1 Advertisement

**Post Title:** Cyber Security Lead  
**School/department:** IT Services / Strategy and Architecture  
**Hours:** full time or part time hours considered up to a maximum of 1 FTE. Requests for flexible working options will be considered (subject to business need).  
**Contract:** Permanent  
**Reference:** 1930  
**Salary:** starting at £41,526 to £49,553 per annum  
**Placed on:** 21 August 2019  
**Closing date:** 21 September 2019. Applications must be received by midnight of the closing date.  
**Expected Interview date:** September / October  
**Expected start date:** As soon as possible

This is an exciting time to join the University of Sussex, supporting us on a new journey of digital transformation. As a Cyber Security Lead you will be playing a crucial role in driving the implementation of new standards of excellence in cyber security.

You will be responsible for:

- Acting as a champion for cyber security across the University, looking to drive improvements in all aspects of IT security including policies, operational processes, cloud security and ensuring a secure future architecture
- Ensuring that threats to University systems and data are identified and monitored with appropriate plans for remediation
- Leading the programme to achieve Cyber Essentials Plus accreditation initially and ISO27001 or other standards accreditation in the future
- Coordinating strategic and operational cyber security efforts across the University

You will:

- Work with the IT Leadership team to define, plan and lead a rolling programme of cyber security improvement activities
- Manage the daily activities of the Cyber Security and Compliance Analyst to ensure monitoring, threats and incidents are prioritised and acted upon
- Regularly review security incidents and update continuous improvement plans to ensure security measures are the best they can be
- Lead and plan the activities necessary to achieve and maintain Cyber Essentials Plus certification
• Be responsible for the definition and maintenance of the cyber security policy framework and associated policy lifecycle management
• Work with the University Information Management team and users to address data protection-related concerns
• Lead on a programme of cyber security training and awareness
• Be responsible for the IT Disaster Recovery plans, ensuring they are actionable and widely understood

You will have:
• An excellent working knowledge of cyber threat landscape including emerging threats, risks and vulnerabilities
• A working knowledge of cyber security legislation and standards such as GDPR, Cyber Essentials, PCI-DSS, ISO 27001
• Experience of cyber security systems, controls and best practice
• Excellent personal skills including the ability to plan and lead the cyber security programme, and communicate to both technical and non-technical audiences
• Demonstrable experience of cyber security tools, information security technologies and best practice processes
• Industry qualifications such as CISM, CompTIA, PCI ISA or similar would be highly desirable
• A solid understanding of security architectures

For full details and how to apply see our vacancies page

The University of Sussex values the diversity of its staff and students and we welcome applicants from all backgrounds.

2. The School / Division

The Department

IT Services delivers a wide range of central and specialist Technology and Information Services to users across our Campus and beyond.

We have 4 main teams delivering these services through a developing service management delivery model:

Strategy and Architecture, ensuring our technologies, policies and standards are secure, up to date and that plans to replace, upgrade and improve our technologies and systems are aligned and prioritised around the University's strategic plans and objectives.

Operations and Research, work across the research, teaching, professional services and student communities to create strategies and plans, ensuring outstanding service provision across the day-to-day operational activity of ITS.
Projects and Programme Delivery provides management and delivery of projects and major change programmes, and provides assurance through a central IT Project Management Office (PMO).

Business Relations, transforming the relationship between ITS and its stakeholders helping meet its ambition of being a globally recognised leader in the use of digital technologies in education, research, student services and university administration.

3. Job Description

Job Description for the post of: Cyber Security Lead
Department: IT Services
Section/Unit/School: Strategy and Architecture
Location: Falmer
Grade: 8
Responsible to: Assistant Director, Strategy and Architecture
Responsible for: Cyber Security and Compliance Analyst

Purpose of the post:

The Cyber Security Lead will be responsible for defining and leading on the University’s cyber security programme working to ensure that Sussex is a digitally safe environment. The role will oversee and maintain excellent standards of cyber security in digital systems and data, and ensure threats are identified and managed, and risks mitigated.

Key Responsibilities:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>To act as a champion for cyber security across the University, looking to drive improvements in all aspects of IT security including policies, operational processes, cloud security and ensuring a secure architecture in the digital systems the University uses.</td>
</tr>
<tr>
<td>2</td>
<td>Ensure threats to University systems and data are identified and monitored with appropriate plans for remediation completed in a timely way.</td>
</tr>
<tr>
<td>3</td>
<td>Lead the programme to achieve Cyber Essentials Plus accreditation initially and ISO27001 or other standards accreditation in the future.</td>
</tr>
<tr>
<td>4</td>
<td>Coordinate strategic and operational cyber security efforts across the University.</td>
</tr>
<tr>
<td>5</td>
<td>Support University efforts around GDPR and PCI-DSS compliance.</td>
</tr>
<tr>
<td>6</td>
<td>Support engagement and procurement of 3rd party systems and service providers.</td>
</tr>
<tr>
<td>7</td>
<td>Provide reports and statistics to the Information Governance Committee, Senior Information Risk Officer (SIRO) and other key stakeholders as required.</td>
</tr>
</tbody>
</table>

Specific Duties:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Working with the IT Leadership team, define, plan and carry out a rolling programme of cyber security improvement activities.</td>
</tr>
</tbody>
</table>
2. Manage the daily activities of the Cyber Security and Compliance Analyst to ensure monitoring, threats and incidents are prioritised and acted upon.

3. Regularly review security incidents and update continuous improvement plans to ensure security measures are the best they can be.

4. Lead and plan the activities necessary to achieve and maintain Cyber Essentials Plus certification.

5. Work with colleagues in Finance, and other business areas, to assure continued compliance with Payment Card Industry Data Security Standard (PCI-DSS).

6. Following agreed strategy, lead activities to achieve any other cyber security related standards such as, but not limited to, ISO 27001.

7. Ensure that an appropriate programme of audits and reviews are planned and carried out to ensure continued compliance with any achieved security standards.

8. Work with the University Information Management team and users to address data protection-related concerns, providing advice and support as required.

9. Be responsible for the definition and maintenance of the cyber security policy framework and associated policy lifecycle management.

10. Be responsible for content and production of regular service reports.

11. Be responsible to plan and action regular vulnerability and penetration testing activities.

12. Lead on a programme of cyber security training and awareness, working with University communications and training functions to improve the general level of awareness of cyber security issues and best practice.

13. Be responsible for the IT Disaster Recovery plan, ensuring it is actionable and is rehearsed and communicated on a regular timescale.

### General

1. To work with the team to ensure excellent outcomes and success of any projects.

2. To keep up to date with latest security-related issues, threats and technology.

3. To represent IT Services within the University and externally as appropriate.

4. To support and educate others in cyber security best practice.

5. To identify risks and issues and address or raise them with others as necessary.

This Job Description sets out initially planned duties of the post that may vary from time to time without changing the general character of the post or the level of responsibility entailed.

### 4. Person Specification

<table>
<thead>
<tr>
<th>PERSON SPECIFICATION – critical requirements for the job</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Skills and Competencies</th>
<th>Essential</th>
<th>Desirable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Skills</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Experience of cyber security systems and controls, including end point security, vulnerability management, web content filtering, intrusion prevention, SIEM, email security, data loss prevention, NAC, IAM, cloud security and firewalls</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>• Experience of cyber security architectures and best practice</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Business Skills</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Able to develop and maintain a good understanding of the University of Sussex business, its aims and objectives and to consider these when undertaking own accountabilities;</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>• Experience of working with senior management to develop business plans, ensuring alignment to strategy with the ability to articulate complex technical solutions;</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>• Experienced in leading and maintaining a balanced approach to IT compliance whilst being performance</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
and delivery focused in support of high performing IT services organisations;

- Excellent planning and organisational skills including identifying short-term actions that are consistent with long-term goals;

**Personal and Interpersonal Skills**

- Builds formal and informal professional networks throughout the University and through external groups;
- Strong communication and interpersonal skills as well as the ability to relay technical issues to a senior non-technical audience in an engaging and informative manner;
- Able to resolve differences professionally and effectively within acceptable risk boundaries;

**Leadership and Management**

- Leads discussions with senior managers in ways that support strategic plans;
- Identifies opportunities and motivates others to realise them;
- Fosters best practice in IT and the wider business and leads by example;
- Effective oral and written communication, issue resolution, training, coaching and motivation;

**Experience and Qualifications**

<table>
<thead>
<tr>
<th>Experience and Qualifications</th>
<th>Essential</th>
<th>Desirable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Experience</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Demonstrable experience of cyber security tools, information security technologies and best practice processes;</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Experience of managing, motivating and leading teams;</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Experience in establishing and maintaining good working relationships with all levels within organisation;</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Qualifications</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educated to degree level or equivalent work experience in technology roles;</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>CISM, CompTIA, PCI ISA or similar cyber security qualifications;</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>TOGAF certification</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>