**Role:** Information Security Manager
**Area:** Business Services
**Sub-Area:** Data Competency Centre
**Location:** Cork/Dublin
**Salary:** Competitive

**Duration:** Permanent **Ref:** GNI012

Gas Networks Ireland operates and maintains Ireland's €3bn, 14,725km national gas network, which is considered one of the safest and most modern renewables-ready gas networks in the world.

Almost 725,000 Irish homes and businesses trust Ireland's gas network to provide efficient and reliable energy to meet their heating, cooking, manufacturing and transport needs.

The gas network is the cornerstone of Ireland's energy system, securely supplying more than 30% of Ireland's total energy and over 40% of the country's electricity generation.

Gas Networks Ireland is aiming to deliver a repurposed, resized and fully decarbonised gas network by 2045. Its "Pathway to a Net Zero Carbon Network" envisions transforming the existing gas network into two separate systems carrying 100% renewable gas, one dedicated to biomethane and the other to green hydrogen, with the potential to carry approximately 30% biomethane and 70% green hydrogen, as well as offering significant long term energy export opportunities.

Gas Networks is an organisation with a very strong legacy and a culture founded on pride in our purpose, to keep Irelands energy moving, and commitment to our vision, to be at the heart of Irelands energy future. Our organisational values demonstrate what is important across the organisation including building on our experience across our organisation to build towards our sustainable future, doing what's right for each other and for the people and communities that we serve and finally energised for the change of our future towards a renewable energy landscape. Throughout your career in Gas Networks Ireland, you will be part of an organisation that has a strong commitment to supporting and developing our workforce today and into the future. You will also have an opportunity to get involved in our ambitious iBelong programme ensuring a diverse, equitable and inclusive environment for us all to thrive. Finally, our Time to Talk Mental Health programme and our wellbeing initiatives ensure we provide support across many areas as you work in our organisation.

## The Role

The Data Competency Centre (DCC) delivers centralised oversight of activities which manage, measure and improve GNI's data. The DCC advise on the governance, design and management of data and monitor resulting data quality. Within the DCC, GNI data management policies and procedures are created, data architecture is managed, information security matters are overseen, and business intelligence and data analytics initiatives are prioritised and delivered in line with enterprise-wide needs.

The Information Security Manager within the Data Competency Centre (DCC) will be responsible for managing, leading and developing the Information Security function, ensuring the delivery of robust, compliant, and forward-looking information security services across Gas Networks Ireland. Reporting directly to the Head of Data, this role will oversee all Information Security activities, including NIS compliance, annual NIS maturity assessments, and competent authority engagements (including managing audits for NI and ROI competent authorities. The role will also be responsible for information security incident management, organisation wide cyber awareness activity including regular phishing simulations and annual staff/executive/board training, overseeing our third-party risk management managed service and associated risks, managing our data loss prevention managed service, solution, and ambitions, and supporting the business in ensuring our procurement and project activity is delivered with information security in mind, all the while managing and developing a high-performing team.

**Duties and Responsibilities:**

- **Strategic Leadership & Governance**
  - Manage and lead the Information Security team, developing and implementing strategies to ensure compliance with NIS (Network and Information Systems) regulations and other relevant standards in both Republic of Ireland and Northern Ireland
  - Shape, plan and drive the annual “Secure Our Data” information security programme initiatives and other key GNI information security initiatives to progress the overall Gas Networks Data strategy.
  - Represent Information Security in enterprise-wide steering and governance forums, providing subject matter expertise and ensuring alignment with organisational priorities.
- **Team Leadership & Development**
  - Directly manage the Information Security Lead and NIS Compliance Analysts, fostering a culture of information security excellence, ownership, and continuous improvement.
  - Provide strategic direction, coaching, and mentorship to team members, ensuring professional development and succession planning.
  - Drive the embedding of the transferred Data Loss Prevention service, and the new Third Party Risk Assessment service across the team, and avoid any single points of reliance.
- **Regulatory Compliance, Measurement, and Engagement**
  - Manage the relationship between GNI and the relevant cyber competent authorities in ROI (CRU/NCSC) and NI (DoF NIS Compliance Team) through regular formal planned and adhoc engagements.
  - Plan, oversee, and ensure the timely delivery of annual NIS cyber self-assessments, and annual maturity reporting to the Executive and Board for both ROI and NI.
  - Keep abreast of a changing regulatory, standards, and frameworks-based cyber environment in the Republic of Ireland and Northern Ireland and align GNI plans and approaches to measuring compliance in each jurisdiction across IT/OT/and ET environments (e.g. pivot from NIS1 to NIS2, NIST1.1 to NIST2.0 and the implementation of CyberFundamentals in Ireland).
  - Procure, plan, deliver independent audits on behalf of the relevant NIS competent authority for the purpose of mandatory independent compliance assurance.
  - Track and assure closure of all identified audit actions, regularly report on same to internal stakeholders and relevant competent authorities, while maintaining a state of audit readiness at all times for possible ad hoc audits.
- **Operational Excellence & Information Security Service Delivery**
  - Manage the Information Security annual capital expenditure and operational costs for project/initiative delivery and service support.
  - Oversee the delivery of key operational Information Security services, including information security incident management and information security service request

management, monitoring performance of ticketing queues and adherence to strict SLAs. Establish and maintain effective processes for incident management, investigations, and follow-up.
    - Integral member of the GNI Cyber Security Incident Response Team, ensuring up to date playbooks for Information Security incident scenarios which are continuously improved with lessons learned after each incident is addressed or post CSIRT dress-rehearsals.
    - Custodian of GNI information security awareness culture and improving same through the assurance of employee and contractor on-boarding awareness training, planning the delivery of, and curating the relevant content of annual mandatory training for all staff, for the Executive team, for the Board, and for High Profile/Risk teams.
    - Improving employee awareness through delivery of regular sophisticated Phishing Simulations, and managing the technical platform for same, delivery of frequent topical information security tips and tricks, and delivery of annual Cyber Security Awareness activities each October.
    - Ensure robust governance of external file sharing solutions and meta-data to drive improved data security.
    - Ownership of the Data Loss Prevention (DLP) service, the supporting technical solution, ensuring managed service partner performance, the monitoring and follow up of regular alerts with end users, and the enhancement and refinement of our DLP ruleset.
    - Ownership of the Third Party Risk Assessment service, ensuring managed service partner performance, annual coverage of identified vendors, the monitoring and follow up of risks identified with RCMs, and quarterly updates to the Audit and Risk Committee.
    - Operational owner of all Information Security Policies, Procedures, and Standards with annual refresh and continuous improvement of same conducted in collaboration with the Head of Data.
- **Procurement, Project & Change Support**
    - Act as a senior business SME for information security aspects of all enterprise projects, with a gatekeeper role at key project phases and gates to ensure the confidentiality, integrity, and availability of GNI data.
    - Ensuring the Information Security team is involved in the scoring of all PQQ/ITT procurement responses and that new vendors and services are introduced with security best practices evidenced.
- **Risk & Performance Management**
    - Proactively manage information security risks and issues, providing timely insights and updates to the Head of Data for functional risk governance, and assure the oversight of all TPRA risks.
    - Balance team capacity with business demand, ensuring delivery to agreed SLAs and performance targets.
- **Stakeholder Engagement**
    - Build and maintain strong relationships across GNI pillars to support strategic security initiatives and cross-functional alignment.
    - Influence and negotiate effectively at all levels to drive adoption of best security practices and continuous improvement.
- Perform other duties as required from time to time.

**Knowledge, Skills and Experience:**

---

- Degree or equivalent in Information Security, Information Systems, IT, or a related field (or equivalent work experience) with 10+ years' experience in a technical discipline, ideally in a regulated or utility environment.

- Deep understanding of information security frameworks, NIS/NIS2 compliance, CAF compliance, maturity assessment methodologies and expanding regulatory requirements in ROI and NI.
- Demonstrated ability to assess, mitigate, and manage information security incidents, risks and complex compliance issues at an enterprise level, and incorporating lessons learned for future incident management/issues.
- Experience in leading security audits, from procurement, to on-site and field execution, draft finding review and agreement, audit report closure, and audit action closure planning, tracking, and reporting.
- Experience in managing annual capital expenditure and operational expenditure budgets effectively, and ensuring maximum value from market partners.

- Experience of Microsoft Purview DLP capabilities, as well as Microsoft Defender for creating and tracking phishing simulations a distinct advantage.
- An innovative mindset to delivering organisation solutions to maximise service offering in constrained resourcing environments.
- Extensive experience in building and maintaining collaborative relationships (both internal and external) with excellent influencing and negotiation skills at all levels in the organisation.
- Proven track record in leading multi-located (resource augmented) teams, through coaching and development while empowering staff through delegation of decision making and accountability.
- You will be a strong advocate for change and constantly seeking out opportunities to create efficiencies and improvements.
- Strong commercial focus while managing operating and capital budgets in line with regulatory allowances.
- Driver of high standards for individual, team and organisational accomplishment and delivering desired results.

**Applications, including current Curriculum Vitae, should be emailed to the following address stating the job title and reference number in the subject line of your email:**
**recruit@gasnetworks.ie**

The closing date for receipt of applications for this vacancy is the 7th January 2026.

**Please note that applications submitted after this closing date will not be accepted.**
***Gas Networks Ireland is an equal opportunities employer***

***We are committed to providing a diverse and inclusive place of work and have a robust strategy and framework called ibelong to enable this. We are an equal opportunity employer and through our recruitment process we welcome and encourage applications from interested and suitably qualified individuals regardless of gender, age, racial or ethnic origin, membership of the traveller community, religion or beliefs, family or civil status, sexual orientation/gender identity or disability.***

*GNI will only hold your data for as long as necessary. By providing a CV to GNI you are agreeing for GNI to process this information about you. If you have any question about how GNI processes your data please see our Privacy Notice. If you have further questions, you can contact us at DataProtection@gasnetworks.ie*