JOB DESCRIPTION

Job Title: Information Security Officer

Reporting To: Information and Cyber Security Manager

Department(s)/Location: Information Governance and Security within Information & Communications Technology

NHS Job ID:

1. JOB PURPOSE

Responsible for the co-ordination and execution of continuous review and improvement of all NHS 24 systems, to ensure security compliance. Selecting, liaising and managing suppliers to ensure contract obligations are met and all modifications to software and hardware adhere to NHS 24 and NHS Scotland policies, standards, procedures and relevant legislation.

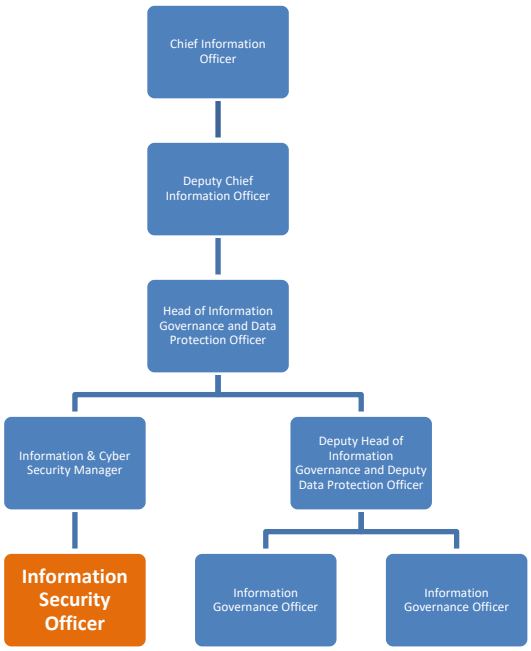
To act as the Lead Technical Security Authority within NHS 24 with responsibility for the three main areas of Information Assurance which are Confidentiality, Integrity and Availability of all information within NHS 24 and the associated Information Security Management System (ISMS) which is used to support information assurance and to ensure NHS 24 Security Policies are managed and updated by interpreting any and all technical, National policy or legislative change.

To provide professional advice as the lead technical security expert in NHS 24 leading the technology development of all security services, providing technical direction, leadership and expertise for all stakeholders, professionals, and staff across the whole of NHS 24 in support of both NHS 24 operations and NHS 24 Strategy.

To plan and ensure execution of the technology Information Security Audit across NHS 24. and ensure that the technology security apparatus within NHS 24 meets the needs of the organisation and provides value for money. Also Responsible for the security of all NHS 24 technology assets both deployed within the NHS 24 centre's or held within NHS 24 stock.

2. ORGANISATIONAL POSITION

The role of Information Security Officer reports to the Information and Cyber Security Manager. The role works closely with Service and Systems Delivery staff, ICT Technical staff, Information Governance staff, business representatives as well as suppliers and business partners.



3. SCOPE AND RANGE

NHS 24 provides the population of Scotland with access to clinical assessment, healthcare advice and information and aims to ensure that those contacting NHS 24 are given the assistance and advice they require in order to meet their health needs via the omni channel access. NHS 24 health services receive calls 24 hours a day and 7 days a week.

The Information Security & Governance function is responsible for ensuring the organisation is compliant with all legal and regulatory requirements for information. This includes all forms of information in all formats i.e., electronic files, published data, records, paper-based information. This function is also responsible for the physical security of the organisation's estate.

The ICT directorate also:

- Horizon scans for Health service and technology development.
- Prepares high level business case for service development.
- Develops Technology road map and provides capability to deliver against strategic goals.
- Measures benefits against planned outcomes both at Operational and Strategic level.
- Develops of relationships to build required capability.
- Provides for opportunity/improvement identification and delivery.
- Establishes and manages contracts required with partners.
- Establishes Information Security relationships with other Health agencies relevant to NHS 24.
- Delivers the Information Security Objectives within the NHS 24 Programme of Work on behalf of the NHS 24 Executive Team.

4. MAIN DUTIES / RESPONSIBILITIES

Information Security Management

- Responsible for co-ordinating all technical aspects of the Information Security Management System (ISMS) which provides a framework for aligning the technical aspects of security within NHS 24, protecting information and supporting systems with the international standards ISO 27001; ISO 27002 and ISO 27799.
- Interpreting National policies and legislation to ensure that the NHS 24 Security framework, Policies and Procedures are maintained and that NHS 24 adheres to relevant National policies or legislative changes.
- Responsible for the co-ordination and maintenance of the Information Security Management System (ISMS) across the entire technical NHS 24 estate, constituting:
    - The IT infrastructure which supports approximately 1800 user base,
    - 5 Main Contact Centres and Local Centres 24/7/365.

    - Data Centre, Data Disaster Recovery and Test and Reference Environments.
    - All main technical suppliers
- Development, Implementation and ongoing review of policies, procedures and technical solutions to safeguard all NHS 24 information and supporting systems.
- Ensuring that the ISMS continues to conform to the defined and published Management Executive and regulatory requirements as well as comply with ISO27001, Information security management using ISO/IEC 27002 thus ensuring the confidentiality, integrity and availability of all NHS 24 information assets.
- As the lead technical security expert in NHS 24, lead the technology development of all security services. providing technical direction, leadership and expertise for all stakeholders, professionals, and staff across the whole of NHS 24 as well as developing the Security components in respect of NHS 24 operations, the NHS 24 Strategy, and the Technology Roadmap.
- Develop Information Technology Security training materials and regularly deliver specialist training to all NHS 24 staff designed to instil a security conscious culture, enabling the objectives of the ISMS, security framework to be met.
- Monitoring of technology security risks introduced by new projects.

Business Continuity Management

- Responsible for the coordination of the provision and applicability of NHS 24's technical disaster recovery solution, to ensure the availability of NHS 24 data during an adverse event.

Business Change Management

- Responsible for coordinating with other business functions, changes due to the implementation of Security Policies, Processes and Procedures via appropriate communications and/or training. Providing expert advice as necessary.

Project Management

- As Lead technical Security expert within NHS 24 provide security expertise to NHS 24 projects to identify, manage and establish appropriate mitigation in respect of risk, to also ensure NHS 24 Security is not compromised and ensure adherence to National and NHS 24 Security policies.

Contract/Procurement Management

As Lead Technical Security Expert within NHS 24:

- Provide input and advice for all technology procurements to ensure that NHS 24 security requirements are defined within all contract specifications.
- Carry out NHS 24 supplier selection through evaluation of Suppliers responses in respect of Security.
- The post holder will be responsible for purchasing security certification for all NHS 24 websites.

Asset Management

- Responsible for the security of all NHS 24 Technology assets both deployed within the NHS 24 centre's or held within NHS 24 stock. e.g. Desktops, Monitors, laptops, Tablets etc. ensuring that these are securely held, appropriately tagged, tracked and issued.

Risk Assessment & Security Audit

Responsible for:

- Providing expert technical assistance to identify vulnerabilities and weaknesses in relation to all NHS 24 systems and infrastructure e.g. through the assessment of complex technical security designs of Supplier infrastructure and application design specifications.
- Investigating Information security issues \ threats to ensure minimal impact on NHS 24 e.g. actual and suspected breaches of information security, providing when required a written Executive report of each incident such as an Executive SBAR paper.
- Establishing formal relationships with suppliers, business partners and internal teams, identifying technical security risks and coordinates the implementation of appropriate corrective actions to minimise and mitigate against these risks.
- Coordinating the planning and implementation of security technologies, where required, to minimise security breaches thus safeguarding NHS 24.
- Leading technical security risk assessments against the relevant ISO/IEC standards range (e.g. ISO/IEC 27001) for applied changes, upgrades and new system implementations.
- Planning and Executing information security reviews for operational systems and changes.
- Carrying out the ongoing examination of all aspects of Information Security within NHS 24 to ensure that security governance and controls are in place as part of continuous service improvement and ensure that these measures are continually being met.
- Monitoring, by various methods, on a regular basis the activities of staff and third parties ensuring compliance with security policies and procedures.
- Determining the level of security required for all new NHS 24 production systems.
- Assessing the relative sensitivity of data used by existing and new systems within NHS 24 and as technical Lead expert advise on the appropriate levels of security.
- Ensuring that the rules for confidentiality, security and release of data for use within NHS 24 conform to National and NHS 24 Information Security Policies and are being observed by all staff.
- Developing and maintaining physical and other security arrangements for NHS 24 and monitor that conformant procedures are being observed.
- Liaising with Users, Internal Audit, Suppliers and the Information Governance group on a formal basis regarding data security and audit.
- Ensuring appropriate communications are presented across the organisation to promote security awareness and reduce the risk of security incidents either by accident or intent. As Lead Technical expert this would involve facilitating workshops, running training sessions and attending cross departmental team meetings as necessary.
- Providing input on all aspects of technical information security.

5. SYSTEMS AND EQUIPMENT

- Responsible for the Governance and Security of all NHS 24 systems
- Ensures that NHS 24 security requirements are defined for all NHS 24 systems.
- The equipment used mostly consists of the Microsoft Office Suite in the production of procedures, reports, presentations and workflow diagrams.
- Monitoring and reporting of the content filtering system managing our email and internet access.
- Regularly provide Business intelligence through Audit, Monitoring and reporting from the utilisation of technical monitoring and reporting software such as System Centre Configuration Management (SCCM) Services, the Microsoft Defender product suite etc. to ensure NHS 24 estate is current and secure in terms of Security patching and protected from the security threats.

6. DECISIONS AND JUDGEMENTS

The post holder is required to make judgements and interpretations across the complete and complex security spectrum including components such as legislation, policies and guidance which have conflicting priorities and expert opinions.

The post holder will be assessing possible courses of action and making decisions and recommendations on the implementation of solutions which may not be readily apparent because of the rapidly changing nature and volatility of the circumstances.

The post holder is required to demonstrate and utilise effective leadership and decision-making skills to support technology staff and effective communication across all areas of the organisation.

The post holder as Lead Technical expert within NHS 24 is required to make judgements about the delivery of complex and difficult information where the recipient is potentially resistant to change or redesign covering:

Risk and Change Management:

- Responsible for assessing highly complex technical information and situations requiring analysis, interpretation and comparison of a range of options prior to approving change or mitigating a risk successfully.
- Providing expert Security advice on operational changes.
- Leading regular Security and risk review meetings and advise on any mitigating actions.
- Assessing Design Change to all NHS 24 systems from a Security operations perspective.
- Managing Technology and Information Security risks and progressing issues with NHS 24 and directly with suppliers and customer organisations.

Project Management:

- Provide expert security input to NHS 24 projects:
    - To identify, manage and establish appropriate mitigation in respect of risk.
    - To act as advisor and ensure project objectives identified within the Data Protection Impact Assessment (DPIA) and the Security measures and controls within the Project System Security Risk Assessment (SSRA) are achieved.

Contract/Procurement Management:

- Provide expert security input to NHS 24 Procurement:
    - To establish NHS 24 security requirements.
    - Carry out supplier evaluation and selection.
    - Purchase Security certification.

Analysis, Evaluation, Reporting and Problem Solving:

- Produce reports from complex technical data suitable for a non-technical audience.

- Use experience and analytical techniques in problem solving in situations with complex facts, situations requiring analysis, interpretation and evaluation against a range of options.
- Responsible for evaluation of new security techniques, tools and technologies.
- Take decisions to ensure the continuing confidentiality, integrity and availability of NHS 24 information technology assets.
- Produce Board and Executive Team papers outlining options and recommendations for approval.
- Consider inputs and recommendations for inclusion in the NHS 24 information security plan and operational processes.
- Lead on any required actions following actual or threatened security breaches.

7. COMMUNICATIONS AND RELATIONSHIPS

Excellent communication skills are required, as a major purpose of the post holder will be required to negotiate and influence senior managers up to Executive Level in NHS 24 who have differing professional backgrounds who may have conflicting views and/or barriers to understanding.

The post holder is expected to communicate highly complex technical information regarding information security to NHS 24 stakeholders who often will not be subject matter experts. Therefore, the post required is required to have excellent presentation skills and to be able to express a view convincingly and coherently.

The post holder will be required to utilise these communication and facilitation skills across the following stakeholder range:

- Internally
  - Executive Team and Senior Managers.
  - Staff at all levels and their representatives.
  - Committees, Steering and Working groups.
  - Internal Auditors.
- Externally
  - All suppliers.
  - NHS Scotland territorial and special health boards.
  - UK healthcare organisations.
  - Key service partners within NHS Scotland.
  - Other stakeholders in the NHS 24 service.
  - Scottish and UK Governments and other security bodies such as Police Scotland, HMG Security Services, CPNI, CESG.
  - Information Security forums at a national level.

8. PHYSICAL, MENTAL and EMOTIONAL DEMANDS OF THE JOB

Physical Effort

- Ability to respond to security issues from users, suppliers and other external agencies.

Emotional Effort

- When investigating security incidents, the post holder may be exposed to highly emotive evidence for example the content of explicit websites.
- Exposure to emotional and upsetting circumstances when required to listen to sensitive calls, and when conducting investigations e.g. security breaches.
- Ability to keep one's own emotions under control when dealing with conflicting situations in a pressurised environment.
- As security measures are generally seen as a hindrance to staff, there are numerous occasions where the environment can be resisted and even hostile.

Mental Effort

- Requirement for periods of intense concentration and decision making e.g. responses to security incidents such as virus attack resulting in denial of service to NHS 24.
- Ability to move rapidly from one task to another where there is contention for service.
- Unpredictable work patterns due to constant interruptions. The post holder is required to react on a daily basis to ongoing security issues that may arise across the organisation.

Working Conditions

- The role will require travel between offices, partner and supplier sites.
- Required to use VDU and telephony equipment for prolonged periods of time without periods of rest when dealing with the command and control and responses to security incidents such as virus attack.

9. MOST CHALLENGING/DIFFICULT PARTS OF THE JOB

- Managing and driving change across the organisation, instilling a culture of security awareness.
- Managing conflicting priorities ranging from developing new and improving existing processes and procedures.
- Responsibility for the confidentiality, integrity and availability of the information for the service.
- Establishing, maintaining and monitoring for compliance the technology security scope and boundaries of all third parties and suppliers to ensure they are appropriate and fully understood and implemented by all.
- The requirement to participate in interdependent projects-based activities to deadlines.

10. KNOWLEDGE, TRAINING AND EXPERIENCE REQUIRED TO DO THE JOB

Qualification

- Tertiary qualification in Information Security.

Experience

- Significant experience in an Information Security role.
- Knowledge and experience of an Information Security Management System complying with the requirements of the international standard, ISO/IEC 27002
- Knowledge and understanding of the application of information technology covering hardware, software, applications and infrastructure.
- Demonstrated knowledge and experience of Programme and Project Management as defined under PRINCE 2.
- Knowledge of Information Security & Governance related laws and regulations such as the Data Protection Act and Computer Misuse Act.

Skills

- Understanding of an IT Strategy and implications for infrastructure.
- Excellent Communicator with a friendly and professional approach.
- Excellent analytical skills with an understanding of technical architectural issues.
- Excellent Facilitation and presentation skills.
- Experience of ITIL practices.

11. JOB DESCRIPTION AGREEMENT	
A separate job description will need to be signed off by each jobholder to whom the job description applies.	
Job Holder's Signature:	Date:
Head of Department Signature:	Date: