JOB DESCRIPTION

Job Title:	Cyber Security & Information Risk Analyst
Department / Unit:	IT / Cybersecurity
Grade:	8
Accountable to:	Cyber Security Operations Manager
Accountable for:	N/A

Purpose of the Post

Provides leadership and guidelines on cybersecurity and information assurance, working effectively with strategic organisational functions such as legal and data governance experts to provide authoritative advice, guidance and assessment on the requirements for internal and third-party security controls.

Key Tasks

1. Develops cybersecurity policy, standards and guidelines appropriate to business, technology and legal requirements and in accordance with best professional and industry practice.

2. Operates as a focus for IT security expertise for the organisation, providing authoritative advice and guidance on the design of all types of security control, including legislative or regulatory requirements such as data protection and software copyright law.

3. Develops, maintains and implements the cyber and information security non-functional requirements used to evaluate the suitability of internally and externally provided applications and services.

4. Leads the review and revision of procedures relating to security control of all IT environment, systems, products or services in order to demonstrate continual improvement in control including creation of auditable records, user documentation and security awareness literature.

5. Reviews new business proposals and planned technical changes and provides due diligence including specialist guidance on security issues and implications.

6. Logs and supports the management of cyber and information security risks.

7. Supports the investigation of breaches of security and provides feedback on appropriate control improvements.

8. Makes key contributions to the development of security architecture, services and systems within the College.

9. Keeps in close touch with and contributes to current developments in cyber security within employing organisation (maintaining knowledge to the highest level), own industry and in appropriate professional and trade bodies.

10. Is fluent at articulating best practice and is a recognised authority in the evaluation of cyber and information security risk and assurance.

11. Co-author and develop University IT-related procedures and policies (acceptable use, data protection, freedom of information, cybersecurity, purchasing etc) and advise colleagues and end-users accordingly.

12. Assist with the creation, maintenance and delivery of cyber security awareness training for colleagues.

Other Duties

The duties listed are not exhaustive and may be varied from time to time as dictated by the changing needs of the College. The post holder will be expected to undertake other duties as appropriate and as requested by his/her manager.

The post holder may be required to work at any of the locations at which the business of Royal Holloway is conducted.

Internal and external relationships

The following list is not exhaustive but the post holder will be required to liaise with:

- IT Senior Management Team
- Technical Service Owners
- Legal & Governance Services
- Strategic Planning & Change
- Industry and sector specific networks
- Appropriate professional and trade bodies

PERSON SPECIFICATION

Details on the qualifications, experience, skills, knowledge and abilities that are needed to fulfil this role are set out below.

Job Title: Cyber Security & Information Risk Analyst **Department: IT**

	Essential	Desirable	**Tested by** Application Form/Interview/Test
Knowledge, Education, Qualifications and Training			
Degree in Computer Information Systems / Computer Science, Information Systems, or other related field, or equivalent professional experience	x		Application Form
Relevant Cyber Security Qualifications (CISP, SANS etc.)	x		Application Form
Skills and Abilities			
Demonstrate experience of carrying out cyber security related due diligence on internal and third-party applications and services	x		Application Form / Interview
Creation and delivery of a cyber-security related risk appetite and assurance frameworks.	x		Application Form / Interview
Demonstrable experience of end user education and assessments.	x		Application Form / Interview
Excellent writing and technical documentation skills to produce clear technical papers, requirements documents, project reports and Systems Architecture diagrams	x		Interview
Knowledge and experience of Visio & MS Office productivity tools (Word, Excel, email etc.)	x		Interview

Proven ability to forge effective professional relationships at all levels, working collaboratively and sharing knowledge and skills (business and technical)	x		Interview
Good command of written and spoken English; highly numerate	x		Interview
Ability to explain complex technical issues to both a technical & non-technical audience for small & large audiences	x		Interview
Experience			
Demonstrable experience of providing policy and standard development in a cyber-security role	x		Application Form / Interview
Supplier/Vendor Relationship Management experience	x		Interview
Experience of managing own workload, including balancing priorities, scheduling, and forward planning of work and resources to meet supply and demand	x		Interview
Other requirements			
Has successfully engaged internal technical and third party technical teams	x		Interview