Livingston James

Skills Development Scotland

POSITION PROFILE

# Head of Cyber Security

# Contents



# Welcome Note from Paul Clark, Chief Information Officer

Dear Applicant,

Thank you for considering this Head of Cyber Security role for Enterprise IS (EIS), a shared service organisation, hosted within Skills Development Scotland (SDS) that delivers shared IT services to ourselves, as well as our partners:

- Scottish Enterprise (SE)
- Highlands and Islands Enterprise (HIE)
- South of Scotland Enterprise (SoSE)

You will be joining EIS, part of SDS at a very exciting time as we expand our wider team to keep pace with a rapidly changing cyber environment and to meet the demands of our Partner's unified, and also individually, unique project portfolio requirements.

Heading up the Cyber Security Team you will lead on and define the cyber security strategy. You will have an amazing opportunity to work closely with our highly skilled staff and customers, contributing to the success of the cyber security program and retainment of the CE+ Accreditation held by all partners. EIS operates via several delivery teams including; PMO, Operations, Strategy Solutions and Architecture and Cyber Security, working independently and together combining their skill sets to deliver value for money and the best possible end goal to our customers.

SDS values its' people. We put our people first and they are firmly at the forefront of everything that we do.

In a recent survey SDS scored 9.3 out of 10 from our employees who say, "My actions are consistent with SDS Values". Respondents scored 8.6 in response to "I am proud to work for SDS" and "I want to stay working for SDS for at least the next 12 months". We also pride ourselves in listening to our staff and offer a flexible work environment to suit.

We hope that you are keen to find out more about this great opportunity, and we look forward to learning how you can help us grow and develop our Cyber Security strategy and shape your future career with us.

**Paul Clark**
**Chief Information Officer**

# Overview of Skills Development Scotland

Skills Development Scotland (SDS) is Scotland's national skills body and contributes to Scotland's sustainable economic growth by supporting people and businesses to develop and apply their skills.

With more than 1,600 colleagues working across the country with businesses, in schools, careers centres and partner locations, we are passionate about skills development and its contribution to a modern, innovative and prosperous Scottish economy.

Working with our partners, we strive to ensure employers have the right skills at the right time in high performing, fair and equal workplaces, and that every individual has the skills and confidence to get a job and progress in the workplace, achieving their full potential. Engaging with the skills system to help ensure it better meets those needs in the short, medium and longer term, SDS' core services and activities include:

- Careers Information Advice and Guidance Services - focused on equipping Scotland's current and future workforce with the career management skills they require to achieve their potential
- Apprenticeships – administering Scottish Apprenticeships on behalf of Scottish Government, SDS is committed to developing and growing a world-class work-based learning system in Scotland
- Skills Planning – robust skills intelligence enables SDS to understand the current and future demand for skills and jobs across Scotland, by geography and by industry sector
- Supporting Scotland's Employers – working directly with employers across Scotland, SDS provides trusted advice that helps employers invest in existing skills, develop new talent and get the right products to grow their business
- Research & Insight – producing and commissioning high quality research on a variety of topics relating to skills and employment, SDS looks to inform policy and practice

As an organisation SDS has four core values which underpin everything it does:

- We put the needs of our customers at the heart of all we do
- We demonstrate self-motivation, personal responsibility and respect
- We continually improve to achieve excellence
- We make use of our continued strengths and expertise to deliver the best outcomes

More information can be found at: [www.skillsdevelopmentscotland.co.uk](http://www.skillsdevelopmentscotland.co.uk)

# The Role

The primary purpose of the role is to lead and define the Cyber Security strategy and implementation of appropriate security controls across the partnership (SDS, SES, HIE, SOSE) Leading a highly specialist technical team to align the advancing technical tools/processes required to deliver security controls the postholder is responsible for the alignment and identification of security in line with business strategies through the effective delivery of Information Security services through the management and orchestration of people, products, providers and processes. The purpose of the role is to establish and maintain the information security program to ensure that information assets and associated technology, applications, systems, infrastructure and processes are adequately protected in the digital ecosystem in an ever-changing landscape which we operate.

## We aim to be an employer of choice

At SDS, we put customers at the heart of what we do. We'll make use of your strengths so you can deliver the best for our customers in a culture of fairness and everyday leadership.
We'll always help you to improve yourself with dedicated hours for professional development and the flexibility to maintain a healthy work-life balance.

## We're an inclusive place to work

At SDS we are ambitious about diversity and inclusion. If you've got the right skills for the job, we want to hear from you. We encourage applications from the right candidates regardless of age, disability, race, sex, gender identity, sexual orientation, pregnancy and maternity, religion or belief. We have an LGBTI+ Allies network Group which is open to all colleagues to help drive LGBTI+ inclusion.

# The Role

Enterprise Information Services is part of Enabling Services Directorate at SDS and is responsible for the provision of ICT services internally and to partner organisations, Scottish Enterprise, Highlands and Islands Enterprise and South of Scotland Enterprise. The service supports approximately 3500 users throughout these bodies, delivering business applications and desktop computing services over an extensive communications network that includes international sites. A number of systems support front-line activities and also client engagements as well as core back-office functions. All four bodies have an increasing business dependency on these systems and information technology generally.

All partners to the Shared Service arrangements are Non-Departmental Public Bodies accountable to Scottish Government, as such the performance, governance and value for money for the EIS service is key.

This role reports to the Chief Information Officer (CIO) and is accountable for all cyber security activity not only related to confidentiality, integrity and availability, but also to the safety, privacy and recovery of information owned or processed by the business in compliance with regulatory requirements. They will also be responsible and accountable for all cyber security and risk management activities related to people, process and technology, to ensure the achievement of business outcomes.

## Responsibilities:

- As well as having budgetary responsibility, this post holder will be responsible for defining and implementation of the Security Maintenance and Support budget (circa £150k annually), as well as the large multi-workstream Security Programme across all shared service partner organisations (circa £500k annually – excluding resource cost)
- They will have Senior Management responsibility for a multi-disciplined, highly skilled Cyber Assurance and Security Operations team. This will ensure development and delivery of appropriate alignment of security processes and technology, along with security architectural toolsets as part of the Cyber Security programme
- The post holder will have accountability for delivery of the overarching Cyber and lower-level Cyber domains strategies, with indirect responsibility for the Security Architects within EIS Strategy, Solutions and Architect team to ensure alignment to these strategies
- Responsible for providing Security assurance at the EIS Technical design Authority for all changes to shared services as well as 3rd Party delivered solutions that feed into shared services
- Support Corporate Risk and Regulatory process, along with internal audit processes to ensure alignment to SDS Corporate Risk. This will ensure alignment to Scottish Government Cyber Resilience Framework and enforcement of security controls to ensure continual attainment of Cyber Essential+ certification
- They will be accountable for the delivery of shared a service information security governance structure through the implementation of a governance program, which includes Chair responsibilities of the EIS Security Council

**Internal:**

- Audit & Risk Committee – to provide updates and information on cyber resilience and risk in line with the legal, regulatory, and contractual obligations

- Senior Directors/Extended Leadership Group (ELG) members – represent EIS at partnership boards and forums, such as the EIS Shared Services Board, Partnership Service Assurance Boards, SDS Software Governance Forum, HIE ISFGG etc to inform on cyber resilience and risk in line with the legal, regulatory, and contractual obligations along with cyber strategy and progress on the Security Programme
- Head of EIS Strategy Solution Architecture (SSA) - to build alignment between the security and enterprise architectures, thus ensuring that cyber security requirements are implicit in these architectures and security is built in by design
- EIS IT Director – to build alignment with security assurance and security operations with operational support thus ensuring that cyber security operations are supportive or delivery of overall service to partners
- Chief Information Officer – to ensure that security is aligned to overarching partnership business strategy
- Data Protection Officers for all partner organisations – to proactively and reactively manage all aspects of cyber security to ensure that data privacy requirements are included where applicable
- Legal/Human Resources - Provide input for the IT section of the company's code of conduct

**External**

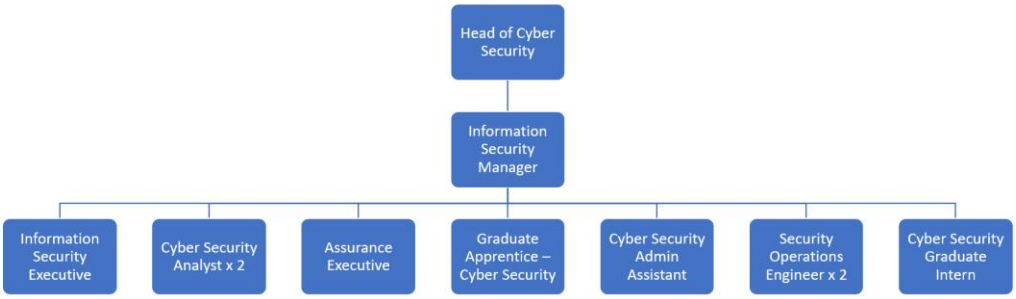
- Shared Service Partners – to lead the delivery of security services covering the non-EIS managed applications and platforms
- Audit – to participate in and be accountable for the outputs of any audit involved cyber security
- Scottish Government – to participate in and take direction from wider Scottish Government security initiatives and programmes and ensure that Partner Cyber Strategy is aligned to Scottish Government Cyber Strategy
- Senior Executives in Supplier Partners under the Multi-supplier outsource approach (Capita, Barrier Networks, Ensono, Leidos, Microsoft, SWAN) – Responsible for lead the delivery of security managed services provided by these suppliers
- External Senior Cyber Security Peer groups to ensure collaboration and information sharing as appropriate
- External authorities - Occasional contact with external authorities (Police, ICO, NCSC) may also be required in response to security incidents
- Development and delivery of a cyber security vision and strategy that is aligned to organisational priorities and enables and facilitates the organisation's business objectives
- Develop, implement, and monitor a strategic, complex, multi-workstream cyber security program to ensure appropriate levels of confidentiality, integrity, availability, safety, privacy, and recovery of information assets owned, controlled, or/and processed by the organisation.

- Provides strategic leadership for:
  - The implementation of security service improvements and innovations that encompass cloud, DevSecOps, infrastructure, O365 and deskside services

  - Provides direction on what emerging technologies should be assimilated, integrated and introduced into security tool stack to ensure that appropriate security controls are implemented in line with the enterprise's business strategy
  - Reviewing and analysing the external threat environment for emerging threats and advise relevant stakeholders on the appropriate courses of action
- Provide leadership in all aspect of cyber security across the shared service to deliver consistent and high-quality cyber security management in support of the business strategy and organisational environment
- Anticipate and proactively protect the company from data breaches, security incidents, imminent and new threats, and ensure the company meets and sustains its compliance requirements
- Design and lead the cyber security operating model in consultation with stakeholders and align with the organisational risk management approach and compliance monitoring
- Manage the budget for the cyber security programme, monitoring and reporting discrepancies
- Define a metrics and reporting framework to measure the quality, efficiency and effectiveness of the security programme, and increase the maturity of cyber security, and review it with stakeholders at the executive and board levels across all partner organisations
- Ownership of the development and implementation of security incident response plans and procedures to ensure that business-critical services are recovered in the event of a security event
- Provide (all three) leadership and direction for cyber security incidents and events to protect corporate IT assets, intellectual property, regulated data and the company's reputation
- Accountable for the security performance and improvements to create a culture of embedding security into all aspects of the working environment
- Acts as a trusted adviser, to build, maintain and influence relationships with other security leaders and key business stakeholders to develop a clear understanding of business needs

Skills Development Scotland

**Cyber Security Department**



## Knowledge, Skills and Experience:

**Essential**

- Educated to SCQF level 11 or educated to a Master's Degree in a relevant discipline (Cyber Security, ICT or Business) or considerable relevant work experience
- Significant experience of working at senior leadership level within a Cyber Security role
- Experience of development and delivery of both overarching and low-level Cyber strategies within a within a Cyber Security Architect or Lead Technical Security role
- Industry recognised Professional Cyber Security qualification such as Certified Information Security Manager (CISM) or equivalent
- Experience of development and delivery of large-scale complex security programme's
- Working knowledge of implementation of information security management frameworks, such as ISO/IEC 27001, ITIL, COBIT, NIST, including 800-53 and Cybersecurity Framework
- Proven track record and experience in developing cyber security policies and procedures,
- Previous experience of dealing at a senior level with customers and suppliers
- Proven track record in managing budgets or financial information/data
- Expert knowledge of cyber security and cyber security technologies
- Excellent stakeholder engagement management skills
- Excellent problems solving and analytical skills
- Excellent communication skills with the ability to deliver key messages with credibility
- Strong influencing skills, persuades others; build consensus through give and take; gains cooperation from others to obtain information and accomplish goals
- Excellent people management skills to motivate, coach and engage teams to deliver high performance in a challenging and dynamic environment
- Experience of leading and managing the implementation of major change initiatives
- Excellent judgement, tactical awareness and decision-making skills

## Personal Attributes

- Strategic thinker with ability to view the bigger picture and build credible strategies to achieve desired vision and long-term outcomes
- Drives strategic priorities within their team which address a diverse range of customer needs & enables achievement of organisational goals
- Quickly cuts through complexities to identify central issues and critical relationships
- Customer focused; appreciating the different challenges that various stakeholders have and endeavouring to delivery operational and transformational improvements
- Prepared to take personal accountability
- Self-motivated
- Role models senior leadership behaviours and treats others with dignity and respect

# Preferred Candidate Profile

- People focussed; coaching, engaging and motivating managers and teams to deliver a high performance
- Commercially focussed, delivering creative solutions to organisational issues that deliver value for EIS & Partnership
- Demonstrates resilience; manages personal effectiveness by managing emotions in the face of setbacks or when dealing with provocative situations

## Benefits of joining us

Alongside an excellent salary, we are proud to offer a wide range of benefits. You will receive competitive pay, generous holiday entitlement, and a number of ways to work flexibly. Our full benefits package includes:

- 30 days annual leave
- 13 days public holiday
- Flexi-time scheme
- The ability to use 'work from anywhere' technology at manager's discretion and subject to business requirement
- Excellent professional development support
- Local Government Pension Scheme - career average revalued earnings scheme with an employer contribution rate of 22.3%. More information can be found at www.spfo.org.uk
- Work and family policy - flexible working options for parents and carers
- Partnership arrangements with two recognised Trade Unions
- Employee Assistance Programme - free, confidential, and impartial advice and support

## The Recruitment Process

The recruitment for this position is being managed by our advising consultants, Livingston James.

Interested candidates should provide a tailored CV to Ali Shaw, alishaw@livingstonjames.com