ADVERT

This is a new role, probably the first of its kind in Oxford colleges, so offers the possibility to shape the future of information security across our group of colleges. Our colleges are lovely places to work, with helpful and friendly communities, and beautiful buildings and grounds. We have some great benefits such as generous annual leave, a generous defined benefit pension scheme, free meals while on duty, a bicycle salary sacrifice scheme, and access to the benefits of a University Card.

As an ideal candidate you'll be a seasoned technical professional with experience of designing, engineering and/or developing a range of secure IT solutions. The Information Security Lead will need to develop a strong working knowledge of all elements of information security and be able to work with, and positively influence, operational IT teams across the group. The role will be hands-on in implementing change for these operational teams where necessary.

You would need to work primarily within Oxford with the option of some remote working. You'd be expected periodically to visit individual colleges for meetings and work with local IT teams.

MAIN PURPOSE OF JOB:

The Information Security Lead (ISL) will lead operational and improvement projects across the North Oxford Share College Services (NOSCS) Colleges to protect information assets and manage information security risks. Working with and reporting to the Head of IT, the ISL will help the group to establish compliance with information security standards and create a prioritised programme of improvements and ensure implementation both technically and practically.

The Information Security Lead will work closely with the Head of IT, Technical Services Manager, Senior leaders and academics, and college IT Managers to review IT security arrangements across existing services in colleges, ensure that security is included by design in new projects and services.

MAIN TASKS:

- Review system security measures, design, and lead implementation of IT security systems and policies.
- Lead on development and delivery of measures and metrics to support the assessment, reporting and ongoing improvement of the information security posture of colleges.
- Develop close working relationships with the Head of IT, Technical Services Manager, senior professional services leaders, academics, and IT Managers to deliver Information Security improvement objectives.
- Work closely with college stakeholders to keep abreast of planned changes to technologies, working practices, and business activities that could have an impact on group and individual college Information Security or risk profiles.
- Audit controls via a security standard such as the University Information Security Baseline, Cyber Essentials, or ISO27001, providing advice to the Head of IT and IT Managers in mitigation options, suggesting and where appropriate, putting in place measures to satisfy control requirements.
- Work with the Data Protection Officer (DPO) and DPO Assistant to ensure that the group can meet Information Security requirements under the UK GDPR and fulfil the array of data subject rights.

RESPONSIBILITIES:

STRATEGIC SUPPORT

- Develop and maintain an Information Security improvement plan for the group.
- Work with IT staff within the group to build on an existing information security program and ongoing security projects that address information security risks and compliance requirements.
- Recommend, coordinate and where appropriate, implement agreed technical controls.
- Be responsible for decisions regarding operational activities in relation to Information Security improvement within the group.
- Work with the Head of IT and College governance structures to create and maintain security policies.
- Monitor and report on compliance with security policies, as well as the enforcement of policies.

- Plan and prioritise own work ensuring effective support to the group and delivery of key Cyber Security improvement objectives.

INFORMATION SECURITY MANAGEMENT

- Research, evaluate, design, test, recommend and plan the implementation of new or updated information security hardware or software, and analyse its impact on the existing environment; provide technical and managerial expertise for the administration of security tools.
- Develop strong working relationships with the Head of IT, Technical Services Manager, and IT Managers to develop and implement controls and configurations aligned with security policies and legal, regulatory and audit requirements.
- Ensure all IT staff have access to IT systems limited by need and role.
- Research/evaluate emerging information security threats and ways to manage them.
- Assist Colleges with maintaining suitable TPSA templates and maintaining a list of assessed third parties.
- Monitor and test vulnerabilities in technological infrastructure, managed services, and devices.

OPERATIONAL SUPPORT

- Use influencing skills to ensure collaborative working to engender a level of quality improvement across the group.
- Consult with IT colleagues to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications, and software as part of Privacy by Design and Default.
- Manage and coordinate operational components of security incident management, including detection response and reporting.
- Manage the day-to-day activities of threat and vulnerability management, identify risk tolerances, recommend treatment plans, and communicate information about residual risk.
- Manage security projects, provide expert guidance on security matters for other IT projects and work with suppliers to obtain best value.
- Evaluate requests for exceptions to policies, ensuring sufficient mitigating controls are in place.
- Ensure audit trails, system logs and other monitoring data sources are reviewed periodically and are following policies and audit requirements.
- Review, escalate and action any unusual event behaviour identified through the groups information security systems.
- Create standards in system hardening, change management, documentation.
- Perform periodic firewall audits.
- Ensure disaster recovery and data restoration processes work.
- Ensure appropriate Corrective and Preventative Actions are implemented in line with best practice guidance.

LIAISON AND NETWORKING

- Liaise with College Management structures and the University Information Security team when system threats or breaches occur.
- Represent the group on technical groups and projects within Colleges and the University as agreed with the Head of IT.

KNOWLEDGE, SKILLS AND EXPERIENCE

ESSENTIAL

- A record of accomplishment in and experience of introducing Information Security Improvement through successfully designing, implementing, and improving IT security architecture and controls.
- Working technical knowledge in broad domains of IT infrastructure such as data networks, server and desktop hardware and operating systems, storage and backups, and related monitoring and management systems.
- Demonstrable experience of applying security controls in one or more of the following areas: Unix/Linux Servers, Windows servers, firewalls, IDS/IPS, vulnerability management, WAF, Wi-Fi, mobile security, Data Loss Prevention, digital certificates, encryption and authentication techniques, forensics, and LAN / WANs.
- Solid understanding of security protocols, cryptography, authentication, authorisation, and security.

- Able to manage own workload, resolve competing demands, and cope with changing priorities in a flexible and proactive way.
- High level of personal integrity, as well as the ability to handle confidential matters and show an appropriate level of judgment and maturity.
- Excellent written and oral communication skills, interpersonal and collaborative skills, and the ability to communicate information security and risk-related concepts to technical and non-technical audiences.

DESIRABLE

- Formal certification (CISSP, CISM or CRISC) and/or formal training in information security standards and best practice (e.g.: ISO 27001/2, COBIT).
- Working knowledge of managing relationships with suppliers.
- Well-developed team skills to foster collective ownership and purpose.
- A passion for information security and a keen interest in IT.
- Demonstrable experience of leading and working as part of a team.