

+

## Cyber Security Lead - Job Description & Person Specification

**Sense single salary point:** CHA55

**Location:** STBP or Loughborough or London

**Responsible to:** Head of Technology Solutions

### About Sense

For everyone living with complex disabilities. For everyone who is deafblind. Sense is here to help people communicate and experience the world. We believe that no one, no matter how complex their disabilities, should be isolated, left out, or unable to fulfil their potential. Our experts offer support that's tailored to the individual needs of each person, whether that's at our centres, through our holidays and short breaks, or in people's own homes. In addition to practical support, we also provide information to families, and campaign for the rights of people with complex disabilities to take part in life.

### About the Sense Data and Tech team

This is an exciting time for data and technology at Sense. We are embarking on a technology and data driven transformation to use data to make better, faster decisions, to



use technology systems drive efficiency and automation, and create a place where simple, intuitive technology frees up our people to do what they do best – be themselves.

It's a bold vision, and to achieve it, the Data and Technology team is central to the design, delivery, and rationalisation of our technology solutions, to meet the aspirations of our people.

Our vision for Data and Technology, from the Sense Data and Systems Strategy is that it will be:

- **User centred** – easy to use, intuitive, easy to find and available to all who need to use it.
- **Accessible for all**, leading the way in meeting all accessibility needs.
- **Consistent** in tools and approach across all departments and directorates.
- **Reliable** – available, secure, trustworthy and transparent.
- **Continuously improved** – bugs repaired; new functionality delivered on an iterative basis; systems selected with rolling development programmes<sup>1</sup>
- **Integrated and automated** – with a preference for machine-to-machine interfaces for data transfers.
- **Compliant with legislation** and supportive of our statutory and legal obligations

Our technology is based on Microsoft platforms, and we are making a major investment in a new Dynamics-based CRM system, with more application evolution planned in the next few years.

---

<sup>1</sup> Sense will procure systems that are being developed by their vendor, and adopt cloud delivered solutions where possible, taking advantages of evergreen principles inherent in these solutions.



## About the role

### Objectives

This role is focused on ensuring the Sense technology estate is secure and compliant, that changes to the estate are evaluated and approved before they are made, and that Sense technology users are supported in their role in keeping our information and data systems secure.

The role will work across all our internal teams and technology suppliers, assessing and monitoring their security measures and ensuring that Sense cyber security risks are managed appropriately. This will include establishing and leading a Cyber Security Governance Group (CSGG).

The role is responsible for managing Sense Cyber incident response plans and pro-active training of everyone in Sense to ensure a good level of cyber risk awareness and mitigation.

Achieve and maintain Cyber Essentials Plus accreditation and manage the technology elements of our annual renewal for the NHS DSPT (Data Security and Protection Toolkit) and other accreditations/assessments collaborating with the Data Protection and Information Governance Lead.

### Key responsibilities

- Develop and manage the cyber security risk management plans for Sense
- Manage a register of all Sense technology suppliers, and conduct routine cyber security assessments based on risk level
- Conduct regular audits and reviews of activities and threat protection.
- Develop and maintain training programmes for all staff using a risk-based approach, including enhanced training for system administrators.
- Deliver phishing simulation exercises and other cyber security training exercises



- Plan and deliver cyber security focus week(s), working closely with data protection teams and internal communications teams.
- Represent Cyber Security within Technology Change Approval Board (CAB) and Technical Architecture Group (TAG) processes
- Manage specialist Cyber Security suppliers, including suppliers for penetration testing, security evaluation and cyber insurance, in collaboration with teams across the business.
- Ensure Cyber Security and other technology risks are represented in Business Continuity planning and support BCP testing and exercises across all business areas.
- Work with other members of the Data and Technology team on shared campaigns and initiatives.
- Report regularly on Cyber Security matters to Sense Leadership and Executive Teams.

## Person specification

- Good knowledge of Cyber Security principles and threats.
- Good stakeholder management and communication skills
- The ability to communicate effectively using non-technical language
- Supplier management skills, including the ability to work in a multi-supplier environment
- Knowledge of Cloud architectures and the principles of virtual networks and Software-as-a-service from a security context
- A methodical approach with good organisational skills
- Experience of achieving Cyber Essentials Accreditation and/or NHS DSPT or equivalent
- A recognised Cyber Security certification, for example CISSP or CHCSP, or be working towards a suitable qualification.



## Knowledge and Experience

- A good knowledge of Cyber Security principles, and the implications of varied technology architectures, for example cloud solutions, software-as-a-service, zero trust architecture
- Experience of working with suppliers, including evaluating the Cyber Security implications of proposed solutions and managing assurance reviews and exercises
- Experience of working in a large multi-site organisation with a diverse range of user knowledge and technology usage
- Experience of using Cyber Security tools and systems, ideally using Microsoft products, or working within Microsoft ecosystems
- Experience of training non-technical staff in aspects of Cyber Security
- Evidence of own continuing professional development.
- A demonstrable commitment to enabling an inclusive and diverse workforce to reflect our community.
- A commitment to people with complex communication and Sense's vision and values; a willingness to learn how to communicate with people with complex communication and identify the barriers to their participation in all aspects of Sense's work.

## Skills

- 5
- SFIA 8 Information Assurance (INAS) level 5
- SFIA 8 Supplier Management (SUPP) level 5
- Satisfactory standard of literacy and numeracy.
- Satisfactory level of IT literacy.

## Personal circumstances

- Some national travel may be required for project and supplier management activities.



## Our values

Everything we do is underpinned by five core values. These values shape the way we work as we pursue our vision of a world where no one, no matter how complex their disabilities, is isolated, left out, or unable to fulfil their potential.

- We include
- We collaborate
- We find a way
- We challenge
- We celebrate

## Other information

- This job description does not form part of the employment contract.
- This post is not exempt from the Rehabilitation of Offenders Act.

**June 2025**