Lothian NHS Board

NHS
Lothian

Lothian NHS Board
Mainpoint
102 Westport
Edinburgh
EH3 9DN
Main Switchboard: 0131 242 100

www.nhslothian.scot

Date	05/12/2025
Your Ref	
Our Ref	10811

Enquiries to	Richard Mutch
Extension	35687
Direct Line	0131 465 5687

loth.freedomofinformation@nhs.scot
richard.mutch@nhs.scot

Dear

FREEDOM OF INFORMATION – INFORMATION GOVERNANCE

I write in response to your request for information in relation to Information Governance.

Question:

- Under FOISA, I am requesting information relating to the makeup of your information governance/information security/information assurance team(s).

  Please provide details of roles (role title and reporting structure), including information relating to Agenda For Change bandings as well as copies of any job descriptions. Please be advised I am not looking for personal details relating to post holders, such as the names of any individual staff members.

  Could you please confirm, for each post, the source of funding e.g. funded by internal budgets (and which budget e.g. medical), funded by Scottish Government etc.

Answer:

I have enclosed NHS Lothian's Information Governanace department structure chart and job descriptions. I am not able to give details of members of staff below senior managment level. Since we do not have their consent to release their personal data, the information is exempt under section 38 of the Freedom of Information (Scotland) Act 2002

I hope the information provided helps with your request.

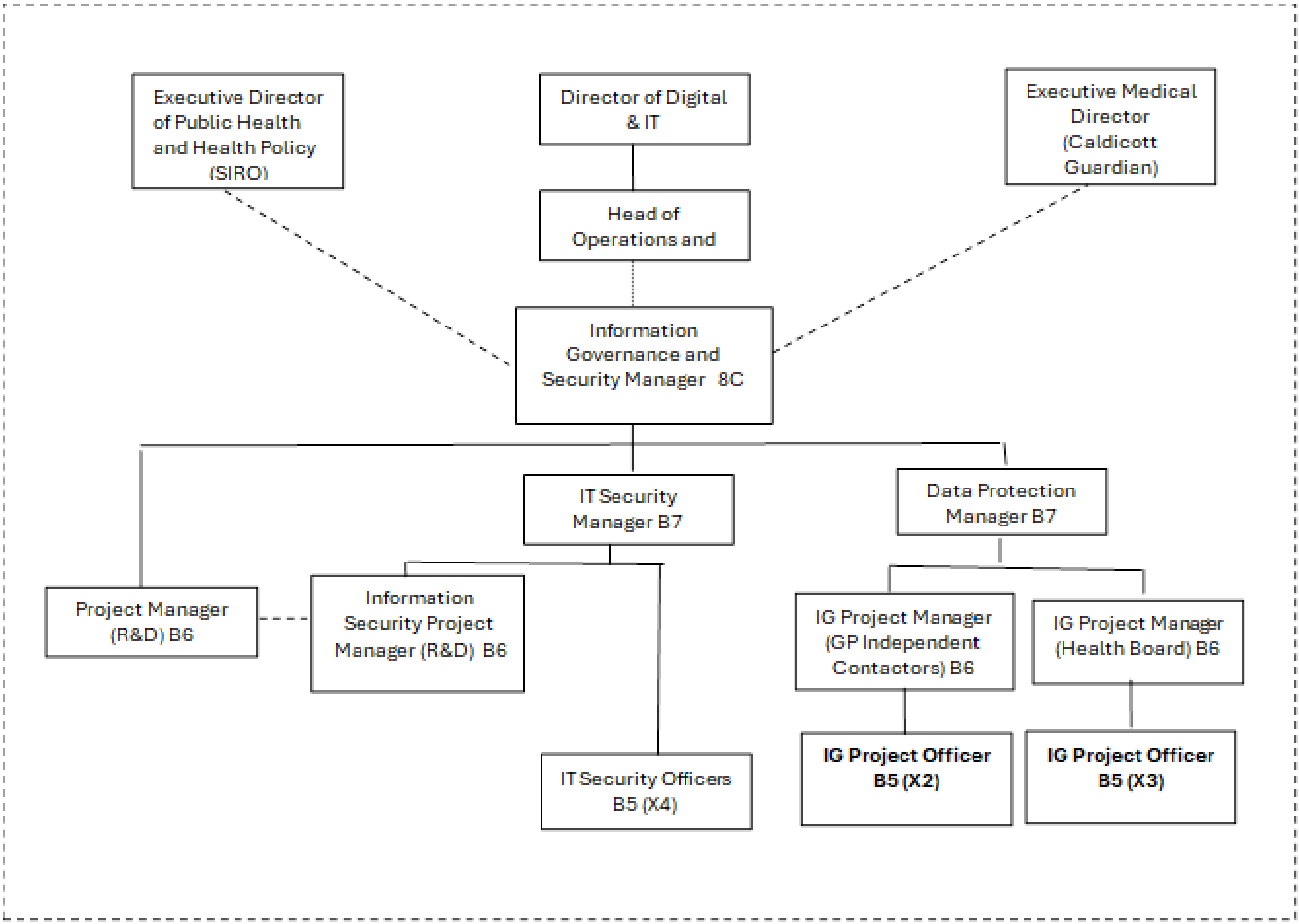
If you are unhappy with our response to your request, you do have the right to request us to review it. Your request should be made within 40 working days of receipt of this letter, and we will reply within 20 working days of receipt. If our decision is unchanged following a review and you remain dissatisfied with this, you then have the right to make a formal complaint to the Scottish Information Commissioner within 6 months of receipt of our review response. You can do this by using the Scottish Information Commissioner's Office online appeals service at www.itspublicknowledge.info/Appeal. If you remain dissatisfied with the Commissioner's response you then have the option to appeal to the Court of Session on a point of law.

If you require a review of our decision to be carried out, please write to the FOI Reviewer at the email address at the head of this letter. The review will be undertaken by a Reviewer who was not involved in the original decision-making process.

FOI responses (subject to redaction of personal information) may appear on NHS Lothian's Freedom of Information website at: https://org.nhslothian.scot/FOI/Pages/default.aspx

Yours sincerely

ALISON MACDONALD
Executive Director, Nursing
Cc: Chief Executive
Enc.


Executive Director of Public Health and Health Policy (SIRO)
Director of Digital & IT
Executive Medical Director (Caldicott Guardian)
Head of Operations and
Information Governance and Security Manager 8C
IT Security Manager B7
Data Protection Manager B7
Project Manager (R&D) B6
Information Security Project Manager (R&D) B6
IG Project Manager (GP Independent Contactors) B6
IG Project Manager (Health Board) B6
IT Security Officers B5 (X4)
IG Project Officer B5 (X2)
IG Project Officer B5 (X3)

JOB DESCRIPTION

1. JOB IDENTIFICATION

Job Title:	Data Protection Manager, NHS Lothian
Responsible to:	Information Governance and Security Manager, NHS Lothian
Department(s):	Operations and Infrastructure
Directorate:	eHealth
Operating Division:	NHS Lothian
Job Reference:	
No of Job Holders:	1
Last Update (insert date):	14 March 2018 org chart update Oct 2022

2. JOB PURPOSE

The Data Protection Manager is primarily responsible for ensuring NHS Lothian remains compliant with the Data Protection Legislation, supporting confidentiality legislation and professional guidance on all issues where the processing of personal data and information management has an impact on NHS Lothian and its staff.

The post holder will be Subject Matter Expert for the organisation and provide guidance and interpretation on all aspects of Data Protection, including policy implementation and development, first line support and specialist training to NHS Lothian staff at all levels of the organisation, including Executive Director level.

The European Data Protection Directive will be implemented in May 2018, and requires public authorities to appoint a Data Protection Officer to support organisational compliance with new legislation.

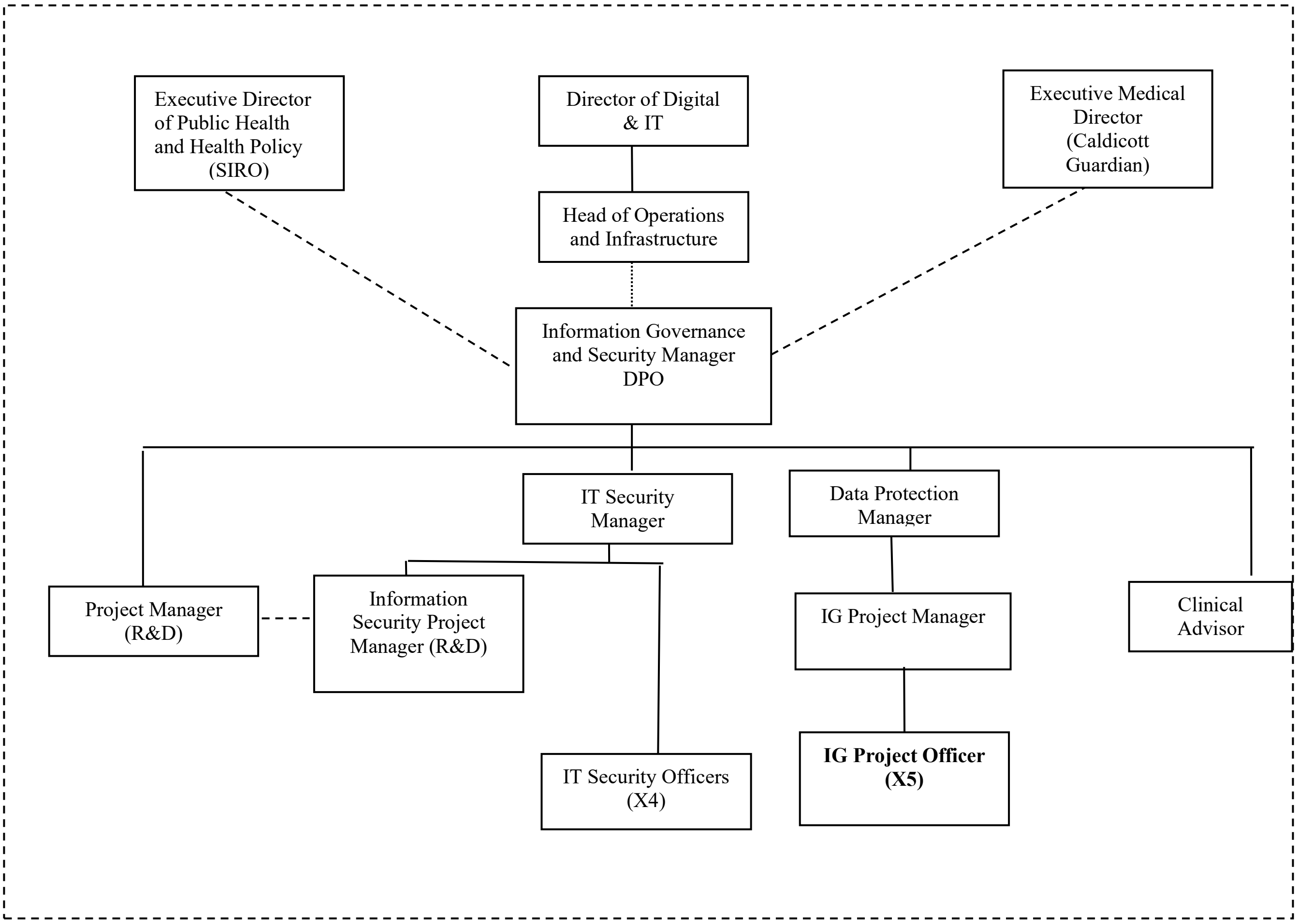
3. DIMENSIONS

- NHS Lothian employs approximately 28,000 staff and provides a full range of health services to the population of Lothian as well as some Scottish wide services, and all are subject to and must comply with Data Protection Legislation. NHS Lothian also has close links to a number of Universities, Further Education institutes and regulatory authorities both within the Lothian area and throughout Scotland and the United Kingdom.

- The Data Protection Bill legislates for the processing of all 'personal data' and has a wide scope within NHS Lothian, impacting on all operational and support departments. As well as patient data, the Act covers activities as diverse as the operation of Closed Circuit Television Systems and Human Resources policy and procedure.

- Limit impact on budget and reputational damage in cases of poor data protection if organisation subject to litigation.
- Line Management of Data Protection Project Officer
- Delivers specialist training to all staff including Executive level.
- Involved in multiple projects with one being complex (Implementation of the new European General Data Protection Directive)

4. ORGANISATION CHART


Executive Director of Public Health and Health Policy (SIRO)
Director of Digital & IT
Executive Medical Director (Caldicott Guardian)
Head of Operations and Infrastructure
Information Governance and Security Manager DPO
IT Security Manager
Data Protection Manager
Project Manager (R&D)
Information Security Project Manager (R&D)
IG Project Manager
Clinical Advisor
IT Security Officers (X4)
IG Project Officer (X5)

5. ROLE OF THE DEPARTMENT

Responsible for the development and implementation of eHealth strategies in NHS Lothian – Acute Division and community/AHP and Primary care / IJBs to support NHS Lothian's short, medium and long-term objectives. These strategies aim to implement a systems architecture that achieves the following Strategic Information Requirements:

- to support healthcare professionals in the delivery of patient care;
- to improve the patient journey through adequate communications between all sectors of healthcare;
- to monitor and improve the quality of care based on the results of medical, nursing and other professional indicators including Clinical Audit;
- to manage contracts between purchasers and the Board divisions effectively;
- to manage and improve service performance in financial and manpower terms;

- to identify the costs of care;
- to support teaching and research.

The provision of a comprehensive support service to our eHealth customers.

The eHealth Department is responsible for:

- eHealth Infrastructure and Operations, including Information Governance and Security
- eHealth Programmes, development and Training
- eHealth Health Records, which provide the following critical services: Admissions & Registrations; Records Library; Legal; Central Returns and Clinical Coding.

6. KEY RESULT AREAS

1. Subject Matter Expert in both Data Protection and associated legislation/practice for NHS Lothian, continually updating personal knowledge to ensure NHS Lothian policies and procedures remain compliant with current legislation and best practice. Associated guidance and legislation include the Human Rights Act 1998, the Freedom of Information (Scotland) Act 2002, the recommendations of the Caldicott Committee and the Public Benefit Privacy Panel for Scotland, the Information Commissioner's guidance and codes of practice and Scottish Government Health Department guidance. The post holder will be expected to deliver keynote speeches on all matters relating to the Information Governance agenda to large multi-disciplinary professional groups at both local and national level.

2. For urgent and also daily information governance or security incidents audit and analyse highly complex situations and facts, interpreting in conjunction with legislation and taking prompt action on behalf of NHS Lothian where there may be no precedent.

3. Propose and lead on the development and implementation of policies and standards for data protection and confidentiality throughout NHS Lothian, including the drafting and consultation of policy documents as well as presenting the documents to the NHS Lothian Information Governance Assurance Board for final approval.

4. Propose and lead on the development, implementation and monitoring of Protocols and actively participate in the implementation and development of systems for sharing and communicating information to and from partner organisations including the four Lothian Unitary public authorities, Lothian and Borders Police and NHS Lothian partner non-statutory organisations.

5. Lead on the development and maintenance of ongoing strategy and action plans to ensure that the organisation achieves and maintains compliance with the Data Protection Legislation, Caldicott Guidance and associated topics relating to Information Governance compliance. The post holder will be directed and assisted in this area of work by recommendations, guidance and professional support from the NHS Lothian Information Governance Assurance Group and Information Governance Working Group.

6. Lead, develop and implement training materials relating to data protection for NHS Lothian, and to deliver appropriate training to clinical, non-clinical and managerial staff at

all levels in the organisation. The post holder will be expected to work with Training staff and Data Protection Officers both within NHS Lothian and in partner NHS Scotland organisations to ensure consistency of work and availability of training on a wide number of media, including the creation and maintenance of e-learning packages.

7. Develop effective working relationships with staff at all levels throughout the organisation to ensure that data protection and confidentiality issues are given a high profile. The post holder will meet with all levels of management and staff side on an ad-hoc basis to promote awareness of staff obligations under the Data Protection Act and Common Law on Confidentiality. The post holder will provide ad-hoc advice to all members of staff, both by telephone and written communication, including email.

8. Review and approve, prior to introduction into routine use, any new or revised documents, procedures and systems to minimise data protection risks, taking into account any change in Data Protection practice and/or changes in technology. The post holder will be required to regularly form part of multi-disciplinary short-life working groups to ensure that this requirement is met.

9. Manage, audit and and oversee the organisation's response to requests from data subjects, under the Data Protection Act, for access to their personal data and other statutory rights given to data subjects under the Sixth Data Protection Principle. Responding to complaints from members of the public and external regulators regarding potential breaches of legislation

10. Ensure that the organisation's Data Protection Notification to the Information Commissioner's Office is kept up-to-date and that renewal applications and fees are remitted appropriately. This requires the implementation and maintenance of an organisation-wide database holding details of all systems processing personal data to ensure the organisation is aware of all the personal data it is controlling.

11. Line management of the Data Protection Project Officer, who will provide professional and administrative support for the post holder. Including recruitment and selection, sickness absence, appraisal, workload allocation, personal development plans discipline/grievance and training

12. Deputise for the Information Governance and Security manager when required to ensure the smooth and effective delivery of services.

7a. EQUIPMENT AND MACHINERY

Using a personal computer (PC), photocopier, scanner, mobile phone in order to carry out day-to-day job.

7b. SYSTEMS

- Microsoft Outlook – writing, reading and managing email communications to and from colleagues, staff, customers and external bodies.
- Microsoft Office – day-to-day usage for production of documents, presentations and general project administration.

- Microsoft Project – development and monitoring of project plans (simple and complex)
- The post holder will review new applications and will have to develop knowledge on each of these.
- The post-holder will access the audit-log functionality of clinical/administrative systems on an ad-hoc basis to monitor and/or identify actual or potential misuse of clinical systems by staff.
- Lead, specify, develop and implement Subject Access register to audit, adapt and improve system to store and disseminate information relating to receipt and management of requests from public and staff in line with DPA legal timelines.
- Lead, specify, develop and implement the NHS Lothian Information Asset Register system as outlined in the General Data Protection Regulation (GDPR). The post holder is responsible for legislation compliance by ensuring NHS Lothian maintain a register of all information assets across all departments which contain personal identifiable information on behalf of the Senior Information Risk Owner (SIRO) relating to the organisations Information assets and associated risks. Supporting service improvement by audit and enhancement.

8. ASSIGNMENT AND REVIEW OF WORK

The post holder will work on a largely autonomous basis to ensure NHS Lothian remains compliant with Data Protection and associated confidentiality legislation and practice. Workload will be self directed with informal discussions and regular meetings with the Information Governance and Security Manager.

Work is reviewed annually through the Appraisal and Development System.

The risks associated with Data Protection require that regular meetings take place between the Data Protection Manager, The eHealth teams and the senior management teams. The post holder will attend the Information Governance Assurance Board and any other Committee as required/requested by senior management.

9. DECISIONS AND JUDGEMENTS

The post holder works to achieve agreed objectives and has autonomy when dealing with both team related decisions and allocation of workload and duties. As Subject Matter Expert for the organisation, the post holder's decision making processes will be mainly based on statute, common law and legal guidance.

The post-holder must be able to make decisions regarding highly complex issues or situations which will have an impact on multiple departments/professions within the organisation.

The post is self-directed, and the post-holder needs to be able to prioritise his/her own workload and that of the team.

10. MOST CHALLENGING PART OF THE JOB

- Plans and organises a broad range of complex activities to support compliance with Data Protection Legislation, contributing to formulation of NHS Lothian organisational strategy for new legislation such as the European General Data Protection Directive.

- To understand and interpret the Data Protection Legislation and associated legislation, and the implications these have throughout the organisation. In some cases this may require the Data Protection Manager to personally challenge long established standards and practice that may be in breach of the Act, and to suggest practical solutions that will minimize risk to the organisation.

- To work autonomously and proactively to achieve an adequate level of awareness of current legislation and its associated responsibilities for all staff throughout a large and complex organisation.
- Receiving and analyzing complex information from stakeholders, colleagues and external sources regarding all aspects of project(s) or incidents, and ensuring that it is presented in an appropriate manner to allow decisions to be made effectively.
- Interpreting complex facts, comparing a range of options and proposing solutions to management.

11. COMMUNICATIONS AND WORKING RELATIONSHIPS

The Data Protection Manager will provide and receive highly complex information relating to legislation and practice where agreement and cooperation is required, including in presentations to large multidisciplinary groups of staff and external organisations.
Liaise with staff in other NHS organisations and agencies regarding the development and implementation of the policies(s).
Liaise, negotiate and communicate effectively with external contractors and suppliers.

Internal:

- Lothian eHealth teams and a range of project Boards.
- Director of Public Health
- local management teams and Heads of Service throughout NHS Lothian

External:

- The Scottish Government policy adviser on confidentiality and Data Protection
- The NHS Scotland Data Protection Adviser
- The Health Compliance team at the Office of the Information Commissioner in Wilmslow
- The Scottish Compliance team at the Office of the Information Commissioner in Edinburgh
- Represent the organisation at NHS Scotland Data Protection Forum.

The postholder is required to communicate directly with patients as a noted point of contact on information leaflets for advice on Data Protection Legislation, subject access and confidentiality matters.

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

- Standard office conditions Light to moderate: includes moving light equipment, e.g., briefcases/lap-tops, projectors for presentations; using keyboards regularly/frequently for word processing, spreadsheets, etc and email. Delivering training sessions can involve prolonged (up to 4 hours) periods of standing.
- Intense concentration/in-depth mental attention frequently required, e.g., 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 complex/changing environments.
- Exposure to distressing circumstances involves from time to time dealing with conflict situations e.g., conversations meetings with distresses or angry patient in relation to their health record personal data. Dealing regularly with challenging problems requires sustained emotional energy/resilience.
- Providing support to staff members on personal issues.
- Frequent travelling to all NHS Lothian sites, other health boards and to suppliers premises.

13 QUALIFICATIONS AND/OR EXPERIENCE SPECIFIED FOR THE POST

Essential

- Educated to MSc level or equivalent in an Information Governance MSc programme or equivalent.
- The post holder must hold the British Computer Society Information Systems Examination Board Certificate in Data Protection.
- Significant highly specialised knowledge and experience of working with the Data Protection Act and associated confidentiality legislation, liaising with legal bodies and appropriately advising the organisation. This need not be in the NHS although highly desirable.
- Skills in interpreting legal and parliamentary language.
- A high level of knowledge of current information sharing practice between public and non-statutory authorities in Scotland.
- A wide knowledge of the National Health Service in Scotland

14. JOB DESCRIPTION AGREEMENT

Job Holder's Signature Date

Senior Officer/Head of Department:

Signature Date

Title

Job Analyst:

Date Job Descriptions Agreed:

JOB DESCRIPTION

1. JOB IDENTIFICATION

Job Title:	IT Security Manager
Responsible to:	Information Governance and Security Manager
Department(s):	eHealth (Digital and IT) Department
Directorate:	Medical Directorate
Operating Division:	NHS Lothian
Job Reference:	HB-FCS-PLDN-ITSM1(RE)
No of Job Holders:	1
Last Update):	27th August 2021

2. JOB PURPOSE

To provide leadership and management of the NHS Lothian IT security team and services providing technical direction and guidance on highly complex matters of Information Security Technical Controls, Procedures and Standards. To ensure that NHS Lothian achieves and maintains the legal, regulatory and governance compliance with Network and Information Security Regulations (NISR), Cyber Essentials and NHS Lothian Security Standards. To collaborate and project manage with partner organisations on a range of complex and sensitive security issues, act as the lead specialist on Information and Cyber Security to other IT Professionals, Clinicians and all staff in NHS Lothian.

To devise, develop, implement, monitor, maintain and report on a range of Information and Cyber Security Policies Standards and Procedures across all of NHS Lothian and ensure staff awareness and adherence. To maintain the security and integrity of digital data and communications for NHS Lothian and to other partner organisations, to the required confidential and legal standards and providing assurance and resilience.

3. DIMENSIONS

Finance

Budget management responsibility

Project – making recommendations on the procurement of security systems and tools used throughout the organisation, once agreed responsible for budget associated with assigned security related projects. Project Budget varies as security work programmes are funded through new business cases

Responsible for proper and safe use of IT equipment by users, and also expensive IT equipment and software.

Staff - Direct

Line Management of 5 security staff (Information Security project manager and 4 IT Security Officers)

Security Projects/Workload

The role will be required to run up to 6 concurrent projects of which 2 or 3 may be complex

End-users / clients affected by Security activities

Service users: 28,000, including Service Managers, Clinicians and supporting staff.

Sites covered: Lothian wide >150 (primary and secondary care including GPs and partner agencies).

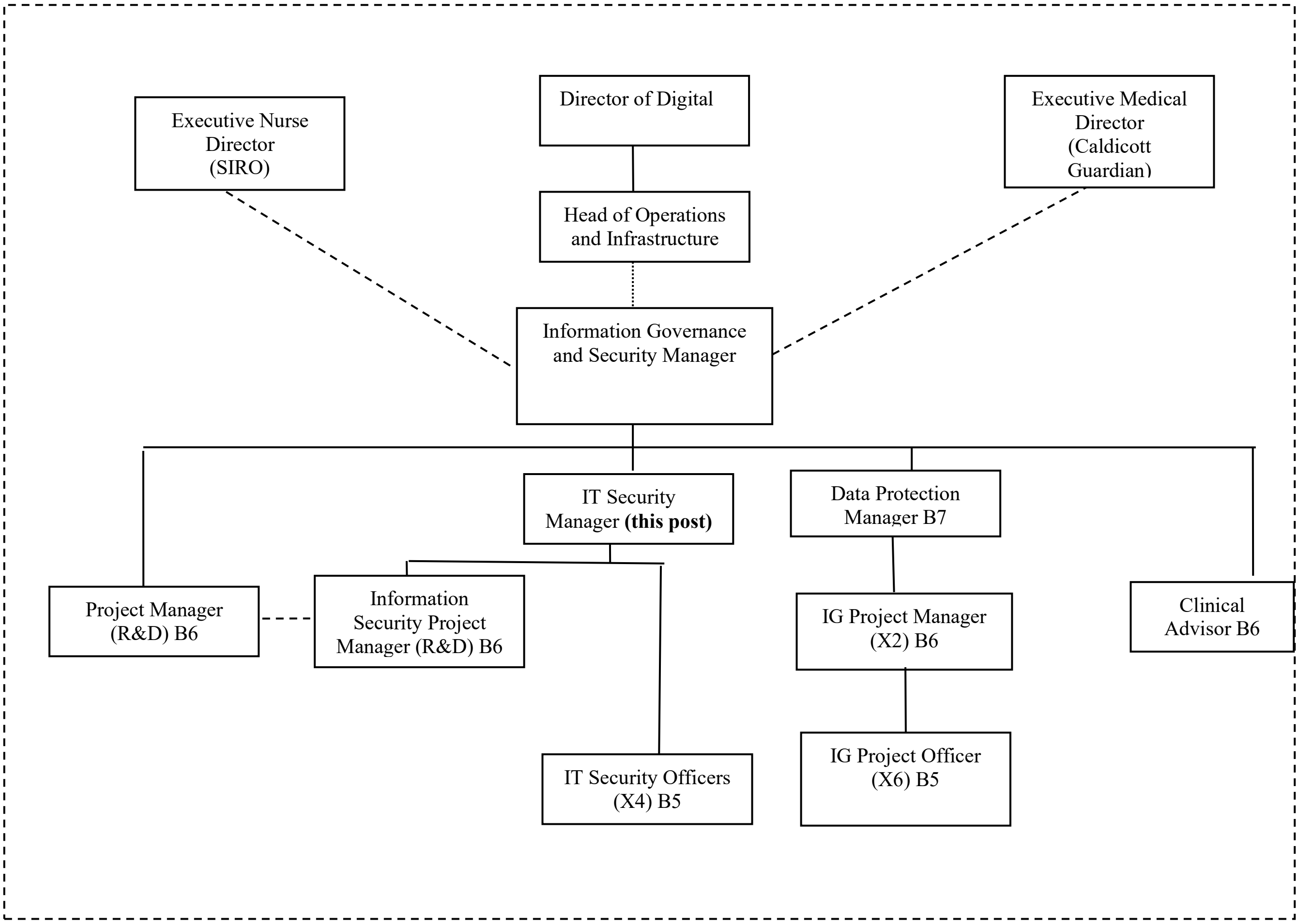
Security Activities

The NHS Lothian IT Security services include area-wide Intrusion Detection, Mail screening, Data Loss Prevention, Web Page and FTP screening, Internet Access control and Firewall protection. The secure communications between NHS Lothian and our partner Local Authority networks and remote access provision are also within the scope of this post.

Reporting performance against external audit for the European Network and Information Systems (NIS) Directive which requires NHS Boards to demonstrate organisational compliance with new legislation and report to the supervisory authority.

The key delivery in this role is to inform, influence and direct NHS Lothian, independent contractors and where applicable, third sector organisations in relation to the security of their information assets, networks and processes.

4. ORGANISATIONAL POSITION add key solid and broken line responsibilities


Executive Nurse Director (SIRO)
Director of Digital
Executive Medical Director (Caldicott Guardian)
Head of Operations and Infrastructure
Information Governance and Security Manager
IT Security Manager (this post)
Data Protection Manager B7
Project Manager (R&D) B6
Information Security Project Manager (R&D) B6
IG Project Manager (X2) B6
Clinical Advisor B6
IT Security Officers (X4) B5
IG Project Officer (X6) B5

5. ROLE OF DEPARTMENT

Responsible for the development and implementation of eHealth strategies in NHS Lothian – Acute Division and community/AHP and Primary care / IJBs to support NHS Lothian's short, medium and long-term objectives. These strategies aim to implement a systems architecture that achieves the following Strategic Information Requirements:

- to support healthcare professionals in the delivery of patient care;
- to improve the patient journey through adequate communications between all sectors of healthcare;
- to monitor and improve the quality of care based on the results of medical, nursing and other professional indicators including Clinical Audit;
- to manage contracts between purchasers and the Board divisions effectively.
- to manage and improve service performance in financial and manpower terms.
- to identify the costs of care;
- to support teaching and research.

The provision of a comprehensive support service to our eHealth customers.

The eHealth Department is responsible for:

- eHealth Infrastructure and Operations, including Information Governance and Security
- eHealth Programmes, Development and Training
- eHealth Health Records, which provide the following critical services: Admissions & Registrations; Records Library; Legal; Central Returns and Clinical Coding.
- eHealth innovation

6. KEY RESULT AREAS

1. Devise, implement and maintain the development and enforcement of NHS Lothian security policies and standards in order to ensure that all known and anticipated risks to the integrity, confidentiality and availability of information are countered.
2. Manage organisation reporting for the maintenance and monitoring of systems that ensure NHS Lothian's compliance with the requirements of NHS Scotland Information Security Policy Framework. Including the current information security legislation that protect the organisations patients, staff and systems from loss, corruption or inappropriate access to their data, such as Cyber Essentials and Network Information Systems (NIS) Directive Reporting performance against external audit (capture this in key results also) for the European Network and Information Systems (NIS) Directive.
3. Provide recommendations on procurement and risk assessments that analyse, interpret and communicate highly complex requirements for internal and external equipment suppliers and contracts, ensuring NHS Lothians IT infrastructure remains technically secure
4. To evaluate, recommend, sign off purchase, installation, training and maintenance of suitable organisational IT systems and equipment and organise and purchase training to be used in the provision of an IT Security service, investigations and secure data transfer.
5. Responsible for day to day line management of the IT security team, including recruitment and selection, sickness absence, leave, appraisal, workload allocation, personal development plans discipline/grievance and training.
6. Deputise for the Information Governance and Security manager when required to ensure the smooth and effective delivery of services.
7. Works closely with various senior staff in the organisation, such as the Digital and IT leads, senior members of Human Resources, senior clinicians to progress actions to enforce policy, advise on matters relating to information and cyber security, contingency planning, manage security breaches from individuals, and advise on disciplinary matters relating to security
8. Responsibility for organisational management of Endpoint Control software, including planning, development, review, update, upgrade. Managing the Data Loss Prevention (DLP) process, whilst ensuring accurate collection and interpretation of evidence and also work closely with other departments within NHS Lothian and equivalents within partner agencies, to ensure adherence to information and cyber security policies.
9. Work closely with technical colleagues to direct, advise and facilitate delivery of effective IT Security and data protection, including projects and services, measuring performance and producing reports for the organisation

10. Planning the provision of a complex IT Security service and associated systems on behalf of NHS Lothian, to ensure compliance with government legislation including the Data Protection Act 2018, Cyber Essentials and Network Information Systems Regulations (NISR) and co-ordinating the provision of local and national IT Security across other health boards
11. Responsible for defining requirements, evaluation and implementation of new security software and systems across the organisation and liaising with various organisational departments to plan the rollout of new systems, projects and policies
12. To plan, develop training material, guidance and deliver training and advice to the organisation around security management of information and its systems.
13. To define, undertake and monitor a formal security vulnerability and penetration testing programme, and derive appropriate test plans to assure compliance
14. Co-ordinate policy and practice with IT Security Officers in the four Local Authority partners to ensure that the security and integrity of joint services are maintained and agreed procedures for systems access are followed.
15. Supervise the maintenance of registers of IT assets, systems, users and access privileges in order to maintain current accreditation details, so that security policies and standards can be monitored.
16. Manage an IT Security service to the Research & Development and innovation teams, reviewing clinical trials and security compliance, to provide risk assessments that analyse, interpret and communicate complex requirements for applications and hardware and inform internal and external sponsors and making recommendations
17. To support NHS Lothian's values of quality, teamwork, care and compassion, dignity and respect, and openness, honesty and responsibility through the application of appropriate behaviors and attitudes.

7a. EQUIPMENT AND MACHINERY

The post holder will have knowledge and experience of the following equipment:

Laptop, Personal Computer, Printer, Scanner, Photocopier.

Data Projectors, Mobile Phone/ Telephone.

7b. SYSTEMS

The post holder will have knowledge and experience of the following Operational and security management systems:

Ivanti Device and Application Control Management (management of endpoints, port control and encryption)

Cisco AMP for endpoints (advanced malware protection)

Cisco Security Management Appliance (Firewalls, web security, mail screening, routing and policy including Data Loss Prevention and investigation)

Microsoft System Centre Configuration Manager (SCCM) Software management

NTX gateway\VPN System\Remote access

ServiceNow IT Services management system

ISO 27001 Information Security Standards

IT Security Knowledge base:

- The UK National Cyber Security Centre (NCSC)
- The Scottish Health Competent Authority
- The Information Systems Security Certification Consortium
- The SANS (SysAdmin, Audit, Network, Security) Institute
- The Information Systems Audit and Control Association
- The US CERT (Computer Emergency response Team) Co-ordination Centre
- The National Institute of Standards and Technology (NIST)
- The Common Vulnerabilities and Exposure system (CVE)
- The NHS Scotland Information Security community
- The NHS Scotland Cyber Security Group

And general NHS Lothian IT Systems:

Intranet/Internet Applications – Cloud based and local hosting Systems.
Corporate Information systems - Management Dashboards, Finance and HR systems including eESS, eLearning (learnPro) modules (Mandatory and Optional) and Turas

MS Office Applications - MS Project, MS Office - Outlook / Email, Visio, Word, Access, Excel, Powerpoint

8. ASSIGNMENT AND REVIEW OF WORK

The post-holder will operate as the lead specialist in IT Security with a high level of autonomy. In particular where matters of security are concerned fast, decisive action is imperative in order to preserve the integrity of key business facilities, systems and electronic forensic evidence.

Responsible for the management and reporting of work requests for the IT Security team from across the NHS Lothian organisation via Service Now (including incident logging with self service capabilities, facilitating change management, and also providing a knowledge base for end users on security matters.

The programme of work is agreed with the Information Governance and Security Manager, and regular reviews of progress will be maintained. Day to day operations and priorities are self - initiated to work effectively with a number of other departments and organisations.

Work is reviewed at routine meetings with line manager and annually through the Turas

Appraisal and PDP System.

9. DECISIONS AND JUDGEMENTS

The post holder is required to make decisions regarding the development of strategy and the execution of supporting policy, processes and procedures necessary to deliver secure IT services in support of key business processes (including review of National security policy and agreeing wider inter-organisational frameworks for security and access, securing cloud-based services such as Office 365, and the security arrangements protecting all information systems that are locally hosted in NHS Lothian)

The postholder has to exercise judgement on the appropriate use of current systems and infrastructure (including risk assessment of the connectivity of new and existing systems to NHS networks, the on-going monitoring of these and investigation of inappropriate disclosure of information, breaches or potential breaches of security and detecting unusual usage trends)

Decisions regarding the efficacy of the existing systems, relating to the on-going need, relevance and practicality of the systems in place (including the Monitoring of system access, fair warning reports, potential local vulnerabilities based on wider cyber threat alerts)

Respond to enquiries from the user community in relation to the use of the mail systems and general IT security issues (including discussion of the security arrangements around Office 365 components such as MS Teams, Sharepoint and Onedrive, and the limitations of local controls of the National NHS Scotland Office 365 tenancy)

Make relevant suggestions/recommendations at operational/risk and IT group meetings; determine best practice at all areas of the business (including what requires to be in place to support information sharing agreements hosting staff and patient information, such as HR and clinical systems)

Define response to incidents in line with the relevant reporting criteria (including incident reporting for small, medium and large data breaches, cyber attacks and the activities of individual staff members who by not following policy leads to security issues)

10. MOST CHALLENGING/DIFFICULT PARTS OF THE JOB

Devising appropriate strategies and initiatives to:

- balance risk management and business operational requirements in a rapidly changing technical environment.
- promote and sustain security awareness and best practice
- exercise problem solving skills in response to a diverse pattern of technical, logistic, management and organisational issues that frequently arise in connection with Information Technology

- balance activities due to prioritising unpredictable and conflicting demands

11. COMMUNICATIONS AND RELATIONSHIPS

Internal

The post holder manages the work of the IT Security Officers and the Information Security Project Manager (R&D). In addition, there are regular communications in connection with:

- Co-ordination with the other members of the eHealth team on matters arising from the technical management of the local network in order to maintain service standards.
- Provide and receive information to and from staff and management at all levels throughout NHS Lothian on highly complex and sensitive Security matters, pertaining to the organisation as a whole and individual staff members.
- Liaise with Staff and Management at all levels throughout NHS Lothian to identify and analyse individual, group and organisational IT security training needs.

External

- Regular communication with the strategic IT service providers on matters of service continuity, security and integrity.
- Liaison with third party contractors for special technical requirements for local and peripatetic users.
- Regular operational contact with IT Security and technical staff in the four LA partner organisations, and their contractors, on communications and related security matters.
- Liaison with Scottish and UK IT Security advisors and management authorities.

Methods of Communication

These will include face to face dialogue, formal presentations, written reports, and response to mail and telephone enquiries.

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

Physical Skills and Effort:

- Computer use on a daily basis using advanced keyboard skills for detailed analysis and review of security information
- Long periods of sitting at screen/keyboard within an office environment

Mental Effort:

- Regular, intense concentration is required for fault diagnosis or the investigation of security alert and for the forensic review of complex security issues, and to maintain a high level of accuracy underpinning reported security matters which may relate to organisational reputation or matters of individual discipline.

- Concentration required when managing security incidents involving shutting down essential clinical services, denying access to services, or investigating illegal activity.

- Concentration required when providing specialist evidence at Hearings, Tribunals or in Court and being subjected to cross examination, on a quarterly basis

- Required to negotiate with external suppliers and external security assessors to ensure quality security products and services are implemented to meet internal organisational and external NHS security requirements.

Emotional Effort:

- Influencing and directing all levels of NHS staff to adhere to security and confidentiality policies and take difficult decisions (such as investigating, following up policy breaches and security breaches and providing reports to senior management, HR and Tribunals for evidence) to ensure that NHS Lothian polices are being upheld.

- Staff management responsibilities which may require undertaking disciplinary procedures if required.

Working Conditions:

- Standard office conditions with ongoing use of computer equipment / VDUs for more than half shift, on a daily basis.
- Required to travel to attend meetings related to security matters and to investigate security incidents, in general at least two days / week, and established meetings on a monthly cycle

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

Requires a Degree or equivalent qualification in an Information related discipline, demonstrating analytical and deductive capacity, and skills to collate, order, and summarise information

Plus additional specialist IT security knowledge or experience obtained through post-graduate diploma or equivalent experience (to SCQF level 10), including:

Formal IT Security qualifications, including Certificate in Information Systems Management Principles or Certified Information Systems Security Professional(CISSP) or equivalent to demonstrate accreditation in IT risk assessment and management and the detection and mitigation of security incidents

Evidence of Continuing Personal Development including industry recognised IT Security courses and attending conferences

Excellent knowledge and experience in the management of IT security systems – including desktop anti-virus protection, mail screening, web access control and monitoring, and firewall configuration.

Experience of creating or maintaining an Information Security Management System

A comprehensive knowledge of a wide range of Microsoft products, desktop environments, and network operating systems.

Experience of staff management/leadership.

Strong interpersonal skills and the aptitude to support and inspire others

Good negotiation skills for the effective planning and co-ordination of work conducted by several organisations.

Effective written and verbal communication skills

Organisational, Planning and Problem-solving skills

Experience operating as part of a multi-disciplinary and/or multi-organisational team

14. 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: Head of Department Signature:	Date: Date:

JOB DESCRIPTION

1. JOB IDENTIFICATION

Job Title:	Information Governance and Security Manager
Responsible to:	Head of Digital Infrastructure and Operations
Department(s):	Information Governance and Security
Directorate:	Digital and IT
.	
Operating Division:	Corporate Services
Job Reference:	L-EHEALTH-IGSM(RE)
No of Job Holders:	1
Last Update (insert date):	September 2023

2. JOB PURPOSE

To develop, lead, influence, advise and provide long term strategic leadership to ensure NHS Lothian manages the integrity, governance and security of NHS Lothian and to ensure the governance and security of NHS Lothian personal data, and operationally independent as the organisation's 'Accountable Data Protection Officer' as required by the General Data Protection Regulations (GDPR) to ensure the Health Board is legislatively compliant.

The post holder is also responsible for organisation management and development of security information systems and development of organisational and national policy, and is audit lead for the Network and Information Systems Regulations (NISR).

Providing corporate level strategic leadership relating to Information Governance driving progress and ensuring that the Health Board is in compliance with all relevant regulations.
The post holder will directly influence and advise NHS Lothian and independent contractors on all Data Protection and IT security matters with other NHS organisations, and with external organisations such as police, councils, voluntary sector, Central Legal Office, and third party suppliers both on behalf of the Health Board and Nationally as chair of NHS Groups.

3. DIMENSIONS

Staff – Direct

i. Line management responsibilities for multiple departments; Information Governance departments (Corporate and Independent Contractors), IT Security departments (Corporate and Research and Development) .

ii. Responsible for line management of over 15 staff including; recruitment and selection, sickness absence, appraisal, workload allocation, personal development plans and disciplinary/grievance.

iii. Management of multi disciplinary project teams and boards, from Health Board, divisional service and user departments, IM&T technical staff and suppliers.

iv. Management and specialist responsibility for Information Governance and Security for the Health Board and all sites, independent contractors, and for numerous systems in use across the councils and other health boards in the south of Scotland.

v. Lead on teaching/training and awareness for Information Governance, Data Protection, IT Security (including mandatory training) across the Health Board for all staff, student and contractors.

Projects/activities

Multiple concurrent complex projects and tasks across multiple areas, completely separate areas and sites.

End-users/clients affected by projects/activities

Organisation wide applications (32,500 users) for multiple Clinical and Administrative functions. Security for all NHS Lothian devices (33,000). Systems used by all Lothian councils and by health boards across the south east region of NHS Scotland.

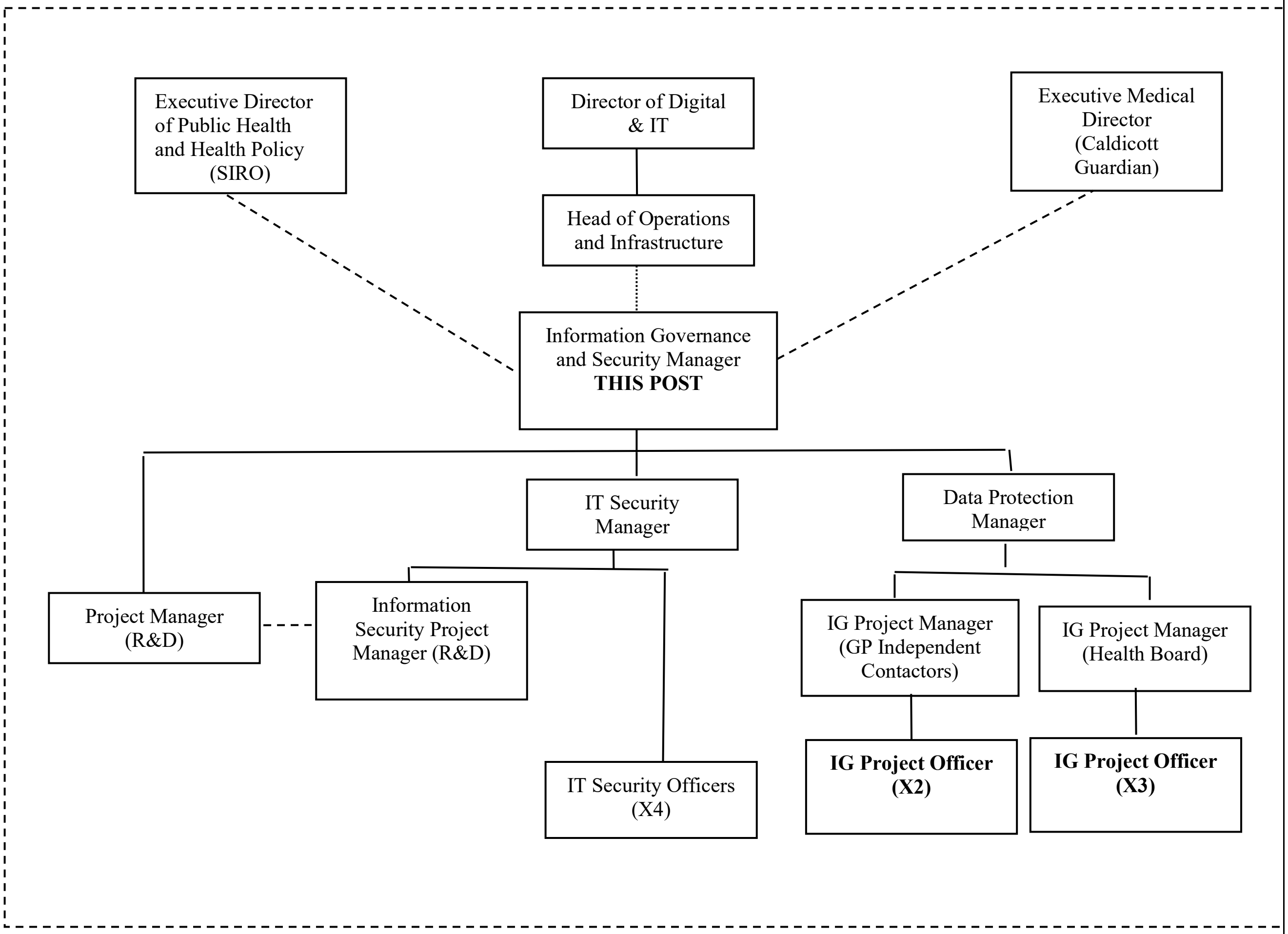
Finance

vi. Budget: responsible for authorising and monitoring of department expenditure and IM&T project budgets of up to value of £150k.

vii. Recommend, specify procure and allocate of Project IM&T equipment such as PC's, printers, consumables, software servers, interfaces and application screens.

viii. Accountable for both pay and non pay expenditure within this allocated budget of £1.5M. This is spread across multiple departments; Information Governance departments (Corporate and Independent Contractors), IT Security departments (Corporate and Research and Development), network security and technical service contracts budgets

4. ORGANISATIONAL POSITION


Executive Director of Public Health and Health Policy (SIRO)
Director of Digital & IT
Executive Medical Director (Caldicott Guardian)
Head of Operations and Infrastructure
Information Governance and Security Manager THIS POST
IT Security Manager
Data Protection Manager
Project Manager (R&D)
Information Security Project Manager (R&D)
IG Project Manager (GP Independent Contactors)
IG Project Manager (Health Board)
IT Security Officers (X4)
IG Project Officer (X2)
IG Project Officer (X3)

5. ROLE OF DEPARTMENT

The Digital and IT Department provides the following functions:

Digital and IT Services brings together Health Records, Infrastructure and Operations, IT Security, Data protection, Training, Programmes and Projects, Software Development and Innovation within NHS Lothian.

The department is responsible for the development and implementation of Digital and IT strategies in NHS Lothian to support the organisation meeting short, medium and long-term objectives. These strategies aim to implement a systems architecture that achieves the following Strategic Information Requirements:

to support healthcare professionals in the delivery of patient care;

to improve the patient journey through adequate communications between all sectors of healthcare;

to monitor and improve the quality of care based on the results of medical, nursing and other professional indicators including Clinical Audit;

to manage contracts between purchasers and the divisions effectively;

to manage and improve service performance in financial and manpower terms;

to identify the costs of care;

to support teaching and research.

The department provides a comprehensive support service to our Digital and IT customers and is responsible for supporting service areas in day to day operation and when considering or undergoing organisational change and to assist them in improving service quality, efficiency and value.

6. KEY RESULT AREAS

1. To lead the long term organisation plan, strategy, management and performance of the Information Governance and Information Security for NHS Lothian, and represent Lothian with external bodies. Lead on corporate reporting on Information Governance and IT Security matters including compliance and with external regulators.

2. Line management responsibilities for multiple departments; Information Governance (Corporate and Independent Contractors) and IT Security departments (Corporate and Research and Development) including recruitment and selection, sickness absence, appraisal, workload allocation, personal development plans and disciplinary/grievance.

3. Take a lead responsibility as an operationally independent ‘Accountable Data Protection Officer’ as required by the General Data Protection Regulations (GDPR), with operational independence and direct reporting to two Executive Directors (Caldicott Guardian and Senior Information Risk Owner - SIRO). The post holder must maintain profile as subject matter expert in Data protection and associated

legislation/practice for NHS Lothian, continually updating personal knowledge to ensure NHS Lothian policies and procedures remain compliant with current legislation and best practice. The post holder will be expected to deliver keynote speeches on all matters relating to the Information Governance agenda to large multidisciplinary professional groups at local, national and international level.

4. Develop and take a lead management role in ongoing teaching and training of staff, students and contractors across the Health Board area relating to Information Governance, Data Protection and Information Security. Ensure that risk from end user computer misuse is minimised by including Information Governance in induction and mandatory training programmes, and undertaking regular audit/analysis of information services functions, policy implementation, user information needs, information system utilisation and effectiveness.
5. Develop and take lead for implementation, development and maintenance of NHS Lothian organisational Information Governance and Security Policies in line with national policy and legislation for the organisation, ensuring organisational policies and procedures are implemented in all Health Board and divisional departments.
6. To Develop lead, manage, implement, initiate and develop Information Governance strategy and policy matters by working jointly with NHS Lothian, IJBs and external agencies to develop and implement patient information sharing protocols, policies and practices within legal constraints, for implementation across the Health Board and all of the associated agencies in line with national policy and legislation. Develop, lead, specify, develop and implement the information governance aspects of the NHS Lothian information strategy, policies and tutored/e-learning based training strategy and service. Liaising with internal and external customers to plan required service provision and service levels.
7. Provide specialist advice directly to both the Caldicott Guardian (Executive Medical Director), Senior Information Risk Owner (SIRO Executive Director of Public Health and Health Policy), senior members of staff in the NHS and in partner agencies, including interpretation on a range of national confidentiality policy and legal matters, including areas where there may be where there may be no precedent.

8. Work productively with senior clinicians and managers , including those in external agencies for; information provision enquiries & reporting, taking a lead in Data Sharing across Lothian and Borders, incident recording, confidentiality and Data Protection Act (2018). Ensure that national & local requirements are supported in respect of the provision of shared, statutory & ad hoc requests for information.
9. Develop and take the lead on planning programme management of the organisation’s information assurance strategy, programme and its constituent projects, providing compliance reports to the Digital Portfolio Group on utilisation of Information Services functions and systems, managing relevant budgets, preparing Business Cases and long term strategic plans which impact across the Health Board, independent contractors and suppliers. Develop and take the lead on the delivery of all Data Protection and IT security Strategic Plan organisation wide as part of the and long term vision of Digital and IT development, encourage collaboration and co-operation within

the spirit of partnership.

10. Undertake regular and one off highly complex audit and evaluation exercises to analyse services, requirements and systems, and participate in research and development designed to improve the information governance function.
11. As Digital and IT service account manager provide management and digital expertise to a number of units and external parties to support Digital performance management for strategic and operational change and act as an escalation point. Manage the interface with the information service delivery and project development groups to ensure that queries and problems are addressed according to agreed standards.
12. Develop and take lead on strategic plan and Project Manage a number of information projects related to the development of the Information Services functions and systems across the Health Board, adjusting long term strategic plans to adapt to changing strategy and priorities. Manage multi-disciplinary project boards and teams to; specify requirements, plan, develop, test, implement, evaluate, realise benefits and rollout information systems. Using PRINCE2 project management methodology and documentation.
13. Develop and take lead for the board on the long term strategic plans and detailed action plans to ensure that organisation wide Lothian achieves and maintains ongoing compliance with the Data Protection Act 2018, Network and Information Systems Regulations 2018 rolling three year audit cycle, Caldicott guidance and associated topics relating to Information governance compliance.
14. Develop and take the lead on long term strategy and management of Health Board and independent contractor Data Protection compliance and service Office, and provide Data Protection Officer (DPO) expert guidance in confidentiality matters. Provides specialist advice, advising the Health Board Caldicott Guardian and Senior Information Risk Owner (SIRO), including interpretation on a range of national confidentiality policy and legal matters, including areas where there may be where there may be no precedent.

15. Oversee and control the portfolio of applications, allocating responsibilities as required, dealing with external suppliers and engaging internal sponsors in order to ensure that all applications deliver the business benefits and in particular: Ensure Information Governance and security aspects are embedded in design, development, review, update and implementation of existing and new information systems across the organisation, to meet user requirements in line with local business requirement and Digital and IT strategy. Ensure that new systems developed and implemented for the health board and independent contractors meets all the requirements of the Data Protection Act, including Caldicott and IT Security legislation.

16. Responsibility for providing general and specialist advice and support to clinicians and managers within the Lothian as required supporting NHS Lothian's commitment to clinical effectiveness and service redesign. Direct the attainment of key benefits in the National, Lothian and local strategies relating to the Clinical and Corporate systems used throughout NHS Lothian which are required to provide an integrated Digital and IT solution to meet the needs of the Healthcare Family. Influence the development of the Digital and IT strategies at local and national level, providing expertise on IT

Security and Information Governance standards.

17. Representing NHS Lothian on National and other groups where specialist advice and expertise is required and drafting national policy. As a member of the National Operational Group and the Public Benefit Privacy Panel for Scotland health and Social care, be involved in decision making regarding research and development relating to redesign, audits and service improvement regard information governance and the implementation of post research outcomes

7a. EQUIPMENT AND MACHINERY

Personal Computer, Personal Digital Assistant, Barcode scanner, digital projector and Printers: to access and use patient information systems, email, internet and MS Office products, on a daily basis for the majority of the day.

Telephone and pager – to communicate with internal and external contacts, on a daily basis.

Photocopier and Printers – for collation of personal work documents.

Recommend, specify procure and allocate of Project IM&T equipment such as PC's, printers, consumables, software servers, interfaces and application screens.

7b. SYSTEMS

Manage, design, develop, review, update and implement existing and new information systems across the Health Board and Operating Divisions, to meet user requirements in line with local business requirement and IM&T strategy.

Manage design, develop, review, update and implement and develop board information services for both IG and security systems implementation, delivering divisional and Health Board staff training, advise departments on related business processes, training system development, user system(s) testing, evaluating and trouble shooting. Including Health Board wide systems for systems for; Device end point management and data loss prevention, email and internet filtering/monitoring and antivirus.

In addition Daily use of office systems word excel outlook powerpoint.

8. ASSIGNMENT AND REVIEW OF WORK

Reporting to the Head of Operations and Infrastructure on work being undertaken but has organisational operational independence as the organisation's 'Accountable Data Protection Officer' as required by the General Data Protection Regulations (GDPR) to ensure the Health Board is legislatively compliant.

The Information Governance and Security Manager's activity will be autonomous, independent and also supporting and in response to the priorities developed from the information strategy through the Head of Operations and Infrastructure, Executive Medical Director (Caldicott Guardian) Executive Director of Public Health and Health Policy (SIRO), NHS Lothian Healthcare Governance and Clinical Risk management Group. The post holder's work will be autonomous guided by and interpreting national policy, acting with the authority of the Executive Medical Director and Executive Director of Public Health and Health Policy.

Review of performance in the post is undertaken through the agreement of performance objectives and individual performance appraisal by the Head of Operations and Infrastructure. Formal appraisal is undertaken on an annual cycle, but the Head of Operations and Infrastructure will undertake more frequent ongoing informal reviews of current development and progress.

In specialist areas the post holder has operational independence working autonomously, developing leading, initiating, interpreting and implementing local and national policy and legal guidelines on behalf of NHS Lothian, which impact the organisation.

9. DECISIONS AND JUDGEMENTS

As Subject matter expert for the organisation, the post holders decision making processes will be mainly based on statue, common law and legal guidance. The post holder will be expected to shape legislation, regulation, policy and strategy.

Interpretation, development, implementation and adjustment of organisational policies, plans and strategy in relation to IG training/ e-learning, information systems projects and confidentiality programmes across the organisation, taking into account the changing services needs and conflicting demands, in addition to interpreting emerging legislative and Scottish Executive developments and policies. Also advising and helping lead strategy in NHS Lothian and associated external agencies on joint areas of work.

Expert providing specialist advice on highly complex situations, recommendations and initiate development of policy, based on analysis and interpretation of Data Protection, Scottish Executive guidance, law, confidentiality issues and associated risks, for patient and staff information on behalf of the Health Board Including disclosure and information sharing matters in new areas with external agencies where there may be conflict of opinions or no precedent. Liaising with peers and colleagues to ensure consistency, seeking legal advice as appropriate. Advise and resolve problems for the Caldicott Guardian in this area, and act as an expert witness if required in relation to conduct/breach of policy.

Expert analysing highly complex qualitative and quantitative data where necessary in relation to analysis of individual level data and IG and security investigations**.**

The Information Governance and Security Manager is required to take decisions and give advice to others on a wide range of issues on a daily basis. The Information Governance and Security Manager is required to exercise judgment and has operational independence to act and is held accountable for decisions made.

10. MOST CHALLENGING/DIFFICULT PARTS OF THE JOB

Lead and manage of Information Governance and Security support within an NHS environment, i.e. coping with demands of an integrated NHS Organisation, limited resources, coordinating and managing input from external suppliers and multidisciplinary project groups, managing satisfactory development of key systems and governance standards for patient care and NHS Lothian business.

Negotiating compromise between agencies based on the law, persuading, consulting upon or informing of agreed standards and process change required at all levels of the organisation, where there may be resistance to change.

Responding to the clinical and managerial information service needs associated with the developing priorities of the Health Board and ensuring that security, confidentiality, integrity or performance are not compromised.

Being part of an organisation realising benefits from the application of IM&T in a rapidly changing environment and leading on Information Governance and Security compliance at all times.

11. COMMUNICATIONS AND RELATIONSHIPS

Internal:

The post holder is responsible for communicating information governance and security policy and guidance throughout the organisation.

Meetings and formal presentations on highly complex IM&T topics to large groups including; Clinical groups and forums, Directorates, Department Management and their staff on; security, confidentiality, information issues, training, support and fault resolution, specifications, negotiating compromise and gaining agreement between service and user departments on information system developments and associated business process changes, and planning and agreement of implementation and service schedules.

Executive Medical Director, Executive Director of Public Health and health Policy, Medical director and Director of Digital and IT on Strategic issues. Project Managers, Service Delivery and Corporate Information Managers for Project development, implementation and handover.

Auditors regarding the data protection, information sharing, IT security associated with NHS Lothian information systems.

Presentations to Directors and Senior Management teams, Project Boards, national and international colleagues to advise or introduce draft and new policy, and action plans for agreement.

Caldicott Guardian (Executive Medical Director) and Senior Information Risk Owner SIRO) (Executive Director of Public Health and Health Policy) to provide specialist advice on security, confidentiality and information sharing matters.

Digital and IT staff to lead, assist and advise on best practice for training and development matters.

External:

NHS managed agencies on contractual negotiations, NSS on National Contracts, Service Level Agreements and data definitions.

IT suppliers on negotiations for; operational requirements, specifications, suitability, cost, contract issues, hardware/software training, functionality issues, systems and applications upgrades and potential acceptance. Management Consultants on information systems projects.

Represent NHS Lothian and the Director of Public Health and Health Policy nationally and internationally on various information groups and multi agency groups, to advise, develop and consult on strategy, policy system matters and governance matters.

Directly with patients as a noted point of contact on information leaflets for advice on Data Protection Act, subject access and confidentiality matters.

Information Commissioner, Office of the Information Commissioner in Scotland, Central Legal Office, Scottish and UK Caldicott Guardians Forum and Council.

Other Key Relationships

Medical Director.
Director of Nursing.
Director of Digital and IT.
Head of Digital and IT Infrastructure and Operations.
Director of Public Health and Health Policy Senior Information Managers.
Clinical Directors and Executive Team.
Clinicians.
Heads of Department.
General Managers/Assistant General Managers.
Clinical Nurse Managers.
Strategic Suppliers/ Partners.
Counterparts in other NHS locations.
Scottish Government, particularly CMO office.
Information and Statistics Division (ISD).
Social Care and Associated Voluntary organisations.
Police Scotland.

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

Physical: Use of keyboard on a daily basis, to prepare documentation.
Required to analyse complex data at speed when investigating urgent/critical information governance or security incidents, ensuring accuracy, preservation of evidence, and the preparation of timely reports, briefings and presentations to limit the consequences of information governance breaches on behalf of NHS Lothian requiring the postholder to check in other systems/data sources and at speed collate data to show what they report and what they show to ensure the update is a valid reflection of a serious situation. This will involve flipping between multiple systems and manipulating and comparing data between those systems.

Move and transport presentation equipment to training and other venue (laptop, projector).

Mental: Intense concentration/ in depth mental attention frequently required e.g leading meetings, influencing NHS staff and managers at all levels of seniority, public speaking, provide timely and accurate workload/project statistical analysis and compilation of reports for service evaluation, planning and project management Pressure to manage service performance, provide timely and accurate workload/project statistical analysis and compilation of reports for service evaluation and action planning. React to Health Board and divisional managers, staff and external agency interruptions with queries and short notice requests for immediate assistance, requiring reprioritising of workload on a daily basis.

Emotional: Providing support to staff members on personal issues. Dealing with conflict situations. Dealing regularly with challenging problems, for example the resolution of longstanding patient complaints requires emotional resilience, and deal with performance/disciplinary matters.

Environmental: Use of VDU computer equipment for more than half of working day, on a daily basis.

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

Degree or equivalent in an Information/security related discipline.

Qualification to Masters level or evidence of equivalent expertise gained through work experience, including;

Highly developed specialist expertise in Information Governance and Security disciplines.

Significant senior experience in a large and complex organisation.

Experience and evidence of advanced professional training qualification or equivalent (e.g. British computer society Information systems Examination Board Certificate in Data Protection).

Expert working knowledge, qualification or equivalent of Data Protection Act (2018), and knowledge of related confidentiality legislation preferably within the NHS.

Experience or equivalent evidence of advanced professional information security qualification or equivalent.

Senior IM&T management knowledge, experience and skills will include a broad and highly developed specialist expertise of information systems governance and security developments, organisational change, organisational development and staff/financial management.

Must have ability to scrutinise systems understand business processes and how systems support these whilst maintaining IG standards throughout.

Experience in strategic staff management and leadership.

Managerial knowledge, experience and competencies including staff management, customer focus, commercial awareness, planning, strategic and analytical thinking excellent negotiation skills.

Experience and expertise of managing multiple objectives within a large scale organisation including the management of financial and staff matters.

14. JOB DESCRIPTION AGREEMENT

Job Holder’s Signature:	Date:
Head of Department Signature:	Date:

GENERIC JOB DESCRIPTION

1. JOB IDENTIFICATION

Job Title:	NHS Lothian – Information Security Project Manager R&D
Responsible to:	IT Security Manager
Department(s):	Digital & IT
Operating Division:	NHS Lothian Corporate Services
Job Reference:	LN-EHEALTH-PM
No of Job Holders:	1
Last Update :	org chart update May 2025

2. JOB PURPOSE

To manage one or more IM&T project(s). The post-holder has overall responsibility and accountability for the financial, operational, people management and customer relationship aspects of project(s). These projects themselves are often conceptualised and initiated by or in consultation with the post-holder, and address highly complex and often sensitive information processing problems.

As a senior member of the departmental management team, the post-holder manages the conceptualisation, development, implementation and maintenance of projects, processes and applications that are aligned to and support wider organisational strategy. The post is highly collaborative in nature and involves communication and negotiation with technical and non-technical experts and managers internally and externally. As such, the post-holder must have highly specialised knowledge in either IT or business related areas, with knowledge that will have been accumulated over several years and/ supported by formal qualifications, training and experience.

The post-holder will provide leadership, advice, support and guidance to multi-disciplinary teams and all other stakeholders.

3. DIMENSIONS

Finance

Project budget £150,000

Staff - Direct

Management of the allocated project team to deliver project.

Staff – Indirect

Up to 2 contractors

Projects / activities

Multiple projects with one being large and complex.

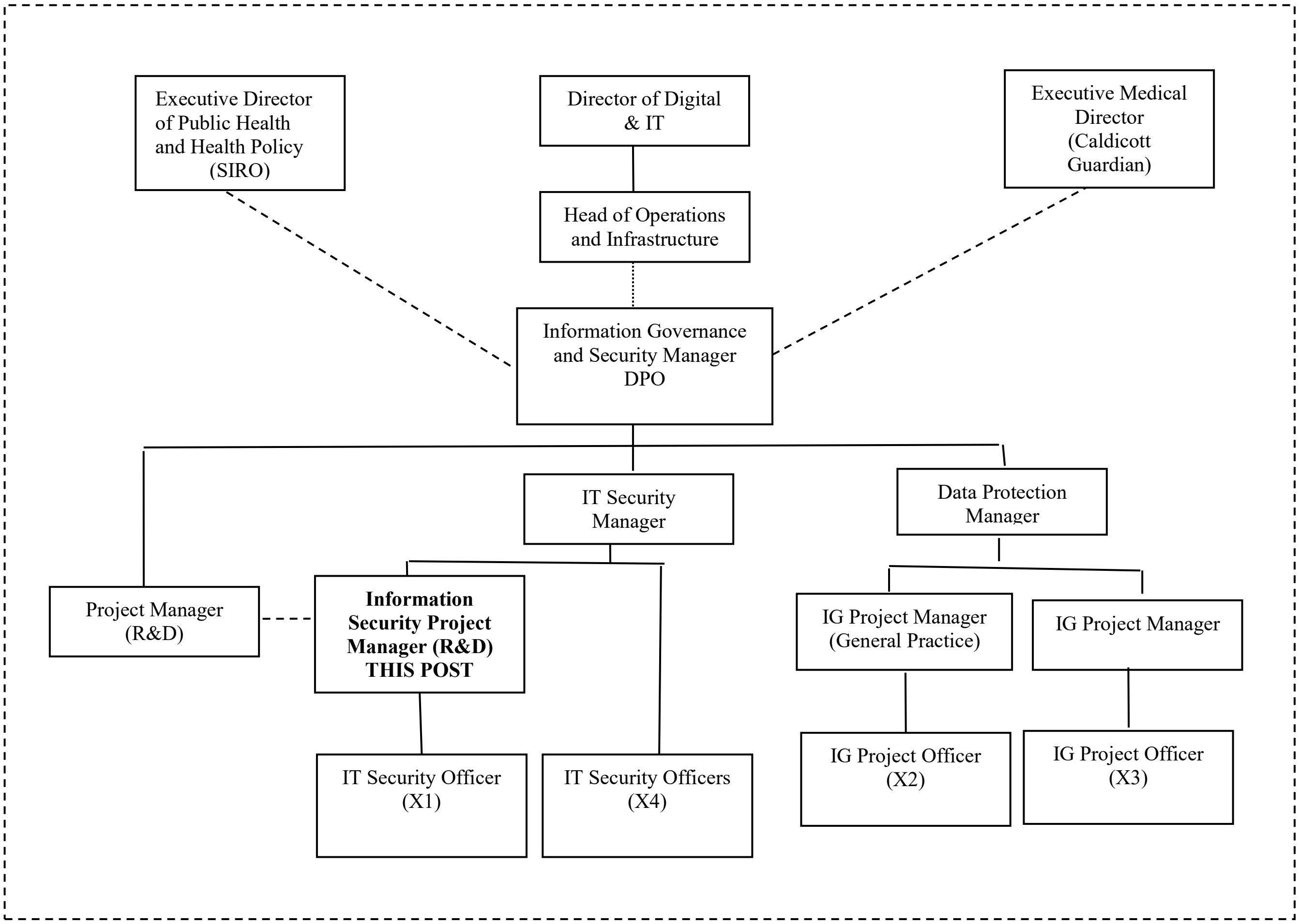
Multiple Activities within the project.

End-users / clients affected by projects / activities

Users: 20,000 +

Sites covered: NHS Lothian and Local Authority sites.

4. ORGANISATIONAL POSITION


Executive Director of Public Health and Health Policy (SIRO)
Director of Digital & IT
Executive Medical Director (Caldicott Guardian)
Head of Operations and Infrastructure
Information Governance and Security Manager DPO
IT Security Manager
Data Protection Manager
Project Manager (R&D)
Information Security Project Manager (R&D) THIS POST
IG Project Manager (General Practice)
IG Project Manager
IT Security Officer (X1)
IT Security Officers (X4)
IG Project Officer (X2)
IG Project Officer (X3)

5. ROLE OF DEPARTMENT

Digital & IT services brings together information and knowledge management, corporate information, health records, system administration and development, infrastructure support services, security, data protection, training, health informatics, programmes and projects within NHS Lothian.

This seeks to assist NHS Lothian staff to exploit the use of Information Management and Technology to enhance clinical and business services within the organisation. This work is governed within the strategic plan for Digital & IT services for NHS Lothian. This ensures local and national programmes and targets are addressed across the many aspects of NHS service delivery, and that there is coordinated and co-operative working in Digital & IT matters across Lothian.

6. KEY RESULT AREAS

Project Management

1. The jobholder will be responsible for project managing, using PRINCE 2, and implementing the projects throughout NHS Lothian. Initially scoping the project and progressing it through to having the project implemented within the defined scope.
2. Development and monitoring of project plans and ensuring the project delivery is on time, within budget and to specification.
3. Identify the priorities for the project and communicate these effectively to the Project Board.
4. Ensure the project is in line with local and national strategies including the requirements to meet with national standards.
5. The jobholder will be responsible for the management of issues and risks and ensuring remedial action is taken. Ensure escalation process is in place for complex issues and risks.

Processes

1. Identification and analysis of business processes and rules to improve the overall implementation and utilisation of systems. These will be developed in collaboration with the business areas.
2. Produce documentation on the analysis and recommendations to the business areas. Present these to the project stakeholders and users to promote ownership of the system.
3. Develop processes for the interfacing of IM&T systems where required.

Communication

1. Develop effective working relationships between all staff involved in supporting and implementing the IM&T project.
2. Establish and co-ordinate a core Project Team.
3. Develop a communications plan to link with all project stakeholders.
4. Attend events and liaise with all involved authorities as indicated by the IM&T project.
5. Communicate effectively with the project team and all areas that will be impacted by the implementation of the project(s)
6. Where necessary negotiate with stakeholders and 3rd party suppliers ensuring developments and deliverables meet with requirements and timescales.

Financial Accountability and Reporting

1. Manage the Project Budget to ensure cost effectiveness.
2. Monitor, review and evaluate the project, to ensure outcomes are achieved on time and within budget, taking action as required.
3. Using the agreed performance indicators and reporting structures provide regular reports to NHS Lothian on implementation progress.

Any other duties associated with the project will be agreed between the post holder and their Line Manager.

7a. EQUIPMENT AND MACHINERY

Using a personal computer (PC), photocopier, scanner, fax, mobile phone and personal data assistant (PDA) in order to carry out day-to-day job.

7b. SYSTEMS

- Microsoft Outlook – writing, reading and managing email communications to and from colleagues, staff, customers and external bodies.
- Microsoft Office – day-to-day usage for production of documents, presentations and general project administration.
- Microsoft Project – development and monitoring of project plans (simple and complex)
- Microsoft Visio – writing and maintaining process diagrams, organisational charts, system diagrams and other diagrams for use in project reports and training material
- Manipulation of data from a number of systems such as Trak PAS; PIMS; iLAB, SCI, eAssess this list is not exhaustive.
- The post holder will come into contact with new applications and will have to develop knowledge on each of these for the lifetime of the project.

8. ASSIGNMENT AND REVIEW OF WORK

1. The post-holder will have primary responsibility for the management of the project within the agreed work plan and will require to initiate and lead key areas of work, monitor progress, and respond flexibly to any developments and needs that arise during the course of the project.
2. The post-holder will lead the Project Team and be a member of the Project Board.
3. The Project Manager's work will be regularly reviewed with their line manager, and shaped by both National and Local priorities.
5. Personal objectives are agreed and reviewed on a quarterly basis with their Line manager.

9. DECISIONS AND JUDGEMENTS

The post holder is assigned projects by the IT Security Manager and is expected to manage these independently. This includes securing appropriate resources, project planning, anticipating and managing problems and ensuring timescales are met.

The Project Manager will have autonomy to take decisions. It is within their remit to develop proposals for the project(s) they are involved in but will seek authorisation from the Project Board when required.

Is guided by national policy but will need to establish the way in which it should be interpreted.
The jobholder has the authority to manage project issues and risks and, where appropriate, escalate these to the IT Security Manager.

10. MOST CHALLENGING/DIFFICULT PARTS OF THE JOB

Planning and organising a number of complex activities and ensuring that designated projects are completed and implemented within defined timescales and budgets, while satisfying ongoing user requests.

Receiving complex information from stakeholders, colleagues and external sources regarding all aspects of the allocated project(s).

Interpreting complex facts, comparing a range of options and proposing solutions to management.

Analysing complex information and ensuring that it is presented in an appropriate manner to allow decisions to be made effectively.

Managing issues and risks within the projects assigned to him/her and informing the strategic management of the Project Board by analysing and recommending risk solutions.

Negotiating and liaising with the different multi disciplinary teams, departments and agencies to access data systems and bring them on board. To utilise and obtain the identified benefits from the implementation of the designated project(s).

Facilitating cultural shift from technology led information to information focussed system implementation.

Working within an environment with active political agenda and ensuring all viewpoints are catered for

11. COMMUNICATIONS AND RELATIONSHIPS

- Communicates technical, analytical, and project management issues which can be highly complex and multi-stranded and may require persuasion or reassurance in order to overcome barriers to understanding to gain co-operation or agreement.
- Liaise with staff in other NHS organisations and agencies regarding the development and implementation of the project(s).
- Liaise, negotiate and communicate effectively with external suppliers.

Who	**How Often**	**How**
IT Security Manager	Ad-hoc Formally	Face-to-Face Telephone Written reports Meetings
Project Team	Daily	Face-to-Face Meetings Written Reports

Departmental Heads;
Service Managers;
Clinicians
	Ad-hoc	As above

All level of Users	Daily	As above
All level of Staff with Digital & IT	Daily	As above

Suppliers	Ad-hoc	Telephone; E-mail Meetings
Stakeholders Project Board	Formally Monthly	Meetings

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

Physical Effort

- Working for long periods on PC.
- Extensive keyboard skills.

Mental Effort

- Long periods of analysing data and producing information on that analysis ie patient matching rules.
- Reviewing of data on a number of IT systems throughout the NHS Lothian organisation.
- Explaining complex information to differing levels of staff.

Emotional Effort

- Occasional dealing with staff and project issues.

Environmental

- In the main office based though will be out and about meeting with staff on all NHS Lothian sites.
- Travelling to all sites through own or public transport.

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

1. Graduate, IM&T or business-related degree or equivalent.
2. Formal management and professional qualifications desirable.
3. Experience of PRINCE2 project management methodology essential, PRINCE2 Practitioner level desirable.
4. 5+ years experience in IM&T or other relevant NHS business area (clinical and/or administrative)
5. 3+ years experience in project/staff management roles.
6. Proven ability to successfully and concurrently implement projects within set timescales and budgets.
7. Excellent communication, presentation and influencing skills.
8. Capable of developing and maintaining effective working relationships with senior stakeholders and with external service providers.

14. JOB DESCRIPTION AGREEMENT

A separate job description will need to be signed off by each post-holder to whom the job description applies. Job Holder’s Signature: Head of Department Signature:	 Date: Date:

JOB DESCRIPTION

1. JOB IDENTIFICATION

Job Title:	Information Governance Project Officer
Responsible to:	Data Protection Manager
Department(s):	Digital and IT
Directorate:	Corporate Services
Operating Division:	NHS Lothian
Job Reference:	LN-EHEALTH-PO1
Last Update:	org chart update May 2025

2. JOB PURPOSE

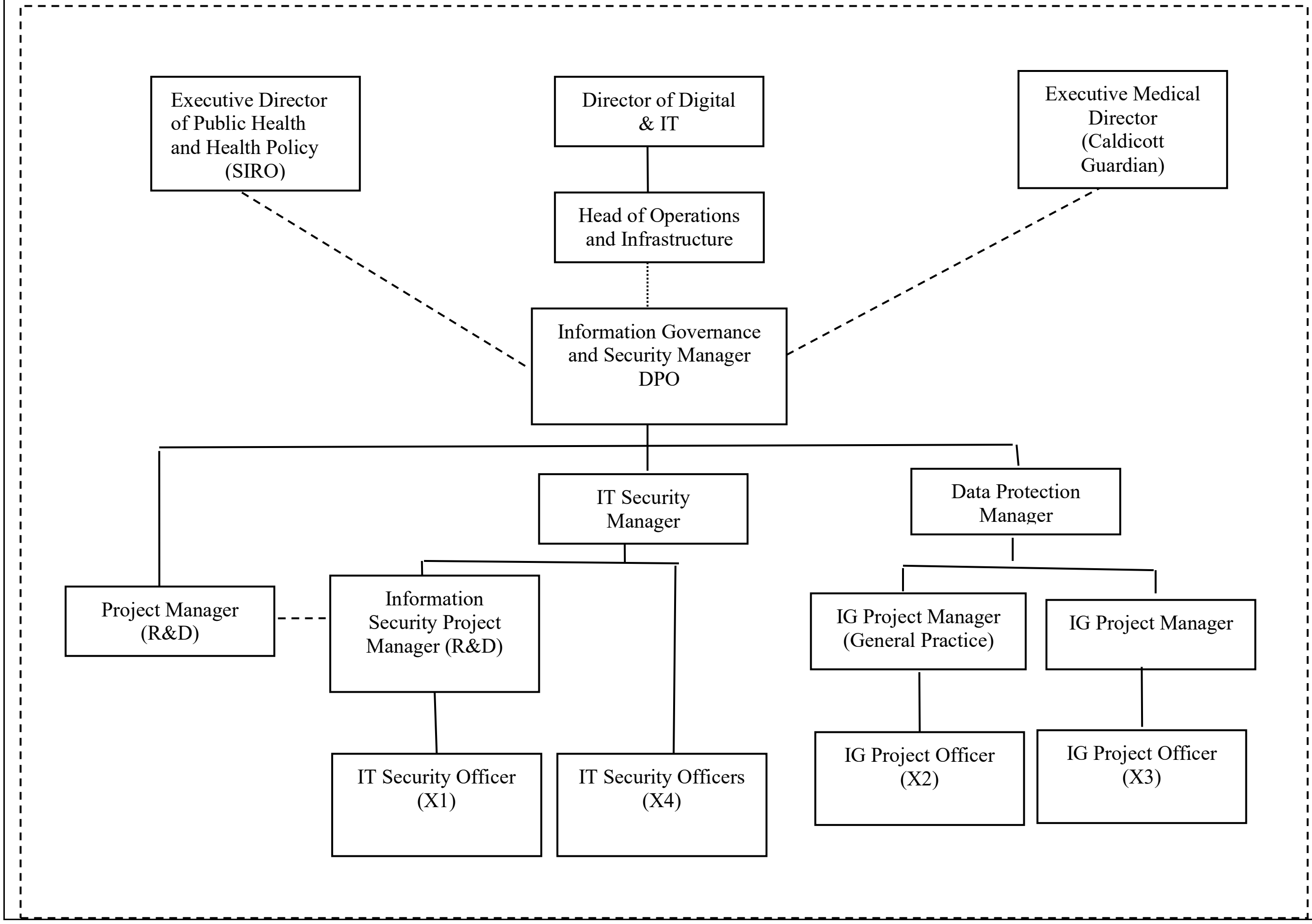
To assist and support the Data Protection Manager in all aspects of the project life cycle, project administration, and information management. Also involved in supporting operational handover to the Support teams as required during project phases.

To provide support and guidance to stakeholders and end-users involved in eHealth implementations of data protection legislation change and associated business process changes.

3. DIMENSIONS

Finance No budgetary responsibilities
Staff Team-based. No direct staff responsibilities. Indirect. Suppliers 3+
Users Up to 20000+ across NHS Lothian
Sites covered: All NHS Lothian and Local Authority sites.

4. ORGANISATIONAL POSITION


Executive Director of Public Health and Health Policy (SIRO)
Director of Digital & IT
Executive Medical Director (Caldicott Guardian)
Head of Operations and Infrastructure
Information Governance and Security Manager DPO
IT Security Manager
Data Protection Manager
Project Manager (R&D)
Information Security Project Manager (R&D)
IG Project Manager (General Practice)
IG Project Manager
IT Security Officer (X1)
IT Security Officers (X4)
IG Project Officer (X2)
IG Project Officer (X3)

5. ROLE OF DEPARTMENT

Digital services brings together information and knowledge management, corporate information, health records, system administration and development, infrastructure support services, security, data protection, training, health informatics, programmes and projects within NHS Lothian.

This seeks to assist NHS Lothian staff to exploit the use of Information Management and Technology to enhance clinical and business services within the organisation. This work is governed within the strategic plan for eHealth services for NHS Lothian. This ensures local and national programmes and targets are addressed across the many aspects of NHS service delivery, and that there is coordinated and co-operative working in eHealth matters across Lothian.

6. KEY RESULT AREAS

1. To define user requirements for allocated project work to ensure effective delivery and implementation of projects to agreed plans. To assist in drawing up specification as necessary, within the timescales determined by the Data Protection Manager and ensure all work is accurately and clearly documented and maintained during the project life cycle.
2. Provide specialist knowledge and guidance in eHealth projects, undertaking the review of systems, testing of developments and upgrades and documentation of information systems with guidance from the Data Protection Manager.
3. Evaluation and implementation of new technology, and or processes in support of assigned project work.
4. Ensuring technical and operational procedures are initiated, developed and implemented as part of the project life cycle and issues such as systems security and operational support are addressed as part of project hand over.
5. To liaise with third parties in relation to the development and support of systems implemented through assigned project work
6. To ensure System Administrators are skilled and have procedures and documentation to support handover of projects to a support environment.
7. Support the Data Protection Manager in all aspects of project delivery ensuring that formal project management principles and documentation are adopted at all times.
8. Producing documentation and reports in line with project timescales.
9. Adherence to help desk response times with regard to support tasks for assigned projects.
10. The post holder will identify proposed project milestones and timescales, as agreed with the Data Protection Manager for assigned project work.
11. The post holder will advise on technical and non-technical requirements and on the advantages of new technology/systems, as part of assigned projects, the post-holder is responsible for the selection of appropriate technology and planning development, analysis, implementation and evaluation.
12. Under the guidance of the Data Protection Manager the post holder will also give attention to data quality, management of change, operational support issues, end user requirements, reporting and respond to changing requirements during the implementation of project work.

7a. EQUIPMENT AND MACHINERY

Responsible for administering project work, testing and supporting a range of software during the project life cycle.

PCs and Peripherals for utilisation by the assigned projects.

Project Planning Tools including Microsoft Project and MS Office applications

Documentation and Report Presentation e.g. Microsoft Office Professional Software

Database System tools

- Microsoft SQL Server
- Microsoft Access
- ODBC connected interactive web based applications

- Business Objects to extract data from large database systems

General Office Equipment for presentation and administration tasks

7b. SYSTEMS

Systems used for administering project work
Structured storage for progress reports, computer programs and documentation

- Microsoft Project and Project intranet hosted websites / publishing tools

Communication systems used to manage project work and liaise with Support, Training and Users

- Ehealth service desk
- EMail – Outlook and NHS mail

Systems utilised within a project environment

- Scottish Care Information (SCI) Tools e.g. SCI Store, SCI Gateway
- Trak
- GP systems
- Information Asset Register

Database Systems supporting project work

- Microsoft SQL Database for data storage, programming environment, security
- Microsoft Access

8. ASSIGNMENT AND REVIEW OF WORK

Work is allocated and objectives set under line responsibility of the Data Protection Manager and will be reviewed via informal discussions and regular meetings.

The post holder will develop procedures prior to hand over as well as supporting operational documents e.g. Project Documentation, Plans and User procedures. These would be reviewed at a project board level.

The post holder's work will be mainly driven by Project requirements set out at the Informatics Management Group (IMG) and by the Information department managers.

The post holder will work with the Service delivery team and the Customer Services team ensuring that the project support and training requirements are met and delivered.

9. DECISIONS AND JUDGEMENTS

The post holder will:

- Take decisions on assigned projects, prioritising workload and undertaking project and support work, to agreed procedures and standards.
- Work with other eHealth specialists to agree on standards and methods to be used within the projects.
- Provide specialist advice and decisions on systems being implemented to a wide cross section of staff within the organisation
- Identify the most appropriate solutions for project development tasks in response to specifications and recognises the need for procedures, developing these as required and reviewing these with the Data Protection Manager and project teams.
- Provide support for escalated calls on assigned project work, provide advice and guidance to users and eHealth staff, and work with project and operational teams to deliver project work.

- Investigate and appraise options for resolution of problems, and arrange potential solutions during development or analysis of reported faults.

10. MOST CHALLENGING/DIFFICULT PARTS OF THE JOB

- Identifying and defining project related user requirements.
- Dealing with resistance to change both in terms of working practice and the project introduction/implementation of new information systems.
- Delivering projects on time, with access to limited resources.
- Identifying and scheduling of resource to assist in project delivery.
- Managing the organisational change associated with the introduction of new information systems

11. COMMUNICATIONS AND RELATIONSHIPS

Ensuring that the External Suppliers \ Contractors deliver on time, to budget and to agreed specification. Support and train lead users in the use of Divisional information systems delivered through project work, and ensuring that sufficient training and procedures are delivered to support the overall hand over from projects to the eHealth, Support and Training teams.

Provision of one-to-one training to new system users as projects progress, ensuring consistency of training delivery and the development of training materials. Also to ensure new users receive all required information-related mandatory training delivered through Divisional training services.

(a) Within own unit/division/department

Regular written and verbal communication with all information department staff, to receive allocated work, seek advice and assistance, and deliver summary of progress made at task level.

Communication with Information Training and Support services

(b) With other unit/division/departments

Regular liaison with end users of IM&T systems, including clinical, management and administrative staff for information collection, analysis, presentation and support, together with other IM&T issues.

Participation in Project Boards and Project Teams

(c) External to the Health Service

Regular contact with third party suppliers and user groups for information systems as defined within project work

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

Physical Effort

Continuous requirement for sitting at keyboard for a substantial amount of time e.g. for reviewing system deliveries, testing of systems, email; includes occasionally moving light equipment. Occasionally required to drive/travel to meetings and other areas of NHS Lothian.

Mental Effort

The postholder will have frequent periods of time where intense concentration is required for analysis, design, report writing, delivery of training to ehealth teams and stakeholders.

Development of presentations and delivery of these to users who maybe resistant to the proposed changes and or the project.

In response to a system failure or at early project implementation times, there will be occasions when frequent interruptions will occur, where timely reactions are required to find solutions.

Environmental Effort

The post requires extended periods of time working at VDUs. This is daily for more than half the shift.

Emotional Effort

Rare exposure to distressing circumstances.

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

Experience, Knowledge and Qualifications

Degree or equivalent plus in-depth knowledge of the project life cycle and 5 years relevant work experience, preferably in the NHS.

In-depth knowledge, qualification or relevant work experience of Data Protection Legislation.

Evidence of additional specialised project management and development qualification or equivalent experience to postgraduate level, including:

Technical project development and support skills
Excellent Communication skills - Both written and verbal
Understanding of the Project development life cycle, project management and rapid application development techniques (knowledge of Prince 2 project management techniques preferred)
Ability to understand and use Microsoft office, client, server and web enabled software
Presentation skills and effective documentation skills
Ability to clearly define and scope new proposed project
Ability to understand complicated business and information processes.
Demonstrate a sound understanding of project management techniques.
Encourage and motivate staff all levels in achieving agreed project implementation goals

Well developed interpersonal skills and ability to apply diplomatic and tactful approach to dealing with project issues.

14. JOB DESCRIPTION AGREEMENT

Job Holder’s Signature:	Date:
Head of Department Signature:	Date:

JOB DESCRIPTION

1. JOB IDENTIFICATION

Job Title: Information Security Officer

Responsible to : NHS Lothian Information Security Manager

Department(s): eHealth (IM & T)

Directorate: Corporate Support Services

Operating Division: NHS Lothian

Job Reference: LN-EHEALTH-SO

No of Job Holders: 5

Last Update :27 March 2007 (org chart update June 2024)

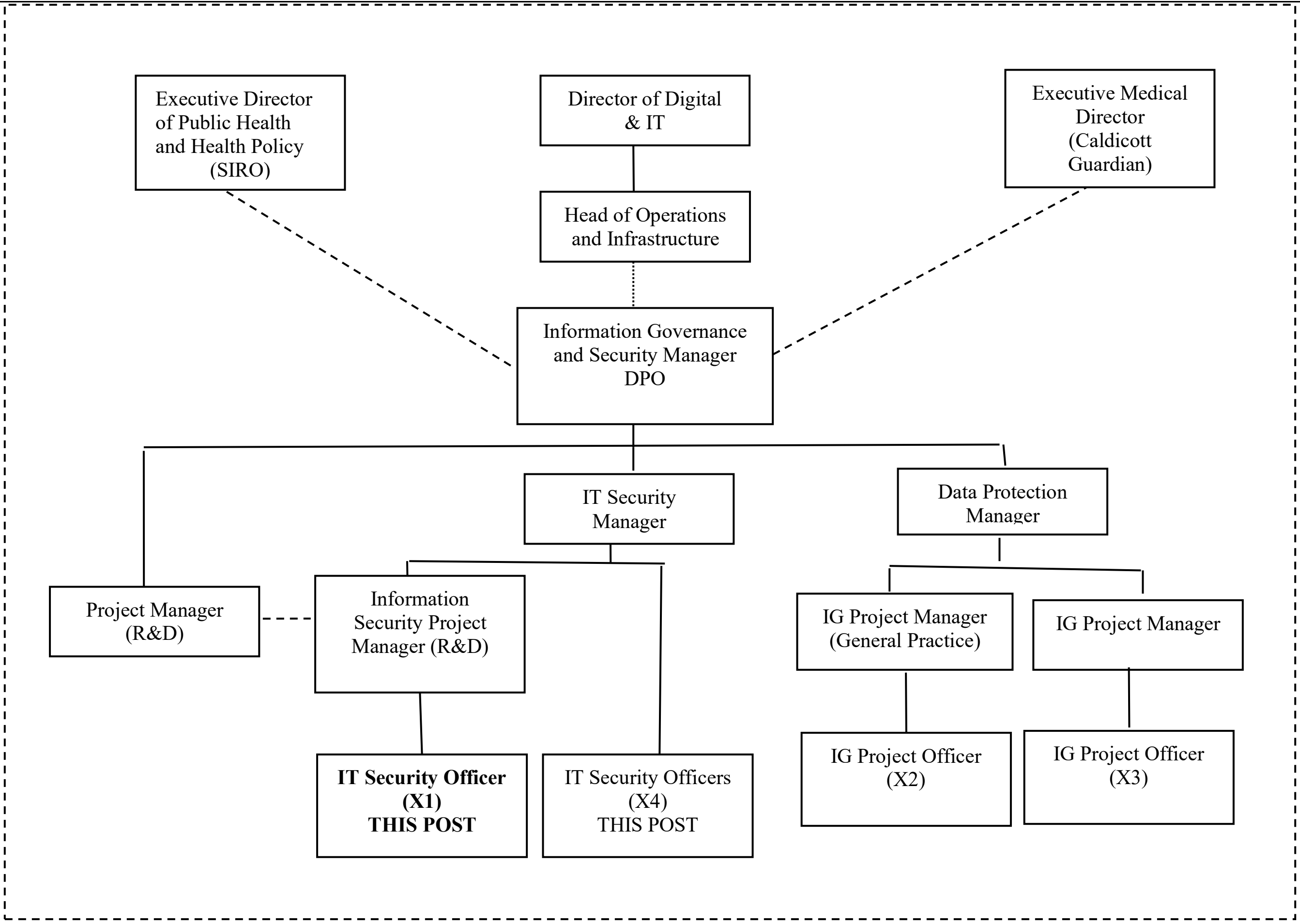
2. JOB PURPOSE

Fully participate in the IT Security Function in the delivery of a comprehensive IT Security support service to a large and diverse user base. Additionally to participate in the development and implementation of technical solutions to develop the IT Security function for all computing users throughout the Board, to maximise security and protection for its users, systems and information, enabling maximum realisation of benefits from its IT investment

3. DIMENSIONS

Finance	None
Staff	Suppliers : 3+
Projects/Workload	Up to 4 concurrent projects, of which 1 may be complex
Users	Up to 18,000 across NHS Lothian

4. ORGANISATIONAL POSITION


Executive Director of Public Health and Health Policy (SIRO)
Director of Digital & IT
Executive Medical Director (Caldicott Guardian)
Head of Operations and Infrastructure
Information Governance and Security Manager DPO
IT Security Manager
Data Protection Manager
Project Manager (R&D)
Information Security Project Manager (R&D)
IG Project Manager (General Practice)
IG Project Manager
IT Security Officer (X1) THIS POST
IT Security Officers (X4) THIS POST
IG Project Officer (X2)
IG Project Officer (X3)

5. ROLE OF DEPARTMENT

eHealth services brings together information and knowledge management, corporate information, health records, system administration and development, infrastructure support services, security, data protection, training, health informatics, programmes and projects within NHS Lothian.

This seeks to assist NHS Lothian staff to exploit the use of Information Management and Technology to enhance clinical and business services within the organisation. This work is governed within the strategic plan for eHealth services for NHS Lothian. This ensures local and national programmes and targets are addressed across the many aspects of NHS service delivery, and that there is coordinated and co-operative working in eHealth matters across Lothian.

6. KEY RESULT AREAS

Assist in the development and implementation of the overall information security strategy and architecture to be used by NHS Lothian.

Work with functional groups and staff in the creation of policies, procedures, and guidelines to ensure the security, privacy and confidentiality of information on NHS Lothian's computer systems.

Maintain currency of expertise in security-related technologies, trends, issues, and solutions.

Undertake routine monitoring and reporting of IT Security systems, logs etc to identify and deal with IT Security breaches

Assist in the creation and maintenance of Disaster recovery and business continuity plans

Investigate security needs, and recommend; plan, implement, test, and monitor information security improvements.

Provide instruction and training for users and other NHS Lothian employees on information security procedures and their application.

Participate as appropriate in the planning and implementation of security related projects.

Perform miscellaneous job-related duties as assigned.

To liaise other members of the NHS Lothian Information Security Team to ensure compliance with the needs of the wider organisation.

To liaise with Information Services department colleagues at all levels in the development and planning of projects, to ensure compliance with the organisations technical platform and plans.

7a. EQUIPMENT AND MACHINERY

PCs Telephone printers and Fax

Specialised software for the management and protection of Network and desk top devices

7b. SYSTEMS

All Desktop and Server applications.

Both Clinical and Non Clinical systems including:

Patient Administration Systems

Email services including Active Directory

Mail filtering system

Laboratory Information Systems

Intrusion Detection Systems

A number of specialist systems, which although not directly managed by eHealth require that policies are managed to comply with the Data Protection Act, security of information held.

8. ASSIGNMENT AND REVIEW OF WORK

The jobholder reports to, and objectives are set by the NHS Lothian Information Security Manager.

The jobholder works mainly under direction from the NHS Lothian IT Security Manager. Workload is generated by the Information services strategy, other departmental and managerial security requirements within the Division and breaches in IT security.

The NHS Lothian and ISSG Security officers will assist in the jobholder's development on an informal basis.

Work in progress is reviewed at weekly meetings with the NHS Lothian Information Security Manager.

9. DECISIONS AND JUDGEMENTS

The post holder will be expected to work on a daily basis with very little input from the line manager. The post holder will be expected to be able to deal with calls and requests and process them accordingly. The post holder will have to determine to what an extent a security breach is a risk to the Organisation and report on to management accordingly. The post holder will be expected to determine what is an acceptable exception to the IM&T Security Policy without causing adverse risks to the Organisation's systems and data.

11. MOST CHALLENGING/DIFFICULT PARTS OF THE JOB

- Ensuring that IT Security breaches are detected and resolved with minimum delay and maximum efficiency
- Ensuring compliance with the NHS Lothian IM&T Security Policy
- Dealing with breaches caused by senior medical staff.
- Ensuring that projects are completed on time and within budget.
- Communicating to medical staff the importance of adhering to the IM&T Security Policy and Confidentiality.

12. COMMUNICATIONS AND RELATIONSHIPS

Internal

Contact With	Frequency and Reason	Type of Contact
NHS Lothian Inf. Sec Mgr	ad-hoc;	face to face/phone
	weekly meetings	
	to discuss progress;	face to face
	monthly progress report	written
Computer users at all levels throughout the Division	ad-hoc, to provide advice, guidance and assistance	face to face/phone
IS colleagues at all levels	ad-hoc, to provide advice,	face to face/phone

External

Providers of computer software and hardware	ad-hoc, to keep up-to-date with market development,	face to face, phone, written to progress projects

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

- Ensuring that IT Security breaches are detected and resolved with minimum delay and maximum efficiency
- Ensuring compliance with the NHS Lothian IT Security Policy
- Ensuring that projects are completed on time and within budget.
- Possible exposure to inappropriate material during investigations

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

Degree with 2-5 years in IM&T.

2-5 years specialised knowledge in at least one of the following areas:

- Operating Systems;
- IT Security;
- Problem Management.

Minimum of 2-3 years experience of a mixed software environment with specialised knowledge in one of: -. Netware, MS Office, Windows, DOS, Unix, terminal emulation.

Excellent communication skills with all levels of technical and non-technical staff.

Proven ability to handle multiple tasks concurrently.

Proven ability to set and maintain technical standards.

Ability to work on own initiative but also work as a team member as required

15. 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: