Yorkshire Housing Role Profile

Job title:	Information Security Manager	**Leader of others:**	Yes
Reports to:	Head of Data, Performance and Information Security	**Contract type:**	Agile - Homeworking
Business Area	Technology, Insight and Change	**Budget holder?**	No

Job purpose

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

This role supported by an information security analyst will develop, implement and manage the overall information security strategy to ensure the protection of Yorkshire Housing's systems and information assets from information security threats.

The Information Security Manager is not expected to provide hands on cyber security engineering, but the role does require a proficient level of technical understanding to work with Technology colleagues.

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

Strategy, Policy & Assurance

- Develop and implement Yorkshire Housing's information security strategy, policies, and standards collaborating proactively with stakeholders to align to operational business and IT delivery
- Lead on the development and implementation of plans to improve Yorkshire Housing's cyber security maturity rating
- Determine the relevant security controls required to protect YH based on its business strategy
- Designs and operates information security controls assurance in collaboration with internal and external stakeholders to ensure compliance with applicable security standards, such as ISO 27001 and the NIST Cybersecurity Framework
- Work with third-party security providers to oversee and coordinate information security audits and reviews, providing recommendations on improvements to senior management

- Work collaboratively with our security partners to orchestrate regular penetration testing to identify potential vulnerabilities, devising and implementing remediation plans to mitigate risk

Risk Management

- Manage the operational risk management process for information security, conducting regular risk reviews and providing reporting (KRI's)
- Responsible for providing reporting on information security risk back to the business to allow decision making
- Collaborate with the Cyber Security team on the creation of the Information Security roadmap ensuring that activities are driving down risk in line with YH's risk appetite
- Collaborate with cross-functional teams to identify, assess, and mitigate day-to-day information security risks and vulnerabilities, escalating to senior management where appropriate
- Stay abreast of emerging cybersecurity threats, assessing their potential impact and risk to the organisation and developing plans to ensure appropriate security controls are in place and kept up to date

Cyber Security Incident Response

- Lead on development and management of the cyber security incident response plan ensuring that procedures are in place to enable Yorkshire Housing to effectively respond to and recover from any information security breaches
- Act as the cyber security incident response lead in the event of a security incident
- Responsible for running regular cyber security incident response exercises

Training & Awareness

- Responsible for designing and delivering an effective information security awareness program that motivates colleagues and changes poor behaviour
- Owns the phishing exercise schedule, designs the exercises and who to target and manages reporting, as well as follow-up training
- Designs and runs security awareness campaigns including regular messages on the colleague intranet and activity during Cyber awareness week

Third Party Security Assurance

- Provide support to the procurement process by assessing the information security risk of YH's third-party suppliers (new and existing) where they have access to YH systems or information assets
- Articulate the information security risks of working with individual suppliers and recommend mitigating controls, where appropriate

Communication and Engagement

- Manage a small team of information security professionals, providing leadership, guidance, and support
- Manage operational relationships with our information security partners and other third-party suppliers, ensuring appropriate SLAs are in place and monitored
- Support the development of the Business Continuity Plan, ensuring plans include appropriate consideration of security controls

- Establish and maintain channels of communication and effective engagement across a network of technology and information specialists, conducting meetings to address known issues and sharing knowledge where appropriate.
- Act as an escalation point and arbitrate when security issues are raised by customers, colleagues, or third-party providers, resolving issues in a responsible and professional manner.
- Act as organisational expert and point of contact on all matters relating to information security.

The above list of duties is neither exhaustive nor exclusive. The post holder is expected to undertake duties commensurate with the responsibility and level of this post.

What you'll bring to the role

The main things:

Experience & technical skills

- Established Information Security professional with experience of implementing security frameworks (e.g., ISO27001, NIST, Cyber Essentials)
- Experience of developing and delivering information security policies and procedures, including practical experience of embedding policy across an organisation
- Technical risk management and impact assessment skills, including an awareness of security risk mitigation approaches
- Knowledge of technical security controls including firewalls, intrusion detection / prevention systems, endpoint security, DLP, encryption and identity and access management
- Relevant Information Security certification (e.g., CISM, CISA, CISSP, CEH, CCSP) or willing to work towards
- Practical experience of working in a cyber or information security role across multiple domains
- Experience managing the response to information security incidents, including liaison with other teams, senior management and third-party organisations
- A thorough understanding of relevant legislation affecting the delivery of IT services (e.g., GDPR, Computer Misuse Act, RIPA)

Personal Skills

- Strong leadership and managerial abilities, with a proven record of managing and developing people
- Excellent communication skills, with the ability to effectively convey complex security concepts to both technical and non-technical stakeholders
- Ability to write concise, plain English that is tailored to the audience
- Committed to continuous personal and professional development, using own initiative to seek out opportunities to gain experience in new skills and technologies
- 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

It would be 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.