JOB DESCRIPTION

Job Title:	Head of Cyber Security
Department / Unit:	IT Services / Cyber Security
Job type	Full Time , Permanent
Grade:	9
Accountable to:	Chief Information Officer
Accountable for:	Senior Cyber Security Analyst Graduate Cyber Security Analyst

Purpose of the Post

Provides strategic leadership and guidelines on cybersecurity and information assurance, cybersecurity expertise for the organisation, working effectively with strategic organisational functions such as legal experts and technical support to provide authoritative advice and guidance on the requirements for 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 application and operation of all types of security control, including legislative or regulatory requirements such as data protection and software copyright law.

3. Manages the operation of appropriate security controls as a production service to customers.

4. Develops implementation approach, taking account of current best practice, legislation and regulation. Ensures implementation of cybersecurity strategy in automated systems and ensures operations of security systems. Analyses results of investigations into complex, or highly sensitive security violations, to determine whether standards are fit for purpose, are current and are correctly implemented.

5. Reports any significant breaches in security to senior management. Interviews offenders in conjunction with the relevant line manager or on own authority if the breach warrants it. Where appropriate, participates in forensic evidence gathering, disciplinary measures, and criminal investigations

6. Ensures that procedures are in place for investigation of system access enquiries referred by support staff and for handling all enquiries relating to cybersecurity, contingency planning as they affect the activities of the organisation, function or department. Authorises implementation of procedures to satisfy new access requirements, or provide effective interfaces between customers and service providers.

7. Devises new or revised procedures relating to security control of all IT environments, systems, products or services in order to demonstrate continual improvement in control including creation of auditable records, user documentation and security awareness literature.

8. Authorises and initiates the provision of training, guidance and support to other security administrators and their agents within the employing organisation, in all aspects of security policy and control.

9. Reviews new business proposals and planned technical changes and provides specialist guidance on security issues and implications.

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

11. Is fluent at articulating best practice and is a recognised authority in the technical specialism

12. 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.

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
- College Executive Board
- Industry and sector specific networks
- Appropriate professional and trade bodies