Hamilton Forth

Midlothian

Client:	Midlothian Council	**Job Title:**	Cyber Security Analyst
Location:	Dalkeith / remote	**Job Category:**	Information Technology
Level/Salary Range:	£35000 - £39,500 per annum	**Travel Required:**	None
HF Contact:	Josh Moreland	**Position Type:**	Permanent
URL:	https://www.ljg-jobs.com/midlothian-council/	**Date posted:**	April 2022
Applications Accepted By:	Ongoing		
Phone or E-mail:	Josh Moreland joshmoreland@hamiltonforth.com 07741 261 151		
Job Description			

About the client:

Midlothian Council is Scotland's fastest growing Local Authority - serving a growing population of over 90,000. Situated just ten miles south of Edinburgh, Midlothian boasts some of the finest green spaces in Scotland including the Pentlands Regional Park. We provide a hugely diverse range of services to our citizens including schools, social care, planning waste and recycling services, libraries, and dozens more.

The council is the largest employer in the with roles for over 4,000 people. We recognise that our most valuable assets are our people and we strive to be an employer of choice by providing a range of benefits to recruit and retain the best people. You can learn more about Midlothian Council by visiting our website visit and watching our video where our young people tell you all about it.

Background to the role:

Amongst the 4000 staff at Midlothian Council includes a host of talented digital and technical change professionals. It is within this area that the Cyber Security Analyst will sit. The successful candidate will be joining the Council at a hugely exciting time as we embark on a wide scale transformation supported by our new Digital Strategy.

Hamilton Forth

Midlothian

Pivotal to delivering our ambitions is a Digital Service that underpins this work, both now and in the future. Not only will you be supporting the development of new cyber defences, but you will also be helping create a more resilient organisation that can quickly respond to the evolving cyber security threats. You can make a real difference to the people who live and work here, collaborating with them and working in a dynamic and flexible environment.

We are looking for a security professional with a collaborative, innovative approach, a high level of drive and commitment, excellent interpersonal skills, a great track record of delivering and securing digital services in other organisations, and experience of successfully managing and improving upon a wide range of security systems and processes.

Role description:

Responsibilities:

- Oversight of the setup, configuration and support of critical IT cyber **defence systems and controls.**
- **Monitoring, investigating and reporting** of security events and making proactive changes in response.
- **Writing, reviewing and updating** Council policies and procedures.
- To provide **competent advice, guidance and support** cyber security technical controls for Midlothian Council.
- To **collaborate** with partner organisations on a range of complex and sensitive security issues.
- Support security **incident response** teams, problems, changes and releases relating to Council systems.
- Leading and co-ordinating **business continuity** activities to ensure Midlothian Council systems are resilient and can recover quickly from any losses or failures.
- To provide support to the Information Governance and Security Lead to investigate any cybersecurity and business continuity **incidents** and advise managers on service improvements, appropriate action and mitigation.
- Consult on system requirements and **configuration** with senior technical colleagues and service managers, responding to and **solving faults or problems**, taking into account security factors internal and external to Midlothian Council.
- Evaluating Information asset and supply chain **risk** and controlling those exposures, taking a pragmatic, risk-based approach to balancing security requirements with business needs.
- Support business managers and service users understand **risk** and advise them on best practice security and information governance measures applicable to their business environment ensuring appropriate Cyber Security consideration is made when executing implementation and transition of delivery programme's into BAU.
- Undertake technical and security **audits** of in-house and hosted third party applications and systems to ensure that their security and integrity is fit for purpose.

- Regularly undertaking **research** into new security products fixes and techniques, evaluating their effectiveness and applicability to Midlothian Council, pursuing innovative ideas and making recommendations on new security technologies.
- Supporting the information Governance and Security Lead and other service managers to ensure operational **compliance** with relevant legislation, regulation and security standards such as ISO27001,

Hamilton Forth

Midlothian

Cyber Essentials Plus, PSN, PCI DSS and GDPR, ensuring effective policies, procedures and controls are in place throughout the Council.

- To develop and deliver security **training and awareness** content to Council staff.

Required skills & experience:

- 3-5 years+ experience in the arena of Digital Security, Cyber, Information Governance & Compliance and / or relevant other field
- Proven track record in dealing with multiple technical and non-technical business stakeholders
- A good understanding of security legislation and governance standards (as detailed above)
- Ability to work on projects as well as BAU activities
- Excellent documentation skills for policies and procedure report creation
- Excellent communication skills and 'can do' problem solving attitude

Qualifications and Education Requirements

It may be advantageous to possess a background in Cyber Security (at degree level) or to have completed CISO, CISSP or relevant other industry accreditation – however, this is not a mandatory pre-requisite.

There is no 'essential' industry experience which candidates should possess – however, anyone who has worked in local government, public sector bodies, tertiary education, charities or quangos may be looked upon favourably.

Interview format:

- Stage 1 – discussion with Information Security Manager (via VC)
- Stage 2 – in depth video interview with ISM and other technical leads
- Stage 3 – HR onboarding discussion

Represented by:	Hamilton Forth	Date:	April 2022