JOB DESCRIPTION

Job Title:	Information Security Specialist
Department:	Information Communication Technology
Agenda for Change Grade:	Band 7
Reports To:	Head of ICT – Business Delivery
Key Working Relationships:	▪ Senior Information Risk Owner (SIRO) ▪ Executive Directors ▪ Trust Risk Manager ▪ Divisional Directors and Managers ▪ Head of ICT ▪ Information Governance Manager

Role Summary

The post holder will act as the designated specialist on information security for ICT Directorate and provide expert specialist advice, in accordance with national and local IM&T security policies across the Trust. The post holder will also be responsible in supporting the Senior Information Risk Owner (SIRO) function and Head of ICT – Business Delivery in assurance that the Trust is meeting its requirements both locally and nationally.

The Information Security Specialist will be responsible for leading and Identifying areas in which the Trust is inadequately covered by ICT security policies and procedures and, in consultation with other ICT specialists within the Directorate and Information Governance develop new policies and procedures to cover these areas.

The Post holder is expected to provide information security expertise and be a focal point for Technical delivery and response and procedural advice. The role will encompass:

- Monitoring, reporting and recording of own projects and their timelines
- Managing the daily and ever changing priorities ensuring that duties are executed with consideration given to demand and resources.
- Be a key figure for IS System development and support.
- Operate a number of core security products to enforce and deliver ICT policy
- Prepare highly complex and or sensitive reports, policies, incident logs and recommendations.

- Act as the focal point for technical and procedural authority for the IS function of the Trust.
- Performing risk evaluation and formal assessments.
- Lead the assessing sing of testing and measure IT systems for vulnerability.
- Ensure the Information Security Strategy links into the overall IM&T strategy for the Trust and is reviewed annually ensuing assurance and compliance.
- Ensuring the Information Asset Register and ICT Request systems are continually developed, maintained and updated providing regular statistical/information reports to support Directorate.
- Adequate information security management and assurance arrangements are in place that comply with the Trusts current information security obligations.
- Senior management at Executive Team and Trust Board level are informed of changes and performance issues which need to be considered and addressed through the Senior Information Risk Owner (SIRO).

Key Job Responsibilities

1. To be the designated specialist on Information Security, provide an expert specialist advice service in accordance with national and local IM&T security policies.

2. Provide support to the SIRO in the delivery of his/her responsibilities and duties across the Trust ensuring compliance and assurance.

3. Act and provide expert speciality advice and support to the ICT directorate and the Trust in relation to IT security standards ISO 27001/ISO/IEC27002 (where relevant). Act as the focal point in supporting Trust staff in dealing with queries relating to ICT information security questions.

4. Lead on the ICT Systems approval process, and ensure that new systems/changes to systems meet all legal and other requirements.

5. The nature of the post will mean that some activities may require completion outside normal core office hours.

General

6. Lead the development of the annual information security Directorate objective plan and strategy by discussing and agreeing information security work programmes with the Head of ICT – Business Delivery and providing in-year monitoring on progress towards delivery.

7. Lead the co-ordinate the ICT Process/Systems approval process, and ensure that new systems/changes to systems meet all legal and other requirements. Liaising with

requestors/customers to understand and support their requirements

8. Supporting the SIRO in providing guidance and advice on corporate records management issues to all Trust staff contributing to all new developments to ensure they meet all Records and Data Management standards as per the IG Toolkit.

9. To attend the Information Governance Committee as and when necessary to provide highly complex and expertise information regarding information security and improvement plans identified through the IG Toolkit. Provide support by making an expert assessment of current information security and proposing measures to develop technical and managerial measures to improve Information Security.

10. Lead in the establishment and maintenance of a register of data owners for sets of information (e.g. paper files, databases) assessing and educating/training the data owners on their responsibilities (what is the data, how is it used, who has access to it).

11. Lead regular ICT Directorate assessment of the Trust's ICT security baselines contained within Information Governance, Assurance Frameworks, N3 Statement of Compliance, BS7799/ISO27001 and other relevant audit tools. This will require the development of an in depth knowledge of these audit tools.

12. Develop/formulate highly complex action plans to address key risks arising from these assessments adjusting plans where necessary, Identify the key risks and propose solutions and obtain and manage the necessary funding and implement these action plans to improve the ratings of Trust and reduce the risks they face through ICT security issues. This will involve negotiating, presenting highly complex information and coordinating the input of key staff at all levels in ICT.

13. Schedule and implement ad-hoc audit programmes to test systems and data security measures, review/analyst findings and implement development/correction plans to improve and develop those system and data security measures.

14. Occasionally required to work flexibly to meet the demands of the service, e.g. to carry out investigations into possible ICT security breaches. This may require activities to be carried out outside normal office working hours i.e. evenings or weekends however, these will be the exception rather than the norm.

15. The post holder will be expected to travel across Trust sites to attend meetings and provide support across site when required, but also to other NHS organisations.

Information Security Policies, Procedures and Liaison

16. As the lead/expert on information security you will be required to write and implement policies and procedures ensuring internal/external network connections adhere to all appropriate security policies.

17. Log and report identified ICT risks in line with the Trusts risk management processes.

18. Identify areas in which the Trust is inadequately covered by ICT security policies and procedures and, in consultation with ICT specialists, data protection, information governance and Information Asset leads, assist in the development of new policies and procedures to cover these areas.

19. Working with the Head of ICT – Business Delivery be responsible for the development, production, review and update of IM&T security documentation and identify new policies for development: -

    - Information Security Policy
    - Internet Policy
    - Email policy
    - Network Security Policy
    - Remote Access Security Policies
    - Information Asset Policy

20. As the experts ensure compliance with legal, statutory, regulatory and contractual obligations in respect of IM&T security by providing an advisory service to the ICT Directorate and other Trust Directorates.

Training and Awareness

21. Plan, organise and deliver monthly Information Security specialist awareness workshops/training sessions on information security and its complexity covering corporate responsibilities and locally at a clinical service level that raises the awareness of all Trust staff and ensure compliance with policies and procedures.

22. Take personal responsibility for delivering information security awareness training programmes monthly and when required. Develop materials to enable others to deliver training in a standard manner.

Security & Investigations

23. As the lead specialist, based on own interpretation of security policy, conduct complex and contentious investigations into suspected or actual breaches of security and provide formal written reports advising how legislation and or policy should be interpreted directly to the SIRO or to the Head of ICT – Business Delivery.

24. Liaise with senior managers of Trusts, the Counter Fraud Service, the Police and external organisations, as required, when investigating incidents.

25. On request, provide regular reports or presentations of complex nature to the Information Governance Committee on the state of information security within the Trust.

26. Lead on ensuring that all new system procurements meet the security requirements of the organisations.

27. Investigations into abuse of ICT facilities such as Internet and e-mail may occasionally expose the post holder to distressing and sensitive images and require the post holder to act as a professional witness in disciplinary hearings etc.

Disaster Recovery

28. To plan and lead the development of disaster recovery and business continuity strategies for ICT Directorate.

29. To assess and monitor ICT disaster recovery plans ensuring they remain up to date at all times.

30. Initiate and lead regular exercises to test ICT business continuity and disaster recovery plans, summarise findings and improve the plans to reduce risks further.

Technical

31. To maintain a good understanding of technical systems and security issues pertaining to them, including but not limited to, Active Directory, firewalls, remote access systems, hardware, operating systems, applications software, networking protocols, etc.

32. To be responsible for assisting with any penetration testing.

33. To continuously review security of technical systems including hardware and software.

The post holder will be expected to be fully committed to and act as a role model for the Trust's corporate Values.

- Cherishing
- Excellence
- Finding a Way
- Innovation for Advancement
- Working Together

This job description is not exhaustive and is seen as a guideline for the post of Information Security Manager. It may be reviewed and changed in discussion with the post holder.

Additional Information:

Infection control

Staff will work to minimise any risk to clients, the public and other staff from Healthcare Associated Infection including MRSA and *C difficle* by ensuring they are compliant with the Health Act 2006 – Code of Practice For The Prevention and Control of Healthcare Associated Infections (They Hygiene Code); and by ensuring they are familiar with the Trust's Infection Control Polices, located on the Intranet.

All employees must comply with the Trust Infection Control Policy. All employees must attend infection control training as required within their department or as directed by their line manager.

Confidentiality

As an employee you have a responsibility to maintain the confidentiality of any confidential information which comes into your possession regarding patients, employees or any other business relating to the Trust

In accordance with the Public Interest Disclosure Act 1998 protected disclosures are exempt from this express duty of confidentiality.

Health & Safety

As an employee you have a responsibility to abide by all of the safety practices and codes provided by the Trust and have an equal responsibility with management for maintaining safe working practices for the health and safety of yourself and others.

All employees must comply with the Trust Infection Control Policy. All employees must attend infection control training as required within their department or as directed by their line manager.

Quality Assurance

As an employee of the Heart of England NHS Foundation Trust you are a member of an organisation that endeavours to provide the highest quality of service to our patients. You are an ambassador of the organisation and, as such, are required to ensure that high standards are maintained at all times.

Equal Opportunities

As an employee you have a responsibility to ensure that all people that you have contact with during the course of your employment, including patients, relatives and staff are treated equally in line with the Trust's Equal Opportunities Policy.

Risk Management

You have a responsibility for the identification of all risk which have a potential adverse affect on the Trust's ability to maintain quality of care and the safety of patients, staff and visitors, and for the taking of positive action to eliminate or reduce these.

Safeguarding

Heart of England NHS Foundation Trust is committed to safeguarding and promoting the welfare of children, young people and vulnerable adults who use our services. The Trust expects all staff and volunteers to share this commitment. As part of the selection process for this post you may be required to undergo a Criminal Records Bureau check and maintain ISA registration. If you are successful appointed, you will receive confirmation of which checks and/or registration you are required to have.

The Job Description is subject to change and may be reviewed by the manager in conjunction with the post holder.

The Trust operates a no smoking policy and is working towards a smoke free environment.