Job Title: Information & Cyber Security Manager

Reporting To: Head of Information Governance & Security & DPO

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

Job Reference number (coded):

1. JOB PURPOSE

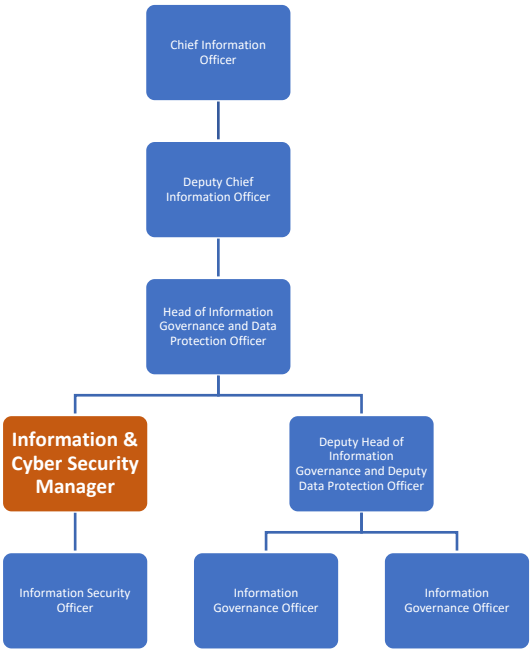
The post holder will manage all operational Information & Cyber Security technical and advisory services for NHS 24 and collaborate with partner organisations on a range of highly complex and sensitive security issues.

The post holder will provide expert specialist advice on Information & Cyber Security to ICT Professionals, Clinicians and all staff in NHS 24. They will manage a small team to build capabilities to detect, investigate and remediate information and cyber threats. In addition, the post holder will work collaboratively with the NHS Scotland Cyber Centre of Excellence Security Operations Centre and appropriate agencies such as the National Cyber Security Centre (NCSC – part of GCHQ), Police Scotland, the Scottish Cyber Co-Ordination Centre (Scottish Government) and others as deemed appropriate and required.

The post holder will be responsible for managing all legislative Information and Cyber Security policies and protocols; locally, regionally and nationally to ensure that NHS 24's Information Security Policies and Procedures are fully compliant with the Network & Information Systems Regulations 2018, the Data Protection Act 2018 and the UK General Data Protection Regulations (and other relevant legislation as it is enacted), national guidance and reflect the latest good practice in the Information and Cyber Security field.

The post holder will contribute to the design, development and implementation of the NHS 24 Information and Cyber Security Strategy, objectives and work plan to ensure that key functions are managed and progressed as appropriate which includes the confidentiality and safety of patient and staff information, maintaining a focus on Security by Design.

2. ORGANISATIONAL POSITION



3. SCOPE & 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 post holder will:

- Be a senior member and specialism lead within the Information Governance and Security Team acting as the deputy for the Head of Information Governance & Security & DPO for all information and cyber security matters.
- Lead and manage the Information and Cyber Security team, delegating work, conducting Personal Development Planning Reviews, managing absence, capability, competence, and taking forward investigations as necessary to the situation.

The post holder is responsible for the day-to-day delivery of the Information and Cyber Security roadmap within NHS 24. This covers the security posture of many critical systems, data interfaces and highly complex technologies; plus, consultancy involvement in many significant developments and projects each year, working in conjunction with other teams in the ICT Directorate and across NHS 24 to deliver a security aware and security by design and by default culture.

Liaise with Police Scotland, the Centre for the Protection of National Infrastructure and other government agencies as required, implementing necessary actions to ensure the physical security of all NHS 24 locations and the safety of all NHS 24 staff.

The post holder has line management responsibilities and will be an authorised signatory for signing-off expenses for the Information Security Officer post(s) within the team. Staff may increase as the service progresses.

The post holder will deputise for the Head of Information Governance & Security & DPO as the organisation's security manager in relation to all aspects of physical security for all NHS 24 premises. In addition, deputise when required for all information and cyber security matters and will attend local and/or national meetings representing NHS 24.

This post is an NHS 24 wide post with an operational responsibility across the whole organisation.

4. MAIN DUTIES/RESPONSIBILITIES

Information and Cyber Security Management and development of services (primary role)

- To work with NHS 24 Senior ICT colleagues, NHS 24 Managed Service Providers, NHS 24 Senior Managers, Heads of Clinical Services, General Managers and clinical and administrative colleagues to maintain and develop Information and Cyber Security controls & preventative solutions.
- The post holder will take a lead role in the development of information and cyber security plans, systems and policies for NHS 24 and will disseminate these and the analysis of this information into advice and guidance to all NHS 24 managers and staff, partner agencies and, where appropriate, the NHS 24 service users. Thus, ensuring that NHS 24 staff are fully aware of their responsibilities for compliance with legislation and NHS 24 policies when providing NHS 24 services and processing NHS 24 information.
- To be the lead investigator responsible for investigating all information and cyber security incidents, ensuring appropriate reports are produced, action plans are developed, agreed, and then implemented. Where Microsoft eDiscovery is used the post holder will be an eDiscovery Administrator.
- Maintain and develop working relationships with key service providers to foster feedback from technical implementations and develop interests and stakeholders for future developments.
- Support the procurement and/or development of new Security Systems, in line with national, regional and local strategy.
- To maintain appropriate contact with Scottish Government, and other NHS Scotland Boards' staff concerned with Information and Cyber Security development and/or with NHS 24 Information Governance & Security strategy and to participate in local and national groups helping to develop and implement new systems and national policies safely & securely.
- To maintain and develop specialist skills and expertise in the area of responsibility for the benefit of the organisation.
- To help identify gaps in the security of information systems and to make recommendations as to how these gaps might be filled in terms of NHS 24's technology strategy.

- To work with client/user departments to identify needs gaps and to recommend how best such needs can be met.
- Ensure that the security of information, systems and processes which support the strategic objectives of NHS 24 are successfully scoped, developed and implemented.
- In support of the Head of Information Governance & Security & DPO, develop and communicate the overall security of the Information Estate within NHS 24, particularly taking account of availability and resilience, including roadmap development, security classification and standards for Applications/Systems and data.
- Provide advice and security recommendations on Applications/Systems Architecture matters to the NHS 24 ICT Architecture Team, Executive Directors and senior operational management.
- Provide input and develop controls as appropriately required to progress System Security Risk Assessments.
- Owner of the NHS 24 security certificate process including, but not limited to, the management and secure storage of, and the primary purchaser for, all security certificates.

Programme Delivery

- To provide expert information and cyber security consultancy required for the safe and secure delivery of procured Applications/Systems over multiple independent project work streams.
- Contribute to the secure design and safe implementation of complex interdependent projects in a governed, risk minimal manner ensuring projects are aligned with other business as usual activities or project dependencies.
- Monitoring and reporting of any information and cyber security threats and vulnerabilities, risk and expectations to the appropriate steering groups.
- Where required, on behalf of the Head of Information Governance & Security & DPO, lead the delivery of the information and cyber security elements of projects on time, in scope and on assigned project budget with the ability to help address any information and cyber security implementation ‘drift’ and ‘manage out’ any associated risk.
- Definition and implementation of Information and Cyber Security associated support requirements necessary to sustain the service during and post project go-live in conjunction with the project and ICT Operations Teams.
- Management of Information Governance & Security staff and external vendors and consultants aligned with the programmes and projects as required.
- Provide Information & Cyber Security controls input to Data Protection Impact Assessments.

Management of Staff (including HR & Payroll Responsibilities)

- Schedule and direct the activities of Information and Cyber Security staff, taking account of individual’s abilities and the requirements of the organisation.
- Provide line management to the Information and Cyber Security Team as a team within the Information Governance and Security Team.
- Guide staff on the interpretation and application of NHS 24 and ICT strategies and project governance arrangements.
- Ensure all work is carried out and documented in accordance with required and agreed standards, methods and procedures (leading in specific areas of standard or processes as directed by the Head of Information Governance & Security & DPO).
- Motivate staff through the provision of appropriate development opportunities, training and objective setting and maintain a Personal Development Plan for each Information and Cyber Security team member.
- Maintain records of attendance, sickness or other absence and leave for team members, as required.
- Communicate with other ICT managers, Workforce and Occupational Health advisors to notify them of any staffing issues and to work with Recruitment on any vacancies.

- Responsible for the recruitment and selection of new staff within the Information and Cyber Security Team as required.
- Encourage and support staff to develop their individual skills and to reach their full potential.
- Take a lead management role for the ongoing teaching / training of all staff across the Board area relating to Information and Cyber Security and associated Information & Cyber Security Risk Register entries and Records Management to ensure that they are aware of their personal responsibility in relation to the use, storage and sharing of information.

In All Work

- Develop and apply analytical approaches and best practices in the formulation of solutions and implementation of services.
- Work to broad priorities agreed with the Head of Information Governance & Security & DPO and, where appropriate, the ICT Senior Management Team.
- Manage the NHS 24 Information and Cyber Security risk register, maintaining awareness of the latest information and cyber security threats and key risk indicators and inform the organisation of current information and cyber security risks, proposing appropriate risk mitigating actions.
- Maintain an in-depth, highly technical and up-to-date knowledge of the wide range of Applications/Systems, environments, systems, software and hardware used within NHS 24 and their security posture and any vulnerabilities, recommending and, when appropriate, implementing improvements to the security posture and mitigations for the vulnerabilities.
- Keep abreast of the changing technical environment, in terms of both hardware and software ensuring NHS 24 make the best use of available security technologies.
- Work within and influence development of organisation and directorate policies, procedures and guidelines, developing the broad range of information governance and security policies and procedures.
- Comply with the requirements of the relevant information and cyber security legislation such as the Network and Information Systems Regulations 2018, the Computer Misuse Act 1990, the Data Protection Act 2018, the Freedom of Information (Scotland) Act 2002 and other appropriate legislation and statues as they are enacted.
- Be familiar with NHS 24's directorates, management structures and operational environments.
- Ensure that the appropriate NHS 24 staff are kept fully informed of progress throughout all work and escalate problems in a timely manner.
- Ensure the overarching principles of Information Governance and Security are embedded in the organisation, setting targets against indicators to ensure these are applied across NHS 24 and therefore deal with difficult issues on a daily basis.

Research, Development and Testing

- As the NHS 24 representative for Information and Cyber Security on NHS Scotland and other National Fora, be involved in decision making regarding research and development relating to redesign, audits and service improvement regarding Information Governance and Security and the implementation of post research outcomes.
- Ensure, on behalf of the Board, that all NHS 24 data, including patient and staff, clinical and non-clinical, is monitored and managed and that the confidentiality of this information is maintained to the required standards.
- Monitor and audit the information systems used including the cyber security of these systems across the organisation.
- Ensure regular testing of security equipment, systems and potential solutions which will have an impact on Board processes and delivery of services in line with statutory requirements.

The above is not exhaustive and the post-holder may be required to fulfil other reasonable requests for support whilst working with integrity and following good practice guidelines. Join the 24/7 ICT On-call rota if required.

5. SYSTEMS & EQUIPMENT

The post holder will be expected to use the following systems and equipment:

- Building Access Control system (system manager). The post holder will be responsible for ensuring that the system is up to date and appropriately programmed.
- Redaction Software to ensure the confidentiality and security of information in any documents is maintained.
- CCTV for all the buildings in the organisations estate (system manager).
- Microsoft Defender for Endpoint, Microsoft Defender for Cloud and other Microsoft security products as they are provided through the national contract.
- Security vulnerability assessment and scanning tools (e.g., Tenable Nessus).
- Microsoft office/Office 365 including PowerPoint, Excel and Word.
- Investigation tools – such as Microsoft eDiscovery as an eDiscovery Administrator.
- Collaboration tools such as SharePoint Online and Microsoft Teams.
- Quality Improvement tools.
- MetaCompliance.
- Programme/Project Management tools.
- Analytical systems for the interpretation of data.
- Data and information business intelligence tools.
- HR Management Information System for recording and managing team members' absence history and approving staff member expenses. (e.g., SSTS, eESS, eExpenses).
- The post holder will require to be proficient in the operation of a PC/Tablet/Smartphone device to access and use corporate systems.

6. DECISIONS & JUDGEMENTS

The post holder is required to exercise a high level of autonomy in progressing objectives agreed with the Head of Information Governance & Security & Data Protection Officer (DPO) (to whom the post holder reports).

The post holder will work in close conjunction with the ICT Operations senior team and other members of the ICT management team. Regular meetings on Information and Cyber Security considerations and strategy implementation will take place with the Head of Information Governance & Security & DPO and the Deputy Head of Information Governance & Deputy DPO and others.

This is a senior Information Governance & Security post, and the post holder is expected to stand-in for the Head of Information Governance & Security & DPO in all matters relating to security at meetings or in periods of absence as and when required.

The post holder will work on their own initiative to ensure safe and secure Systems and Services and support safe delivery of NHS 24 programmes and projects. The post holder is expected to anticipate problems and to resolve them, plan and supervise the workload and deliverables of appropriate staff within the Information and Cyber Security section of the Information Governance & Security Team. The post holder will have the discretion to identify security solutions to both technology, service support and process issues. Then direct, in conjunction with the ICT Operations department the managed service providers managers and engineers to resolve issues, threats and vulnerabilities.

The post holder requires skills in developing relationships and it is particularly important to work closely with other Senior ICT Managers and other NHS 24 staff, clinicians, business managers and

programme and project managers. The post holder will also require the skills to manage / control and maximise input from the NHS Scotland Cyber Centre of Excellence Security Operations Centre, work constructively with Regional and National peers, suppliers and other third parties.

The post holder is expected to use their initiative, be decisive and prompt with their responses to loss of NHS 24 systems and services during a cyber incident which can create elevated levels of stress.

Any other areas of responsibility and agreed priorities and objectives will be agreed with the Head of Information Governance & Security & DPO.

Work will be reviewed as necessary to the scope of the job. Formal Personal Development Planning and Review will take place annually when objectives will be discussed and agreed.

7. COMMUNICATIONS & RELATIONSHIPS

The post holder is required to have excellent communication and interpersonal skills, both written and verbal. Strategic thinking and the ability to anticipate and resolve problems before they arise and respond to sudden unexpected demands.

Provide detailed Information and Cyber Security advice, guidance and support to Managers and Accountable Officers in their roles, regarding all aspects of the confidentiality, integrity and availability of NHS 24 information, systems and services in line with the requirements and controls laid down in legislation and as required by the statutory regulators.

Deal directly with service users and staff regarding complaints and investigations, including Serious Adverse Events and Information and Cyber Security incidents that need to be dealt with in a discrete and delicate manner.

When deputising for the Head of Information Governance & Security & DPO influence and advise the EMT and sub-committees of the Board on all aspects of Information and Cyber Security and with Partner agencies and Managed Service Providers. This will require communication with very complex technical content. This needs to be communicated in a way that is understandable by those without technical expertise.

The post holder must be diplomatic and show the utmost discretion in communications regarding information and cyber security elements such as sharing information regarding breaches, break ins, cyber-attacks etc.

Deal with particularly difficult situations including the production of Information and Cyber Security Incident reports which must be looked at from the organisation and staff's perspective which can include ethical and moral dilemmas that may cause concern.

Take part in conversations and meetings where the subject matter may be delicate and upsetting, having to direct the conversation in a way that causes the least angst in trying to reach consensus.

Interpret changes in legislation for the NHS 24 senior management staff to ensure that the organisation complies with its legal responsibilities in relation to Information and Cyber Security governance and legislative compliance and advising the public regarding these where appropriate.

Train small and large groups of staff regarding Information and Cyber Security in relation to the confidentiality, integrity and availability of NHS 24 information and services, Physical Security of the NHS 24 estate and give presentations on a regular basis within and outwith the health service, including directly to the public, when required.

Develop and maintain effective, positive relationships with key partners and partner organisations, providing a positive role model for partnership working within NHS 24.

Investigate Information and Cyber Security incidents that involve potential breaches in confidentiality, sharing information inappropriately, and involvement in social media conversations relating to the Board or staff who work for the Board and other Information and Cyber Security incidents.

The post holder will provide and receive highly complex, highly sensitive and, at times, highly contentious information which may involve hostile, antagonistic and emotive episodes.

Internal Stakeholders

- Senior Information Risk Owner.
- Caldicott Guardian.
- NHS 24 Executive Team and, when required, sub-committees of the Board to report on and explain information governance and security reports.
- When deputising for the Head of Information Governance & Security & DPO Chairpersons and non-Executive members of the sub-committees of the Board.
- NHS 24 Senior Management Team in relation to information and cyber security requirements
- Programme Management team to discuss information and cyber security implications and requirements on their programmes of work.
- Heads Of Clinical Services.
- Heads of Department.
- Staff within NHS 24.

External Stakeholders

- Information Commissioners Office.
- National Records of Scotland.
- Scottish Government Health Competent Authority.
- Relevant Scottish Government departments as required based on the legislative portfolio of the role.
- NHS Scotland Information Security Forum.
- Information and Cyber Security leads in other NHS Boards.
- Scottish Business Resilience Centre.
- Police Scotland.
- Scottish Government Cyber Resilience Centre.
- NHS Scotland Central Legal Office.
- The National Cyber Security Centre
- The National Protective Security Authority
- Members of the public.

8. PHYSICAL, MENTAL, EMOTIONAL AND ENVIRONMENTAL DEMANDS OF THE JOB

The post holder is expected to deliver, in line with system availability needs and expectations, project plans, unforeseen events can have an adverse effect on how time/resource is managed. As with any non-scheduled support environment, user expectation is of quick fix, which means post holder will

react to situations. The job requires the juggling of large numbers of complex tasks large and small to ensure that priorities are met for the clinical and business services in NHS 24.

Working Conditions

- Requirement to occasionally work in clinical areas where services are deployed which, on occasion, may be in close proximity to sensitive patient / clinical situations.
- Regular exposure to confidential / sensitive data and involvement in sensitive Information and Cyber Security incidents and forensic investigations.
- Incidental contact with service users.
- Occasional requirement to manage or directly participate in programmes of work being undertaken out-of-hours (evening, weekend and holiday) work to minimise disruption to clinical services during IT system and infrastructure implementations and upgrades.
- Inter-site and intra-site mobility including travelling anywhere as required (especially within NHS 24 sites).

Mental Effort

- Frequent requirement for concentration required to perform detailed, technical analysis of system issues and incidents relating to Information and Cyber Security and provide a balanced assessment of recommendations and / or solutions. Given the nature of the role the post holder will be subject to frequent interruptions.
- Lengthy periods of concentration are required whilst acknowledging interruptions and change of task are an unavoidable element of the role and working environment (e.g., many hours focused on collaborating with key suppliers in response to information and cyber security incidents).
- Review cyber security related information as necessary which requires lengthy periods of focussed concentration and may involve disturbing elements that need to be gathered as evidence.
- Attend meetings to present findings in relation to suspected perpetrators and provide specific and complex Information and Cyber Security advice and guidance.
- Attend formal meetings with Police Scotland and the National Protective Security Authority where all matters of physical security are reviewed and assessed.
- Frequently use in-depth mental attention when leading meetings, influencing NHS staff and managers at all levels of seniority, public speaking, analysing technical and other system problems and proposing solutions, often working under pressure and balancing multiple demands in a complex / changing environment.

Emotional Effort

- Deal with situations where there is conflict and / or heated discussions, e.g., at emotionally charged meetings where a member of staff may be in breach of Regulations and give advice regarding subsequent actions that need to be put into place.
- Direct line management requires emotional effort when applying Human Resource policies and procedures i.e., addressing and managing sickness, disciplinary and performance management issues. This may involve delivering or investigating uncomfortable and disputed issues.
- Deal with cases where there may be a need to challenge standards and practices that may be in breach of legislation, and to suggest practical solutions that will minimise information and cyber security risk to NHS 24.
- Deal with conflicting and challenging problems, as and when required, that require sustained emotional resilience such as when there is a need to respond immediately to questions or

advice that is being sought, particularly when there has been an Information and Cyber Security incident or a Severe Adverse Event.
- Deal occasionally with data subjects who may present severely challenging behaviour under emotional circumstances.

9. MOST CHALLENGING/DIFFICULT PARTS OF THE JOB

Managing a complex mix of protecting the production environment, supporting interdependent programmes and projects, resolving the conflicts and contributing to their successful delivery within an environment of competing priorities and limited resources. Maintaining a pragmatic balance between a hardened approach to the Information and Cyber Security posture and information being readily available where and when it needs to be.

Working in an unpredictable and often stressful environment, where the post holder must negotiate and manage the impact of:
- The availability, resilience and security of the core infrastructure, data and Endpoints across NHS 24.
- Project work often being reprioritised because of external factors including support issues, audits, business-political issues and changing strategies.
- Considerable periods of peaks in demand due to budget cycles, organisational targets and new unforeseen and unplanned demands.

Working within an increasingly technical, complex, rapidly evolving and growing environment; gaining, retaining and expanding appropriate technical knowledge and skills to ensure the confidentiality, integrity and availability of this environment and clearly communicating these highly complex issues to colleagues, project teams and customers.

Ability to meet the demands of controlling and communicating complex programmes of work and continue to deliver initiative, proactiveness and subjectivity at times of high demand, pressure and stress.

Ability to deal with complexity of IT infrastructure and systems.

Understanding and succinctly presenting the complexity of the current Applications/Systems, integrations, data flows, data architecture and how it can be best secured.

Persuasively presenting problems and solutions appropriate to the scale and complexity of NHS 24 to colleagues, suppliers, local and national project teams and other NHS organisations; sometimes where they are not accustomed to or do not understand the impact of such issues in a large-scale organisation with a significant and complex infrastructure.

Working within limited staff resources (when compared to commercial organisations), so compounding all the challenges and stresses summarised above and having to accordingly manage customers and suppliers' expectations.

Recommending service improvements necessary to ensure the confidentiality, integrity and availability of an ever increasing and evolving range of NHS 24 services, whilst managing limited available resources.

Establishing, maintaining and monitoring - for compliance - the security scope and boundaries of third-party suppliers to ensure they are appropriate and fully understood and implemented by all.

Establishing, maintaining and monitoring - for compliance - the physical access to buildings and adherence to policy regarding the physical security of NHS 24 sites.

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

Qualifications
Educated to degree level in an appropriate Information and Cyber Security qualification.

Additional Information and Cyber Security accreditation is essential to be able to perform to the required level and standard.

Experience
Substantial amount of experience working within the field of Information Governance and Security.

There is a requirement to have experience in creating, developing and implementing policies, procedures, guidance and protocols.

There should be a proven track record in the provision of creative and innovative solutions in meeting organisational requirements.

Skills
Demonstrate integrity and effective leadership and management skills together with a proven track record of achievement in strategy and policy development and implementation.

Evidence of developing and maintaining effective, positive relationships with key individuals and organisations, providing a positive role model for partnership working within NHS 24.

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:**