| | Last Updated: 30 March 2026 | | |
|---|---|---|---|
| **Job Title** | (TBD) Cyber Security Continuous Improvement Manager | | |
| **Faculty/ Department** | Information Services | **Legal Entity** | University of Surrey |
| **Job Family** | Professional Services – IT & Digital | **Job Level** | Grade 6 |
| **Reports To** | Director of Cyber Security | **Line Manager's (role title(s))** | Director of Cyber Security |

**Job Statement**

In this senior role, you will shape and strengthen the University's cyber resilience, ensuring our security capabilities, controls and behaviours continuously evolve in response to an ever-changing threat landscape.

You will play a central role in how the University identifies, manages and adapts to cyber risk—using data, intelligence and sector best practice to guide decision-making. The post leads our shift from reactive to proactive security, driving behavioural and cultural change across the institution and embedding clear accountability for cyber risk.

Beyond formal project delivery, you will oversee continuous improvement activity—translating operational insight from metrics, audits, incidents and risk assessments into practical, business-as-usual enhancements. This work ensures faster detection and response, greater organisational readiness, and more resilient incident management processes.

You will also support the Director of Cyber Security and the Head of Cyber Security Operations during cyber incidents, providing structured facilitation, documentation and communication. The role ensures decisions and actions are clearly captured, consistently followed through, and leveraged for organisational learning. Acting as the primary communications and engagement interface for cyber security, you will also contribute to wider IT Services communications to ensure clarity, consistency and strong stakeholder understanding.

Through effective coordination, communication and continuous improvement, this role contributes directly to safeguarding the University's reputation, strengthening cyber capability, maintaining operational continuity, protecting assets, and enabling growth and innovation—while supporting informed decision-making at senior levels.

**Key Responsibilities** This is not designed to be a list of all tasks undertaken but the main responsibilities (5 to 8 maximum)

1. Lead continuous improvement – develop and implement a structured, continuous improvement roadmap to enhance the University's cybersecurity maturity over time.
2. Drive risk reduction initiatives – oversee the identification, tracking and mitigation or cyber risks, ensuring continuous reduction of vulnerabilities across systems and processes enabling and influencing executive risk decision making.
3. Lead on internal exercises and post incident reviews – Lead lessons learned activities, ensuring root causes are addressed and translated into practical, proportionate improvements. Accountability for ensuring organisational learning is embedded.
4. Establish metrics and reporting – define and manage key performance indicators and key risk indicators to measure the effectiveness of controls and improvement efforts and which allow informed and timely decision making at senior levels of the organisation.
5. Support during cyber security incidents - Assisting the Director of Cyber Security and the Head of Cyber Security Operations by facilitating structured engagement between Cyber Operations, Cyber Risk & Compliance, IT Services, Communications, and other University senior stakeholders, ensuring clarity of roles, actions, and timelines.
6. Promote security culture and awareness – support the development of a culture of continuous improvement and security awareness through training, communication and engagement initiatives, ensuring risk reducing behaviours are embedded and well understood.
7. Oversee the governance and lifecycle of cybersecurity policies - updating policies, standards and control frameworks to reflect evolving threats and regulatory requirements.
8. Develop and coordinate clear, proportionate communications relating to cyber incidents, cyber policy and risk, and resilience, tailored for technical, executive, and non-technical audiences across the University.

**N.B. The above list is not exhaustive.**

**Role Scope and Impact** This is a summary of the post holder's role in delivering outcomes, making decisions, and the complexity of problem-solving involved in the role.

1. Accountability: Describe level of autonomy and decision making

Operating with a high degree of autonomy, the role owns the continuous improvement roadmap, aligns activities to recognised frameworks such as ISO 27001 and provides clear, data driven assurance to leadership on cyber maturity and risk posture, and providing the expertise to allow leadership to make informed decisions around technical response, risk acceptance

2. Problem solving: *Describe complexity and nature of problems handled.*

The role involves handling complex, sensitive, and often time-critical situations where information may be incomplete or evolving. The postholder is required to analyse issues, balance competing priorities, and coordinate responses across multiple teams while ensuring governance, clarity, and proportionality are maintained.

**Person Specification** This section describes the knowledge, experience & competence required by the post holder that is necessary for standard acceptable performance in carrying out this role.

| **Qualifications and Professional Memberships** | | |
|---|---|---|
| Professionally qualified with a relevant degree/postgraduate qualification, plus significant relevant managerial experience and leadership experience, or substantial experience and proven success in a strategically important specialist area.<br>Or:<br>Extensive vocational and strategic management and leadership experience demonstrating professional development through involvement in a series of progressively more demanding and influential work/roles, backed by evidence of significant development | | Essential |
| Professional qualification or certification in information security, change management, communications, continuous improvement, or related discipline | | Desirable |
| Membership of a relevant professional body | | Desirable |
| **Technical Competencies (Experience and Knowledge)** This section contains the level of competency required to carry out the role (please refer to the Competency Framework for clarification where needed and the Job Matching Guidance).<br>Level 1: basic level of understanding/experience and can apply it with guidance.<br>Level 2: good level of understanding/experience and can apply it with little or no guidance.<br>Level 3: expert level of understanding/experience and can apply, develop it and guide others. | **Essential/ Desirable** | **Level 1-3** |
| Incident or case coordination involving multiple stakeholders | Essential | 3 |
| Continuous improvement outside formal project delivery | Essential | 3 |
| Development of clear communications for complex or sensitive issues | Essential | 3 |
| Understanding of cyber security, risk, and assurance concepts (non-technical) | Essential | 3 |
| Security awareness or behavioural change initiatives | Essential | 3 |
| Stakeholder engagement at senior leadership level | Essential | 3 |
| Experience in Higher Education or public sector | Essential | 2 |
| Background in cyber security or investigative environments | Essential | 3 |
| **Special Requirements** This may include a Disclosure and Barring Service (DBS) check, regular overseas travel, driving licence, shift work. | | **Essential/ Desirable** |
| Ability to respond flexibly during cyber incidents | | Essential |

| | |
|---|---|
| Occasional out-of-hours working during incidents | Essential |
| | |
| **Core Competencies** This section contains the level of competency required to carry out this role. (Please refer to the competency framework for clarification where needed). n/a (not applicable) should be placed, where the competency is not a requirement of the grade. | **Level 1-3** |
| Communication | 3 |
| Adaptability and Flexibility | 3 |
| Customer, Client service and support | 2 |
| Planning and Organising | 3 |
| Continuous Improvement | 3 |
| Problem Solving and Decision Making Skills | 3 |
| Managing and Developing Performance | N/A |
| Creative and Analytical Thinking | 3 |
| Influencing, Persuasion and Negotiation Skills | 3 |
| Strategic Thinking and Leadership | 3 |

This Job Purpose outlines the core activities of the role. As the Department/Faculty and the post holder evolve, the duties and focus of the role may change. The University expects the post holder to adopt a flexible approach to work, including undertaking relevant training when necessary. If significant changes to the Job Purpose are required, the post holder will be consulted, and the changes will be reflected in a revised Job Purpose.

**All staff are expected to:**

- Positively support equality of opportunity and equity of treatment to colleagues and students in accordance with the University of Surrey Equal Opportunities Policy.
- Work to achieve the aims of our Environmental Policy and promote awareness to colleagues and students.
- Follow University/departmental policies and working practices in ensuring that no breaches of information security result from their actions.
- Contribute towards broader university initiatives that have a positive impact on student experience, recruitment and campus operations. This may include participation in cross-functional activities such as open days, confirmation and clearing, welcome week, graduation.
- Ensure they are aware of and abide by all relevant University Regulations and Policies relevant to the role.
- Undertake such other duties within the scope of the post as may be requested by your Manager.
- Work supportively with colleagues, operating in a collegiate manner at all times.

**Help maintain a safe working environment by:**

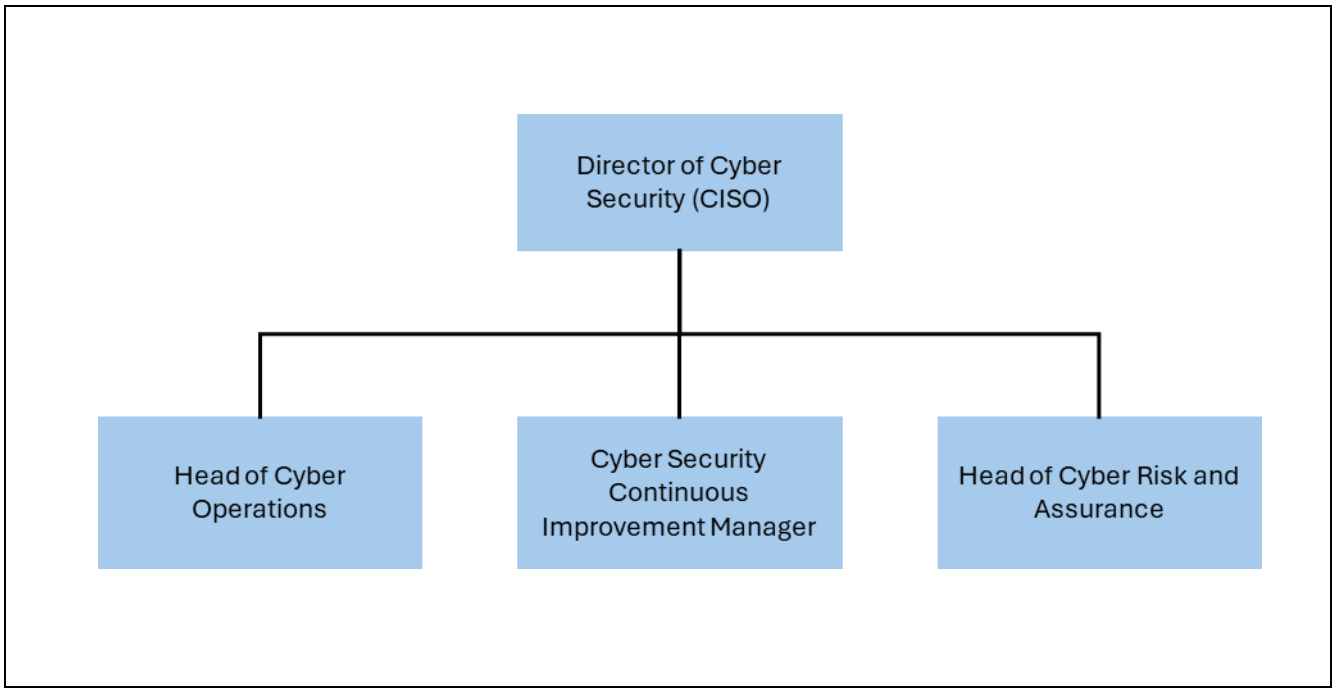
- All staff have a statutory responsibility to take reasonable care of themselves and others and to prevent harm by their acts or omissions. All staff are, therefore, required to adhere to the University's Our Safety Policy Statement and associated Procedures.

## Organisational/Departmental Information & Key Relationships

### Background Information

Information Services provides the digital, technology, and cyber security services that underpin the University's education, research, and professional services. The Cyber Security function plays a critical role in protecting the University's information, systems, and reputation while enabling innovation and digital transformation.

This role supports the University's commitment to resilience, continuous improvement, and effective risk management by strengthening coordination, communication, and learning across cyber-related activity.


Director of Cyber Security (CISO)
Head of Cyber Operations
Cyber Security Continuous Improvement Manager
Head of Cyber Risk and Assurance