# NHS FORTH VALLEY



# JOB DESCRIPTION

 **1. JOB DETAILS**

**Job Title: Cyber and Information Security Manager**

**Responsible to: Head of Information Governance**

**Department(s): Information Governance**

**Job Reference: BN-AC-504**

**2. JOB PURPOSE**

To provide leadership, technical direction and guidance on matters of Cyber / Information Security Technical Controls, Procedures and Standards. To ensure that NHS Forth Valley achieves and maintains the assurance standards provided by Network and Information Security Regulation and Data Protection legislation. To be lead assessor for all Cyber Security Technical controls for NHS Forth Valley and to collaborate with partner organisations on a range of complex and sensitive security issues providing expert specialist advice on Information and Cyber Security to other IT Professionals, Clinicians and all staff in NHS Forth Valley. To assist and advise the Head of Information Governance and Director of Digital on ensuring that NHS Forth Valley Information Security Policies, Procedures, Active Cyber Defence Tools and Configurations are mitigating the Cyber Security Operational Risks, are following National Guidance, reflect the latest Good Practice for the Digital Estate, and aligns with the IT / Cyber Security industry.

**3. KEY DUTIES**

**Responsibilities**

* **Policy and Service**

**There is a responsibility to:**

1. Lead on the implementation and maintenance of the Scottish Public Sector Cyber Resilience Framework as local lead assessor for compliance with the Network and Information System Regulation (NIS) and custodian for evidence submitted by departments for annual NIS audits conducted by the Scottish Government’s approved auditors.
2. Lead, develop and monitor strategies and procedures in support of the Head of Information Governance and the Caldicott Guardian in safeguarding the confidentiality of personal data throughout NHS Forth Valley.
3. Lead investigations and local response to Information and Cyber Security incidents which take place on NHS Forth Valley computers, networks, information systems or contain NHS Forth Valley data; liaising with Police Scotland, Counter Fraud Services, Central Legal Office, partner organisations, and national intelligence agencies where appropriate.
4. Deputise for the Head of Information Governance as and when required.
5. Create, develop and ensure effective implementation and understanding of Information Governance and Digital/eHealth policies. Additionally, actively suggest changes to policies of any other service area to ensure they reflect legislative requirements in relation to Information Governance and security.
6. To ensure clear links to other NHS Scotland Boards and partners and ensure NHS Forth Valley is kept abreast of strategic developments in Information and Cyber Security at local governance groups.
7. Lead, promote, facilitate and influence changes to the working process and organisational culture within NHS Forth Valley to meet Information Governance objectives.
8. To monitor and regulate the use of the internet, e-mail and cloud storage to ensure compliance and adherence with local polices and legislation and to make staff aware of policies regarding misuse of internet etc.
9. Provide highly specialised advice, guidance, and support to local service managers and accountable officers in their management roles, in all aspects of cyber and information security and associated legislation.
10. Lead operational audits into all NHS Forth Valley Cyber Security services and defence technologies, as well as others linked to partner organisations or suppliers e.g. cloud hosted information systems.
11. Provide specialist advice to review and approve, prior to introduction into routine use, any new or revised documents, procedures and systems to minimise risks associated with non-compliance with current legislation e.g. System Security Policies, Standard Operating Procedures, Cyber Risk Assessments.
12. Lead development of and maintain the NHS Forth Valley Cyber Incident Response Plan as part of requirements of the Cyber Resilience Framework.
13. Create and manage communication plans in relation to Cyber Security incidents.
14. Advise and support Service Managers in the implementation of Cyber Security, Information Security and Information Governance recommendations identified in external or internal audit reports.
15. Contribute to the cross-organisation Better Information Governance Group (BIGG), ensuring services have appropriate opportunities to participate and are kept fully informed of NHS Forth Valley policies, protocols and guidance in relation to Information and Cyber Security.
16. Provision of business case development in relation to Cyber and Information Security products and services for NHS Forth Valley.
17. Lead design, scoping and review of cyber security testing of NHS Forth Valley infrastructure, services and products e.g. penetration testing of networks by a third party.

1. Lead the development and delivery of a comprehensive cyber security exercise program e.g., NCSC Exercise in a Box. Continuously evaluate and refine response plans based on exercise outcomes, actual incidents, and emerging cyber threats.
2. Manage and monitor a range of Cyber and Information Security products, resolving incidents and alerts promptly, and ensuring the tools are providing value to the organisation by effectively mitigating risks.
* **Finance and Physical Resources**

**There is a responsibility to:**

1. Manage a portfolio of cyber and information security monitoring products and services deployed across the entire organisation, ensuring these are:
	1. Reviewed appropriately and where necessary create fully costed business cases for replacements; where necessary coordinate with the Procurement Department to hold a mini-competition or initiate a tender process.
	2. Kept up to date with latest developments, software upgrades and report any exceptions to the appropriate department managers for action; following up on these actions through governance groups.
	3. Risk assessing gaps in NHS Forth Valley defences and presenting appropriate action plans to senior management for action or fully costed business cases where appropriate.
2. Ensure Cyber Security testing recommendations are appropriately scoped to cover organisational needs in relation to Information Security legislation.
3. Provide accurate reporting of lost/stolen information assets to the NHS Forth Valley finance department annually.
* **Staff Management/Supervision, Human Resources, Leadership and/or Training**

**There is a responsibility to:**

1. NIS Audit Compliance Lead. Coordinating efforts of multiple services to ensure NHS Forth Valley shows continual improvement in compliance year on year with exceptions reported to the Senior Leadership Team with an appropriate recommendation and action plan.
2. Develop training, guidance, and advice to all staff in relation to the requirements of Information Governance and security legislation and standards. Ensure training and awareness materials for Information and Cyber Security are available organisation wide.
3. Represent NHS Forth Valley at the National Information Security Training Forum and ensure local training is in-line with national strategy.
4. Lead development and communication of local cyber security awareness initiatives, with the goal of building and maturing a security aware culture. Locally developed awareness materials and strategies are shared nationally where appropriate to promote a positive culture across NHS Scotland.
5. Supervise the Information and Cyber Security Team, ensuring team members undertake appropriate duties with suitable support and expert guidance. Ensure the team are developing skills by agreeing Personal Development Plans (PDPs).
6. Develop a healthy, safe, and dynamic working environment with a focus on staff wellbeing where individuals are supported and motivated effectively.
* **Information Resources**

**There is a responsibility to:**

1. Manage NHS Forth Valley Cyber and Information Security products (web content filter, vulnerability management etc).
2. Handle large volumes of sensitive personal information contained in clinical system logs as part of Privacy Breach Detection efforts (50 million + / month) and personal access logs of all NHS Forth Valley staff via the internet (1.2 million accesses /day).
3. Produce, analyse and report proposals, incident reports, privacy breach reports, policies and guidance in relation to Information Governance and Cyber Security for all levels of management and governance groups.
4. Analyse staff use of information systems to determine use which is likely against policy or legislation, generate details reports for all levels of line managers and participate in disciplinary panels and boards are necessary.
5. Resolve or escalate Cyber and Information Security and Governance risks and issues to appropriate stakeholders.
6. Lead forensic analysis of logs, use of systems and information assets for NHS Forth Valley e.g. NHS email, malware investigations. Cooperating with law enforcement and counter fraud agencies as required.
* **Research and Development**

**There is a responsibility to:**

1. Act as lead assessor for NHS Forth Valley during the assessment of new products and services e.g. new clinical systems. In relation to Cyber and Information Security.
2. Research threats to the security and / or integrity of NHS Forth Valley’s computer held data. This activity includes identification, evaluation, assessment and recommendations based upon the risk that any threat poses to NHS Forth Valley computers networks. The post holder will also research and develop responses to each threat as and when they become known.
3. Maintain awareness of security threats and techniques, technologies and best practice that help control or mitigate risk.
4. To assess the relative sensitivity of data used by existing and new systems and to advise on the appropriate levels of security and compliance with relevant legislation.
5. To devise and maintain a reporting mechanism for logging and identifying IT security and privacy breaches and to report these to appropriate Managers and appropriate external intelligence agencies.
6. Audit and assess IT systems for risk and report them to the Director of Digital and Head of Information Governance on the state of information and cyber security within NHSFV, making appropriate recommendations for improvement or development where necessary (ongoing basis).
7. To liaise with internal audit, the Head of Information Governance, the Head of Information Management and the Director of Digital on a formal regular basis regarding data security and audit.
8. Maintain links with external agencies (NCSC, CiSP etc) to ensure NHS Forth Valley is informed of anticipated cyber attacks from state actors or malicious groups and research appropriate actions to mitigate risks where possible.

**Skills**

* **Physical**

**There is a requirement to:**

1. Frequent requirement for periods of prolonged concentration in relation to checking information, audit, investigations, and responding to general queries from staff and members of the public.
2. Light physical effort with regular requirement to carry uneven, bulky loads.
3. Delivering training sessions and presentations to governance groups and committees involves limited periods of standing.
* **Communication**

**There is a requirement to:**

1. Communication is a core element of this post from motivation / persuasion though to negotiation. Types of communication will include email, telephone, formal and informal presentations, written, verbal workshops, meetings, face to face onsite etc.
2. Effective listening and questioning skills are essential to assist with staff/public/patient enquiries in respect of all elements of information governance and security. This may include dealing with stressed, agitated members of the public in person or via telephone.
3. Responsibility for communicating the vision of Information Governance and influencing key clinicians and managers in Forth Valley to adopt and embrace the required culture change.
4. Providing clear analysis of complex, sensitive and highly contentious information during emotive investigatory meetings with staff members, HR and management; but interpreting and conveying this information in a straightforward and unambiguous way.
5. Presenting complex information to large groups of staff at investigations, governance groups and committees both locally and nationally. Answering any questions groups may have on a wide range of topics. (Occasionally Groups typically 30+)

1. Effectively communicate task requirements with the Cyber and Information Security team. Create a supportive and collaborative environment where team members are comfortable giving and receiving feedback. Provide constructive feedback on job performance in a manner that respects individual learning styles and encourages personal development.

* **Analytical**

**There is a requirement to:**

1. Actively interpret, compare and analyse highly complex log files from various sources and in varying formats, building timelines of activities and judging where inappropriate or illegal actions may have taken place. This will regularly (most days) require long periods of intense concentration, using specialist knowledge to identify inappropriate actions; comparing to previous breaches and authoring easily understood reports for managers.
2. Manage cyber security systems and interpret differing data points to draw conclusions relating to attempted or successful cyber attacks. This may mean prolonged periods of research and analysis to correctly identify attacks taking place on the organisations infrastructure internally and externally.
3. Interpret Information Governance and Security legislation and the implications of these for NHS Forth Valley. In some cases, this may require the individual to challenge senior members of staff over standards and practices in order to minimise risks to the organisation.
* **Planning and Organising**

**There is a requirement to:**

1. Create, manage and plan the Cyber Security Awareness Strategy which will require to coordinate activities at least 12 months in advance and link with national awareness programmes.
2. Manage, monitor and escalate issues relating to the Scottish Public Sector Cyber Resilience Framework; the legislative standard which NHS Forth Valley are held to under the Network and Information Security Regulation as “Operators of Essential Services”.
3. Regularly test infrastructure and technical controls via the use of penetration testing and audits to prove compliance with industry best practice and legislation e.g. Network and Information Systems Regulation.
4. Develop a 3-5 year plan to match audit requirements for the Network and Information system Regulation and take into account any known changes to the regulation due to come into effect during that period.
5. Collaborate with the Information Governance Unit in developing the annual work plan for the unit.
6. Use effective project management techniques to manage the Cyber Security team’s daily and longer-term tasks to meet the ever-changing demand e.g. Agile project management methodologies.

**Effort and Environment**

* **Physical**

**There is a requirement to:**

1. Occasionally lifting equipment and materials such as projector, laptop, handout material (in excess of 5/6kg) for e.g. preparing and conducting presentations and staff awareness sessions.
2. Extensive periods working on computer for word processing, creating presentations, using the email and analysis of data. Prolonged typing and gazing at screen up to 7 hours per day.
3. Prolonged periods of standing, delivery training awareness to all levels of staff.
* **Mental**

**There is a requirement to:**

1. To understand and interpret the Data Protection and Cyber / Information Security legislation and the implications these have for the NHS FV. In some cases this may require the post holder to personally challenge standards and practice that may be in breach of legislation, and to suggest practical solutions (e.g. Network and Information System Regulation has implications for Digital/eHealth) that will minimise risk to NHS FV.
2. Intense concentration/in-depth mental attention frequently required e.g. leading meetings, influencing NHS staff and managers at all levels of seniority, public speaking at national forums, analysing technical and other system problems and proposing solutions, often working under pressure and balancing multiple demands in complex/changing environment. Meetings can range from 1 hour to over 3 hours depending on agenda and the post holder can attend 3 or 4 meetings per week on average.
3. Occasionally deal with conflict situations, e.g., at emotionally charged meetings. Dealing regularly with challenging problems requires sustained emotional energy/resilience.
4. Detailed and critical technical analysis of system and database problems and the detailed balanced assessment of recommended solutions.
5. Reviewing system logs and incidents (minimum of 3 to 4 times per week) requires long periods of intense, prolonged concentration (over 6 hours) and may involve disturbing images or content to be viewed and gathered as evidence. Due to working environment, frequent interruptions are commonplace. Attendance at the subsequent 1st stage interview with suspected perpetrator is also emotionally demanding.
6. Working under pressure and balancing multiple demands in complex/changing environments.
* **Emotional**

**There is a requirement to:**

1. Occasional exposure to distressing or disturbing images, content or video when reviewing system or internet logs and activity.
2. Occasional involvement in stressful situations such as disciplinary investigations and meetings where post holder may be required to present findings involving highly distressing content to those present and answer queries into the method used to gather and analyse the evidence.
3. Rare requirement to appear as an expert witness for GMC hearings and/or court proceedings on behalf of the board in relation to Information and Cyber security breaches.
* **Working Conditions**

**There are:**

# Mainly office / home based with the requirement for the post holder to travel regularly within NHS Forth Valley, with occasional travel to national meetings within the United Kingdom.

# Frequent prolonged use of computer and printer equipment on a daily basis. (this takes into account statutory breaks and recommendations for Display Screen Equipment users)

# Laptop and projector for training purposes (over 5/6kgs in weight)

# Photocopier

# Office filing systems

# Electronic systems including: Microsoft Word, Visio, Outlook, Excel, Safeguard, Fairwarning, and several cyber security applications not listed for security reasons e.g. XDR solutions, web content filter, vulnerability management, network traffic analysis tools.

**4. FREEDOM TO ACT WITHIN THE JOB**

1. This post operates with a significant level of autonomy.
2. The post holder is responsible to the Head of Information Governance for professional management, work review, and formal appraisal of performance.
3. The post holder is expected to prioritise their workload while striking a balance between often competing and/or conflicting priorities and exercise their initiative and judgement in making decisions in line with project objectives, Information Governance strategy and Digital and eHealth strategy.
4. Performance against objectives will be managed consistent with NHS Forth Valley arrangements for Performance Management. This will involve structured meetings with the Head of Information Governance to review the performance against agreed objectives and the post holders personal development planning.
5. The postholder will also be responsible for overviewing and delegating work and setting objectives, as appropriate, to staff both within the Information Governance team and elsewhere within NHS Forth Valley (where appropriate), providing advice and guidance as required.
6. The post holder is responsible for ensuring accurate interpretation of legislation in relation to cyber and information security and creating technical policies, guidance and giving advice to NHS Forth Valley staff of all levels as an expert in this capacity.
7. The post holder is responsible for ensuring forensic evidence is protected for use by or to be shared with law enforcement e.g. GCHQ and is expected to take action to ensure the evidence remains admissible at court. This may mean initiating action which is not in the best interest of services, but of NHS FV collectively.

**5. KNOWLEDGE, TRAINING AND EXPERIENCE REQUIRED TO DO THE JOB**

1. Graduate or equivalent level qualification in Cyber Security or extensive experience within an Information Security role and an industry standard qualification preferred e.g. CISM, CISSP.
2. Experience of creating or maintaining an Information Security Management System (ISMS).
3. Strong change management skills, including team leading experience.
4. Knowledge of incident response and analysis, along with experience and awareness of the business issues in the NHS.
5. Demonstrable experience of managing Information/cyber security applications and risks in a related area either in NHS, service industries or commerce.
6. Experience of staff management/leadership.
7. Evidence of Continuing Personal Development.
8. Experience of procurement of information systems and associated tender processes.
9. Ability to influence others and develop and maintain effective working relationships with senior managers, clinicians, administration staff, Informatics staff and third party service providers.
10. Excellent interpersonal, negotiation, facilitation and communication skills.
11. Effective team manager, with motivational skills and organisational ability.
12. Ability to effectively manage and prioritise own and team workload.
13. Ability to understand, analyse and re-engineer complex processes.
14. Excellent organisational & time management skills.
15. Ability to negotiate & influence change at all levels.
16. Ability to understand, analyse & disseminate complex concepts to a wide range of staff with varying levels of technical understanding.

**6. DEPARTMENT ORGANISATION CHART**

|  |
| --- |
|  |

Line Manager Responsibilities

Professional Responsibilities

Medical Director/ Caldicott Guardian

Medical Director/Caldicott Guardian

Director of Digital

Head of Information Governance / Data Protection Officer

Cyber & Information Security Manager

**This post**

Information Governance Administrator

Information Rights Officer

Information Asset Administrator

Records Management Co-ordinator

Cyber & Information Security Analyst (x2)

Cyber & Information Security Technician

Data Protection Support Officer (x3)

IG Project Manager

Corporate Records Manager

Freedom of Information Manager

Data Protection Manager