ROLE PROFILE

Job Title:	Role Reports to:	Business Function:	Evaluated Grade:
Information Security Analyst (Technical)	**ICT Head of Security & Governance**	**ICT Comms & Tech**	**D**

Job Purpose:	**Key Competencies:**
Take the lead and provide technical expertise and support for a range of security related activities, engaging with ICT and Business stakeholders in business as usual, change management and new project design and delivery, supporting plans to develop and improve Information Security and compliance to all ISO and other standards and regulations at YHG	• Flexibility & Resilience • Meeting Customer Needs • Interpersonal Understanding • Results Focus • Commercial Focus • Future Focus • Problem Solving and Decision Making • Gathering/Seeking Information • Building Relationships • Impact & Influence

Key Responsibilities:

1. Identify, assess, report and mitigate technical security related risks, threats and vulnerabilities within business processes, projects, systems and third-party data supply chain.
2. Ensure all application components are fully supportable and secure, including privilege and standard user access control management.
3. Work with ICT and business stakeholders to support the development of secure and compliant IT and business solutions including the secure design, deployment and operation of cloud and on-premise infrastructure/services, incorporating appropriate compliance processes such as data deletion, pseudonymisation, encryption or other security measures.
4. Work with ICT and business stakeholders to develop and implement cloud security best practices, including PaaS (Platform as a Service), SaaS (Software as a Service), IaaS (Infrastructure as a Service).
5. Provide ICT and business stakeholders with technical security and risk assessment support.
6. Administration of security-based technologies, both cloud and on-premise inc. access controls, content filters, DLP (Data Loss Prevention), mail gateways, MFA (Multi-Factor Authentication) and MDM (Master Data Management).
7. Support the implementation of compliant and consistent encryption technologies across the YHG infrastructure.
8. Establish effective relationships with senior ICT and Business stakeholders providing subject matter expertise, ensuring engagement on business and technical projects which could introduce information security/data privacy risk.
9. Work as part of the YHG ICT Security team across a number of security improvement work streams, acting as security lead on multiple projects simultaneously, proactively identifying areas for improvement, developing project plans and driving the execution of these plans to ensure project success.
10. Provide risk assessments across all ICT projects, including advice and guidance on appropriate measures & controls.
11. Engage with the DevOps team for the design and development of secure business applications and solutions.
12. Participation at key management and governance bodies including ICT CAB (Change Advisory Board), ICT Risk Management Committee and the Technical Design Authority.
13. Provide security guidance in all stages of ICT project and change delivery, including performance of risk and impact analysis on proposed changes and projects to the security infrastructure.
14. Manage Information Security risks with third party Data Processors, including strategic ICT partners, to ensure emerging threats, implementations or changes to control frameworks are understood and incorporated.
15. Coordinate and manage third party supplier security reviews for new and incumbent suppliers, to ensure YHG effectively manage their data supply chain security risks, including supplier risk assessments, contract reviews and privacy impact assessments.

16. When required work with third party suppliers to ensure compliance with YHG's security process and standards.
17. Support regular major incident and disaster recovery rehearsals.
18. Ensure business continuity and disaster recovery capabilities, developing and implementing business continuity plans to ensure service is continuous when a change programme is introduced, a security breach occurs or in the event that the disaster recovery plan is invoked.
19. Plan, develop and implement Information Security Training & Awareness initiatives, including the delivery of IS related presentations across YHG as required;
20. Evaluate and report on new and potential beneficial security technologies.
21. Help to develop and maintain the suite of Technical Security Standards necessary to ensure a consistent and up to date technically secure environment.
22. Build positive relationships with developers, infrastructure, applications and governance colleagues within ICT Services.
23. Undertake additional duties appropriate to the role and/or grade.

	Essential	Desirable
Knowledge	• Understanding of applying the GDPR (General Data Protection Regulations), PCI DSS (Payment Card Industry Data Security Standard) certification standards, and other related legislation, standards and codes of practice • A good working knowledge of information security including ISO/IEC 27001 Information Security Management Standard & ITIL • Knowledge of digital and cyber security principles and prevention methods • Demonstratable knowledge of both business and technical aspects of information security, including third party security risk • Administration of on-premise and cloud security-based technologies • Demonstrable knowledge of relevant exploits and vulnerabilities, their effects and mitigations • Understanding of security risk, threats, attack techniques and related incidents and issues.	

	Essential	Desirable
Skills	• Ability to influence internal and external stakeholders on matters relating to security and information risk • Good verbal and written communication skills, with ability to communicate effectively at all levels • Strong analytical skills applied to security requirements and relate these to appropriate security controls • Strong risk-based analysis and decision-making skills • Project Management and problem solving/ troubleshooting (technical and business) • Ability to maintain a calm and process driven focus when reacting to an adverse situation. • Self-motivated and able to work independently/without supervision (manage own workload); • Good planning & organisational skills • Collaboration and interpersonal skills (effective team player)	

	Essential	Desirable
Experience	• Experience performing risk analysis, business impact analysis, control effectiveness reviews and vulnerability assessments • Ability to identify, assess, report and mitigate technical security related risks within business processes, projects, systems, and third parties • Development and maintenance of documented Technical Security Standards and Processes • Operating within and contributing to an Information Security Management System environment • creating well defined communications and educational material • explaining technical concepts to non-technical colleagues • managing organisation wide Information Security Risks • designing security controls and embedding in to change initiatives	

Qualifications/Education	• Educated to degree level in an IT Security related discipline • Recognised Information Security/ IT qualification, or working towards a relevant certification (e.g. CISSP (Certified Information Systems Security Professional), or commensurate experience	

People Management Responsibility?	No line management responsibility
Budgetary Responsibility?	No budgetary responsibility
Key Relationships (internal/external)	• ICT Operations, Applications & Infrastructure Teams • ICT DevOps Team • PMO • Operations • Marketing & Comms • Finance • Governance, Risk & Assurance
Safeguarding of Children Young people and Vulnerable Adults Your Housing Group is committed to safeguarding and promoting the welfare of children, young people and vulnerable adults and expects all staff to share this commitment. As a Your Housing Group employee, it is your responsibility to attend safeguarding training in accordance with YHG safeguarding training strategy and to be aware of and work in accordance with the YHG safeguarding policies and procedures and to raise any concerns relating to such procedures which may be noted during the course of duty.	

Key Role Performance Indicators
1. Establish an ICT Security Strategy, policy and procedures that are and remain relevant to the protection of YHG assets, customers and services. **2.** Develop and operate an annual programme of ICT security and general ICT control audits to improve security and adherence to the various policies and procedures operated across the ICT environment, Inc. penetration testing and other cyber related threats **3.** Liaise and manage all ICT related security incidents, internal and external ICT audits and follow up reviews to an agreed and satisfactory conclusion **4.** Lead, maintain and execute an ICT Security Risk Management Framework, meeting regularly and collaborating with the wider Governance and Compliance functions within YHG accordingly. **5.** Deliver and demonstrate through annual testing our capability to recover against a full range of DR scenarios as set out in the Groups BCP. **6.** Through the correct implementation of an ICT Info Sec strategy prevent any major breaches of data or regulation that would have a material impact financial or reputationally to YHG

Date Role Profile Created/Updated:	**March 2019**