

# Yorkshire Housing Role Profile

<b>Job title:</b>	Cyber Security Manager	<b>Leader of others:</b>	Yes
<b>Reports to:</b>	Head of Technology	<b>Contract type:</b>	Agile - Homeworking
<b>Business Area</b>	Technology, Insight and Change	<b>Budget holder?</b>	No

## Role purpose

The Cyber Security Manager works within the Technology, Insight and Change Directorate and reports directly to the head of service. In collaboration with the Information Security Manager you will ensure that security is maintained across Yorkshire Housing's technical infrastructure.

This hands-on role will lead a small cyber security team and together will ensure the protection of Yorkshire Housing's systems and information assets from cyber threats.

As part of the Technology, Insight and Change Directorate, the role holder will work collaboratively with their peer group and the wider business to strive to deliver an exceptional colleague and customer experience.

## Key responsibilities

Develop security architecture and technology solutions to address the growing cybersecurity and compliance requirements of this profitable charity

Ensure new projects involving technology build security into the solutions, including any updates required to the infrastructure

Review the existing cyber security architecture, identify gaps and recommend appropriate enhancements based on evaluation of YH's business strategy and the threat landscape

Identify security risks associated with business process and operations and advise on appropriate operational security controls

Lead a team of cyber security engineers who are responsible for managing a number of operational security controls

### Portfolio Delivery

- Responsibility for establishing security requirements as part of a new system implementation, testing and challenging at all stages of development into business-as-usual operations
- Provide oversight and champion the implementation of security requirements ensuring 'security by design' is a core principle in new system development
- Identify security design gaps in existing and proposed architectures and recommend changes or enhancements

- Liaise with stakeholders across YH in relation to cyber security issues and provide timely support and future recommendations
- Document all appropriate security design decisions and customisations to future-proof the security of systems
- Demonstrate compliance with industry standards, such as NIST, Cyber Essentials etc
- Provide technical support to the delivery of projects involving IT in relation to security issues

### **Operational Security**

- Responsible for the operational management and monitoring of security across the organisation's data, systems and networks
- Provide direction and advice related to the security technologies to strengthen the overall cybersecurity posture
- Provide support during technical deployment, configuration, integration and administration of security technologies
- Oversight of configuration management to ensure solutions remain secure
- Responsible for ensuring security controls and processes are considered as part of the change management process
- Act as the deputy Cyber Security Incident Response Lead in the event of a security incident
- Supported by other incident responders from across YH, manage the technical response to a cyber security incident
- Responsible for maintaining and testing the technical playbooks that support the CSIRT
- Contribute to effective disaster recovery plans and methods to ensure business continuity in the event of any security breaches
- Support the delivery of cyber security training (specifically regular phishing exercises) and help raise awareness of security issues across Yorkshire Housing
- Responsible for 1st line security risk assessments, contributing to risk policies, providing input in risk decisions and fostering a risk-aware culture.
- Ingest threat intelligence from multiple sources and include in threat modelling activities and/or attack surface analysis
- Responsible for ensuring the Information Security team is supported whilst determining the appropriateness of third party supplier's technical security controls
- Lead the technical response for audit activity in relation to security controls
- Responsible for supporting investigations (internal & external) with the collection and provision of data to an evidential standard
- Ensure team processes are effective, documented and regularly reviewed

### **Communication & Engagement**

- Promote a security culture across the organisation ensuring that Information Security remains a top priority for all business areas
- Collaborate with the Information Security Manager on all security matters
- Form positive close working relationships with stakeholders across Yorkshire Housing
- Manage operational relationships with our cyber security partners and other third-party suppliers, ensuring appropriate SLAs are in place and monitored
- Build and maintain relationships with stakeholders across other organisations to ensure that Yorkshire Housing's technical security environment reflects current thinking and good practice

- Stay abreast of developments in cyber security technology ensuring that Yorkshire Housing continues to use the best available tools to manage security across the technical landscape
- Tracks industry and application trends and relates these to planning current and future IT needs
- Contribute to the development and maintenance of information security and other related technology policies, procedures and standards, challenging at all stages to support a culture of continuous improvement
- Communicate technical issues in a clear and concise way that can be understood by a non-technical audience

## **What you'll bring to the role**

### **The main things:**

#### **Experience & technical skills**

- Working knowledge of security architecture methodologies such as SABSA
- Relevant Information Security certification (e.g. CISM, CISSP, GIAC, CEH, CCSP) or willing to work towards
- Practical experience of working in a cyber security role including the development and management of security controls including securing cloud services for a minimum of 5 years
- Experience of security monitoring including use of a Security Operations Centre (SOC) and/or Security Information and Event Management (SIEM) tools
- Extensive knowledge of technical security controls including firewalls and intrusion prevention systems (IPS), endpoint security, web filtering, email filtering and network security logging and monitoring
- Experience of supporting secure infrastructure change through to business-as-usual operation, maintenance and support
- Ability to provide security expertise, guidance and assurance to a complex change portfolio
- Able to provide oversight of testing plans, recording of results and remediation recommendations
- Experience of administering and supporting security technologies
- Proven team leadership with the ability to motivate and mobilise individuals outside of their reporting line
- Flexible and willing to work outside of normal business hours on an occasional basis

#### **Personal Skills**

- Great communication and interpersonal skills, with an approachable style
- Excellent written skills (English)
- Committed to continuous personal and professional development, using own initiative to seek out opportunities to learn new skills and technologies
- A natural coach, able to support and develop others
- Meticulous, organised and able to systematically plan work to ensure delivery to deadlines
- Builds trust and credibility with stakeholders quickly and establishes strong networks across an organisation

### **A bonus if you have:**

- A degree in a technical or cyber security-related subject

## Our values:

Our values describe what matters most to us, and what our colleagues should expect from each other. We're all expected to show how we support and live up to these values in our work.

**Create trust** • Do the right thing, not the easy thing • Be honest and open • Do what you say.

**Be curious** • Think differently • Ask questions • Keep learning.

**Make it happen** • Own it • Do it • Be empowered.

**Achieve impact** • Do things that matter • Deliver results • Show pride and passion.

**Have fun** • Enjoy work • Be yourself • Stay connected.

We want colleagues to feel free to be themselves - so we're all responsible for making sure we promote a culture of equality, diversity and inclusion. And, as you'd expect, we're responsible for our own health and safety, following our policies and doing any training needed for our roles.