# Role profile

* **Job title**: Lead Infrastructure Engineer (Security)
* **Grade:** 10
* **Business area:** Digital Services - ICT
* **Reporting line:** Delivery Manager (Technology)
* **Team:** Technology Team

## Job Purpose

Lead day-to-day operation of GMCA’s cyber security team to secure and protect the organisation’s data, systems and network.

Contribute to the design of solutions and services with embedded security controls specifically engineered to respond to and mitigate security threats.

Identify and analyse threat intelligence from various sources, mitigate and monitor incidents that could adversely affect the confidentiality, integrity, and availability of GMCA’s information assets and infrastructure.

Mange and deliver an incident response, intrusion detection, security testing and vulnerability management capability.

|  |  |
| --- | --- |
|  |  |

## Key working relationships

* Delivery Manger (Technology)
* Associate Infrastructure Engineer (Security)
* Security Architect
* Head of Digital Solutions
* Infrastructure Engineers
* Digital Services Team Leaders
* Digital Services Service Operations Team
* Suppliers
* Customers/users within GMCA

## Key Responsibilities

* Lead and manage a small team of security focused infrastructure engineers, providing guidance and direction to team members.
* Providing technical and operational support and guidance on cyber security matters to Digital Services and the wider organisation.
* Establishing and maintaining an appropriate cyber security posture across the technical infrastructure, including patching, application deployment and operating system hardening.
* Providing advice on potential and current threats to the organisation’s cyber security posture, with appropriate mitigations and coordinating the specific response to the threat, working closely with risk owners and the risk process.
* Collaborating with cross-functional teams to identify potential security risks and threats and implement measures to prevent them.
* Monitoring the overall effectiveness of the organisation’s cyber security controls through the definition and reporting of key metrics and measures, presenting reports on security incidents and trends to senior stakeholders.
* Coordinating and contributing to the production of specific cyber security policy and procedures.
* Creating, quality assuring and maintaining security related documentation including technical procedures to be issued to other Infrastructure Engineers as part of ‘Business As Usual’ activities.

Identify, prioritize, and remediate vulnerabilities based on risk and threat assessments, while establishing and maintaining a comprehensive Vulnerability Management function that ensures continuous monitoring, reporting, and mitigation of security risks.

* Proactively configuring and monitoring security alerts to identify areas of concern and areas.
* Responding to and owning security alerts from multiple sources based on SLA and risk.
* Monitoring and analysing security breaches and leading incident response efforts to mitigate the risk and impact in a timely manner.
* Liaising with suppliers, contractors, service providers, regulators, and other external agencies to support activities relating to the organisation’s cyber security posture.
* Supporting knowledge transfer between internal teams to deliver stable, available, and secure operational IT services.
* Contributing to small, medium, and large IT security projects and providing support to other projects and teams from an IT security perspective.

Assist in testing of Disaster Recovery/Business Continuity procedures.

Coordinate penetration testing, remediate findings, and report progress to ensure the security posture is continuously improved.

**General**

* Build effective relationships with clients, customers, key stakeholders and specialist suppliers (e.g. third parties undertaking annual IT Health Check activities).
* Where required, coach system users to develop effective skills, and provide guidance and support on the use of systems and tools to enable them to undertake their roles.
* Provide positive challenge to colleagues across the organisation in considering how things can be done better and more effectively.
* Communicate effectively to ensure all relevant stakeholders are informed and up to date with relevant information, statuses, and progress.
* Proactively contribute to continuous improvement of systems and processes to ensure procedures, policies and guidance are updated in line with legislative and social changes.
* Review key performance indicators to identify and address issues arising, spot trends and take appropriate action to learn, share and improve.
* To always hold yourself and others to a high standard of professionalism, demonstrating your commitment to our values and behaviours as well as ensuring service confidentiality is maintained throughout all we do.
* Working with other teams internally and externally collaboration is maximised and supporting on activity where appropriate.
* Ensure the services delivered internally and externally are inclusive and accessible.
* To align work area to the Sustainability Strategy and ensure work practices are inclusive of this value and strategic intent.

**NB: This list of duties and responsibilities is by no means exhaustive, and the post holder may be required to undertake other relevant and appropriate duties as required.**

## Knowledge, Skills, and Experience

**Knowledge and Experience**

* Educated to degree level in a relevant subject or significant demonstrable experience.
* Considerable experience of working in a cyber security or equivalent role.
* Knowledge of common cyber threats, vulnerabilities, and attack vectors, as well as techniques for preventing, detecting, and mitigating cyber-attacks.
* Knowledge of IT security best practice principles such as Zero Trust, Assume Breach, JIT/JEA.
* Strong knowledge of network protocols, firewalls, and secure network architecture.
* Strong knowledge of authentication, authorisation, and access control methods, as well as best practices for managing user access to systems and data.
* Familiarity with encryption algorithms, key management, and secure data transmission and storage.
* Ability to assess and manage security risks, including conducting risk assessments, developing security policies, and implementing security controls.
* Knowledge of monitoring and detection tools.
* Knowledge of forensic tools, techniques, and methods.
* Good understanding of security frameworks and best practice.
* A thorough understanding of:
	+ Microsoft Active Directory
	+ Microsoft Group Policy
	+ Microsoft Defender Suite
	+ Microsoft SCCM
	+ MDM (e.g. Microsoft Intune or similar)
	+ SIEM tools (e.g. Microsoft Sentinel or similar)
	+ Remote Access solutions (e.g. Microsoft Bastion or similar)
	+ Microsoft Windows Update for Business
	+ Third party patch management tools
	+ Vulnerability scanning tools (e.g. Tenable/Nessus or similar)

**Desirable**

* Experience with Microsoft Purview, compliance centre, DLP.
* Experience with automation / scripting (e.g PowerShell, Bash, Python, etc.).
* Certification such as CompTIA Security+, Certified Information Systems Security Professional (CISSP), or Certified Information Security Manager (CISM), Microsoft Security, Compliance, and Identity Fundamentals.
* Experience of working with security frameworks (e.g. ISO/IEC 27001, PCI DSS, Cyber Essentials, etc.) and incident management best practice (e.g. NIST, NCSC, etc.).
* ITIL® 4 Foundation Certificate in IT Service Management.
* Experience working in an ITIL aligned environment.

**Skills, Values and Behaviours**

* Well-developed verbal and written communication skills.
* Ability to convey often complex information and guidance in a clear and understandable manner appropriate to the recipient.
* Ability to build strong and trusting relationships with clients, customers, and colleagues.
* Self-motivated with an ability to prioritise and organise work effectively to meet deadlines.
* Ability to collate, critically appraise and reference information from a range of sources using excellent analytical skills.
* Ability to generate new ideas, alternative options and develop realistic and practical solutions.
* Excellent relationship management skills with demonstrated ability to develop effective relationships with key stakeholders and colleagues.
* Clear focus on delivering positive outcomes.
* Acting as a role model for the directorate.
* Able to work flexibly and independently, covering other areas of the department as required.

## Corporate Duties

*Do not behave in way which discriminates against your fellow employees, or potential employees on the grounds of their sex, sexual orientation, marital status, race, religion, creed, colour, nationality, ethnic origin or disability.*

*Safeguard at all times confidentiality of information relating to staff and pensioners. Refrain from smoking in any areas of Service premises.*

*Behave in a manner that ensures the security of property and resources. Abide by all relevant Service Policies and Procedures.*

***Records Management / Data Protection*** *- As an employee of the GMCA, you have a legal responsibility for all records (including employee health, financial, personal and administrative) that you gather or use as part of your work with the Service. The records may be paper, electronic, audio or videotapes. You must consult your manager if you have any doubt as to the correct management of the records with which you work.*

***Confidentiality and Information Security*** *- As a GMCA employee you are required to uphold the confidentiality of all records held by the GMCA, whether employee records or GMCA information. This duty lasts indefinitely and will continue after you leave the GMCA employment. All employees must maintain confidentiality and abide by the Data Protection Act.*

***Data Quality*** *- All staff are personally responsible for the quality of data entered by themselves, or on their behalf, on GMCAs computerised systems or manual records (paper records) and must ensure that such data is entered accurately and, in a timely manner, to ensure high standards of data quality in accordance with Departmental protocols. To ensure data is handled in a secure manner protecting the confidentiality of any personal data held in meeting the requirements of the Data Protection Act.*

***Health and Safety*** *- All employees of GMCA have a statutory duty of care for their own personal safety and that of others who may be affected by their acts or omissions. Employees are required to co-operate with management to enable GMCA to meet its own legal duties and to report any circumstances that may compromise the health, safety and welfare of those affected by the Service’s undertakings.*

***Service Policies*** *- All GMCA employees must observe and adhere to the provisions outlined in these policies.*

***Equal Opportunities*** *- GMCA provides a range of services and employment opportunities for a diverse population. As a GMCA employee you are expected to treat all employees / partners / members of the public and work colleagues with dignity and respect irrespective of their background.*