Cyber Security Manager

Information Technology – Information, Systems and Change

Role profile

Overview	
Role Purpose	The primary role of the cyber security manager is to ensure all system, information and data across NHG manage are safe and secure for staff, residents and stakeholders in NHG. An expect in analytically assessing an information security situation and then reacting appropriately. This role is not limited to simply responding to events if needed – that is a daily reponsibilty. The cyber security manager creates and assesses security plans for existing vulnerabilities, prioritises security strategies to best cover strategically important data, analyses reports generated by the Microsoft Security Stack, threat & vulnerabilities monitoring systems, penetration test, cyber awareness, phishing campaigns and maintaining security risks scores across the entire system estate. The Cyber Security Manager lives and breathes cyber security, running continuous testing to anticipate future issues using defence in depth, MITRE and NIST frameworks to define approaches to proactively respond to threats and vulnerabilities. The Cyber Security Manager leads and manages the security department's team, working closely with the Head of Cyber Security, Head of Infrastructure and Director of IT. Additionally actively engages with the wider IT community and builds strong and enduring personal relationships with the business to promote a security first culture. Communication is key to ensure the continual importance of cyber security and involves any department in the organization, so that issues can be taken care of quickly as well as ensuring that all follow information security policies and procedures. This includes keeping abreast of the current information security landscape across the sector. Typical duties include creating and maintaining information security policies and procedures, selecting and implementing new information security technologies, creating information security training programs and interviewing potential information security team personnel.
Responsible for	• Provide information security awareness training to organization personnel • Supporting the Head of Cyber Security for the development of cyber security strategies • Oversee information security audits, whether by performed by organisation or third-party personnel • Manage security team • Provide training to security personnel during onboarding • Assess current technology architecture for vulnerabilities, weaknesses and for possible upgrades or improvement • Implement and oversee technological upgrades, improvements and major changes to the information security environment

Role profile

	• Serve as a focal point of contact for the information security team and the customer or organisation • Manage and configure physical security, disaster recovery and data backup systems • Communicate information security goals and new programs effectively with other department managers within the organization • Attending Housing Warp and Collective Intelligence Forum in Sector. • Ability to mentor junior staff members in cyber security with a view to making them ready for the next step in career. • Defines learning pathways for staff, tailored to individual and supporting NHG operational objectives. • Works closely with our security related supplier to ensure they deliver to contractual SLA. • To identify and assess complex security risks and control, and relate them to the business environment • Works closely with the Architects to ensure new systems/technologies meet Information security requirements as per Architectural and Security principles • Understanding of data and information security architecture across the NHG IT estate -both internal and SaaS systems and Infra. • Expert in Microsoft Security Stack including intrusion detection, intrusion prevention and perimeter defence across internal and customer facing systems. • Understanding of trends and analysis required for event monitoring across the system estate, in addition lead and coordinate penetration testing and vulnerability assessments. • Good understanding of threats and vulnerabilities in the world in general and how it would impact a housing association and property service provider. • Champion and technical expertise for all items related to information security. • Good intelligence and networks with central cyber and information security agencies. • Close working relationship with Governance and compliance in regards to all information security items and data protection. • Stay up to date with changes in the Cyber Security World to identify emerging threats, how they could pose a risk to Genesis and identify mitigations • Maintaining professional and technical knowledge by attending educational workshops, reviewing professional publications, establishing personal networks, benchmarking state-of-the-art practices and participating in professional societies. • Cyber security strategy development and delivery. •
Reports to	• Head of Cyber Security
Line management	• 3 Cyber Security Analysts • Cyber Security Apprentice
Date	12 May 2023

Role profile

Role relationships	
Internal	Executive Board and other committees Directors Heads of Service Managers Directors, Head of Service, Mangers and Executive Board
External	Represent NHG at various forums and meetings as necessary Auditors G15 and other peer colleagues

Role accountabilities

Leadership

- Provide strong leadership for cyber security team.
- Provide strong and effective leadership to implement and manage agreed plans aligned with NHG's values to ensure the best possible results.
- Effectively promote collaborative approaches to engage reporting team(s) to work successfully to deliver high quality services with cost-effective outcomes.
- Establish and maintain a culture of service improvement, supporting staff to deliver change projects to meet developing and evolving customer needs.
- Proactively provide relevant senior level advice and guidance as required.
- Lead your team in line with NHG's management behaviours in order to get the best out of your staff.
- Represent NHG externally; develop and maintain NHG's reputation as appropriate and build effective relationships with relevant stakeholders.
- Support the Head of Cyber Security to develop, a 5-year cyber strategy to support NHG's integration plans and corporate strategy.
- Effectively promote collaborative approaches to engage reporting team(s) to work successfully to deliver high quality services with cost-effective outcomes.
- Represent NHG externally; develop and maintain NHG's reputation as appropriate and build effective relationships with relevant stakeholders.
- Ensure that you and your teams follow relevant Health and Safety policies and related procedures, keeping up to date with changes and acting to maintain personal health and safety and that of others.

ıation Technology

- Maintaining and managing the entire security stack for threat and vulnerabilities
- Continue to develop and implement a '21st Century' IT team that can support new technologies need by NHG to modernise operating models.
- Develop successful relationships with external partners in-particular in XDR, MDR and SOC services.
- Ensure core elements of service delivery are conducted in compliance with legislation, regulation and NHG policy.
- Establish and maintain positive relationships with internal client teams.
- Staff Recruitment and personnel development

General

- Ensure you follow the financial regulations, policies and procedures at NHG.

Role profile

● Ensure that you follow relevant Health and Safety policies and related procedures, keeping up to date with changes and taking action to maintain personal health and safety and that of others.
The tasks and responsibilities outlined above are not exhaustive, the post holder may undertake other duties as is reasonably required.

How do you meet the role requirements?

To do the job well, we have outlined the key behaviours we'll expect of you, and the knowledge, experience and skills you need to do the job. You'll be assessed on these criteria at various stages throughout the selection process.

Role behaviours	
Customer focus	● Commit to providing the best service to customers, set realistic expectations, keep your promises, and act with integrity always. ● Lead on commercial awareness / VFM in your team. Make decisions and recommendations in line with this. ● Promote a culture that balances the needs of the internal customer with those of the business/IT ● Learn lessons from your experience and ensure that they lead to genuine change to allow for continuous improvement
Accountability and delivery	● Be accountable for the accuracy and completeness of your work, remaining calm under pressure, making informed and reasonable decisions. ● Take well considered risks and monitor and manage risk proactively. Manage the Risk Management process for IT ● Identify and interpret the impact or opportunities posed by the external environment
Service improvement	● Approach your work with rigour, challenging yourself to identify opportunities for service improvement, working in partnership with others to make NHG better for customers and colleagues. ● Seek out and encourage others to seek out and implement improvements. ● Translate changes in business strategy into practical actions for teams ● Be persuasive, passionate and enthusiastic about introducing new ways of working to maximise services ● Develop a culture of continuous improvement, ensure learning from previous issues and new solutions are shared to achieve excellence in customer service
Communication and inclusion	● Communicate clearly and openly, including all and celebrating differences, listening and responding positively to others. ● Be emotionally intelligent and self aware ● Develop effective networks internally and externally for shared gain

Role profile

	• Consider the needs and concerns of all stakeholders and deliver difficult messages clearly and effectively, with respect and sensitivity
Management	• Lead by example and with empathy, ensuring your team deliver on their promises; getting the best from your staff by offering them appropriate support, guidance, and development • Provide clear and decisive leadership at all times, and particularly through change and uncertainties • Set an example and inspire others to achieve the NHG vision • Communicate corporate and department goals and create a working environment that empowers and supports others to take responsibility to achieve these
Dimensions: Financial	• Ensuring Value for Money for new and existing implementations • Ensure the projects are delivered within budget (and scope) • Owns & maintains all IT contracts within security applications
Dimensions: Non Financial	• Recruitment and management of staff, • Successful implementation of the cyber security programme and all BAU systems solutions • Owns the teams monthly IT/ISC performance/report/dashboard • Presentations of cyber solutions in business terms to senior leadership teams • Development and maintenance of Cyber Security Strategy.

Essential knowledge, experience and skills	
Professional expertise (know how & experience)	• CISSP, CISM or alternative cyber security qualification. • Threat and Vulnerability management • Understanding of ISO27001, cyber essentials • NIST framework. • Working knowledge of data protection legislation including GDPR, principles of information security and governance including NIST 800 and PCI-DSS • Threat Intelligence network with NCSC and Security suppliers.
Skills	• Cyber security strategy development • Developing and managing relationships across IT and within the business • Strong influencing skills and negotiation skills • Good communication skills and ability to build relationships • Ability to explain IT security risks to business stakeholders and be able to relate these to corporate risks • Understanding of threat and vulnerabilities modelling across the IT perimeter. • Being able to explain decisions clearly • Documentation and clear writing skills • Presentation skills to higher management levels within the organisation • Manage simultaneously and conflicting priorities • Experience in Microsoft Sentinel and KQL/threat-hunting

Role profile

	• Experience in Microsoft Windows Defender for Cloud, Mobile (Android and iPhone), and Endpoint (Server and Workstations), configuration, deployment, architecture, management, and reporting. • Experience in Microsoft InTune and SCCM technologies for deploying security baselines, Antivirus technologies and configuration and compliance profiles • Experience with SIEM/SOAR/MDR platforms and working with managed SOCs • Experience with vulnerability management (TVM, Qualys) • Basic understanding of operating under a zero-trust security methodology • Technical experience with Microsoft Identity and Access management (Azure Active Directory, Azure Active Directory premium solutions, Conditional Access, SSO, MFA, PIM). • Documentation and report writing skills, good communication skills, and meticulous attention to detail • Desire to progress across the broader aspects of Information Security
Qualifications and/or professional membership	• Good knowledge of Information Security concepts and standards (CISSP qualification desirable) • Good knowledge and experience of Microsoft Azure infrastructure and security concepts and tools (Desirable qualifications include Microsoft Security Administrator) • Knowledge of ITIL Framework

Role requirements	
DBS	• Yes
Data and information processing	• Information/Data User across all systems and databases
Data protection role	• Cyber Security Champion • Information Champion • Data Owner • Data Steward