and policy in a complex organisation, including setting strategy and delivering against a multi-year roadmap	E	
Experience in leading, developing and motivating a team, including setting direction, managing performance and growing capability	E	
Governing outsourced security partners including SOC and SIEM providers, including the contract and commercial relationship, and assessumg third party supply-chain risk across vendors and SaaS	E	
A background of leading cyber incident responses, from tested plans to coordination on the day	E	
The capability to author, publishand drive the adoption of security policy and requirements	E	
Experience of achieving and maintaining recognised certifications and compliance regimes, such as Cyber Essentials Plus and PCI DSS for card-payment environments	E	
A background in running organisation-wide security education and awareness programmes, and security testing programmes (including penetration testing and red-teaming)	E	
Able to chair or co-chair governance forums and represent security to senior and executive audiences (including boards and committees), and work with data protection functions on privacy and GDPR	E	
A background in building or leading a lean security function that owns direction and outsources execution		D
Experience within higher education or another complex, regulated environment		D

Knowledge, skills & competencies		
Knowledge of information security and assurance: risk and vulnerability management, security governance frameworks, identity and access governance, privacy and data protection, and business continuity	E	
Knowledge of security testing methodologies, third-party and supply-chain security, and threat intelligence	E	
The ability to translate technical risk into clear business terms for non-technical owners	E	
General attributes & personal qualities		
Independent and credible, able to provide assurance without marking their own homework	E	
An engaging people leader who wins support through influence, trust and relationships across teams, using formal authority sparingly and well.	E	
Able to hold senior colleagues to account constructively	E	
Calm and authoritative in an incident	E	
A clear communicator of risk to technical and non-technical audiences	E	
Other / special requirements		
A commitment to inclusivity, sustainability and continuous improvement	E	
Demonstrates awareness of health and safety responsibilities	E	
A flexible approach to working patterns appropriate to a senior role	E	