Comhairle Contae
Dhún na nGall
Donegal County Council

Information Systems

Project Leader – Cyber Security

(Grade VII)

Information for Candidates

January 2025

1. The Position

Donegal County Council is seeking applications from suitably qualified candidates with relevant experience for the position of Information Systems (IS) Project Leader – Cyber Security.

It is proposed to form a panel of qualified candidates from which any vacancies, permanent or temporary which arise will be filled during the lifetime of the panel.

The successful candidate will report to the Council's Head of Information Systems or other appropriate person as determined by the Council from time to time.

2. Role, Duties & Responsibilities

Donegal County Council is a large rural Local Authority with an extensive ICT infrastructure serving in excess of 100 locations countywide and 1200 employees. The Information Systems Department manages this network, one of the largest Local Authority networks in Ireland, as well as delivering a corporate information systems programme designed to support Council internal work-programmes and customer services initiatives.

The I.S. Project Leader Cyber-Security will support the Head of Information Systems in the development and management of the organisation's Information Communications Technology (ICT) and Information Systems (IS) Cyber Security strategies. The role will need to align the Council with the National Cyber Security Baseline Standards and European Directives (NIS2)

The I.S. Project Leader Cyber-Security will manage the security portfolio and related systems in the Council. The successful candidate will be part of the ICT Management Team and will constantly develop, implement, test, support and review the organisation's information networks, systems and infrastructure to make sure that the information systems are confidential, intact, and accessible.

Information Systems Project Leaders are responsible for the management and delivery of the Councils ICT services throughout the Council across multiple disciplines. This is a leadership role in the advancement of ICT services and policies including the development of business cases to support the implementation of new infrastructure or systems through engagement with internal stakeholders and third-party suppliers. The ideal candidate should be highly motivated with a commitment to delivering ICT services to the highest standard and to deliver strategic change for the benefit of Donegal County Council.

The duties will include but will not be limited to the following:

- Developing, implementing and communicating security policies, protocols & procedures: This involves creating comprehensive sets of controls,

including policies, processes, and measures, to protect systems and data from threats.

- Managing the ICT Cyber-security team: Overseeing staff involved in information security. Supervise, manage and mentor ICT staff, including Training & Development needs.
- Securing network and digital assets: Oversee the continuous monitoring and protection of all ICT systems. Evaluate suspected security breaches and recommend corrective actions. Collecting and analysing digital threat intelligence
- Developing risk management assessments: Identify potential threats and create plans to prevent and mitigate problems.
- Conducting regular system tests: Lead internal and external audits to ensure the effectiveness of security measures.
- Staying up-to-date with the latest security systems, standards, authentication protocols, and products: Continue to learn about new threats and technologies to protect the company's digital assets effectively. Develop practices to ensure the full ICT Team are kept abreast of new technological developments, and to provide in-house training when required. Supervise and participate in the Performance Management Development System.
- Responding to all security breaches: In the event of a security breach, have a plan in place to minimize damage and downtime, including communicating with the team and any external stakeholders.
- Ensuring compliance with the changing laws and applicable regulations: Understand the legal implications of security and ensure the council is always compliant.
- Training: Develop a Cyber Security Training programme for Staff and Stakeholders. Staying up-to-date with the latest security systems, standards, authentication protocols, and products: They should continuously learn about new threats and technologies to protect the company's digital assets effectively. Continue to develop ICT skills as technology changes.
- Manage the analysis, specification and deployment of Corporate Applications and upgrades to an agreed methodology to achieve successful outcomes.
- Actively review, improve and manage ICT security initiatives.
- Provide insights into technical issues related to security, risk assessment, and threat mitigation. Additionally, assisting in the development of long-term, strategic plans for ICT requirements within the Council should include robust cybersecurity measures to safeguard sensitive data and ensure the integrity of systems.
- Responsible and accountable for changes affecting the ICT infrastructure, ensuring such changes take place in a controlled and auditable manner.

- Responsible and accountable for the integrity of the Council's electronically held information and provide input into the Business Continuity planning.
- Provide leadership on emerging technologies and best practice.
- Reporting and Communication**:** Regularly report to the Head of Information Systems about the status of the information security program, incidents, and potential security risks.
- Assist the Head of Information Systems in developing long-term, strategic plans, for the development of ICT capabilities within the Council.
- Establish and manage service level agreements for contracted services and suppliers.
- Provide Technical assistance and guidance in GDPR and Data Protection.
- Contribute to the development and review of ICT policies.
- Input into the ICT department budgeting and service delivery planning processes.
- Design, implementation and support of a Disaster Recovery environment and knowledge of technologies such as backups, replication, de-duplication, recovery and restores.
- Procurement and award of high value contracts for ICT hardware and systems.
- Other duties as may be assigned from time to time.

3. Qualifications & Requirement of the Post

The post of Information Systems Project Leader – Cyber Security is analogous to the grade of Information Systems Project Leader. The Minister for Housing, Planning, Community and Local Government has declared that the qualifications for the position of IS Project Leader shall be as set out hereunder.

a) Character

Candidates shall be of good character.

b) Health

Candidates shall be in a state of health such as would indicate a reasonable prospect of ability to render regular and efficient service.
Successful candidates will be required to undergo a medical examination carried out by the Council's Occupational Health Doctor prior to appointment.

c) Education, Training, Experience etc.

Candidates must have on the latest date for receipt of completed applications:

(i) A qualification at Level 8 on the National Framework of Qualifications (NFQ) major award (i.e. honours degree), in a relevant computing discipline ***and*** at least 4 years directly relevant, recent ICT hands-on experience from your employment to date*

OR

(ii) A qualification at Level 8 on the National Framework of Qualifications (NFQ) major award (i.e. honours degree), or higher, with computing taken in the final year ***and*** at least 5 years directly relevant, recent ICT hands-on experience from your employment to date*

OR

(iii) A qualification at Level 7 on the National Framework of Qualifications (NFQ) major award (i.e. ordinary degree), in a relevant computing discipline **and** at least 5 years directly relevant recent ICT hands-on experience from your employment to date*

OR

(iv) A Level 6 NFQ major award qualification in a relevant computing discipline and at least 6 years directly relevant recent ICT hands-on experience from your employment to date*

AND

(v) Have a satisfactory knowledge of public service organisation or the ability to acquire such knowledge.

**Relevant ICT hands-on experience should include, but is not limited to: areas such as managing delivery of digital solutions, enterprise architecture, software and applications development projects involving a range of technologies and platforms covering web development, data management, database administration, business analysis/discovery, business intelligence and data analytics, DevOps, enterprise architecture, technical infrastructure, service design and delivery, server and client operating systems and architecture stacks, telecommunications and networking infrastructure delivery support, technical support, ICT service Management, operations and server support, ICT/Cyber security, mobile device management, virtualisation delivery support, database and application support, cloud computing, etc.*

d) Desirable requirements

The following are desirable but not limited to:

- **Vulnerability Assessment and Penetration Testing (Pen Testing)**: Professionals should be adept at identifying vulnerabilities and simulating real-world attacks. Conducting penetration tests helps uncover weaknesses in systems, networks, and applications.
- **Security Incident Response**: Practical experience in handling security incidents is essential. This involves detecting, analysing, and mitigating breaches promptly. Familiarity with incident response frameworks and tools is valuable.
- **Secure Coding Practices**: Developers must understand secure coding principles. Writing code that is resilient to common vulnerabilities (such as SQL injection, cross-site scripting, and buffer overflows) is critical. Knowledge of secure coding languages and libraries is beneficial.
- **Network Security:** Professionals should be well-versed in securing networks. This includes configuring firewalls, implementing intrusion detection/prevention systems (IDPS), and understanding network protocols (TCP/IP, DNS, DHCP).
- **Identity and Access Management (IAM)**: Experience with IAM solutions (e.g., Active Directory, LDAP, Single Sign-On) is crucial. Managing user access, authentication, and authorization falls within this domain.
- **Encryption and Cryptography**: Practical knowledge of encryption algorithms, digital certificates, and secure communication protocols (such as TLS/SSL) is essential. Protecting data at rest and in transit is a key responsibility.
- **Security Tools and Technologies**: Hands-on experience with security tools like SIEM (Security Information and Event Management), antivirus software, intrusion detection systems (IDS), and vulnerability scanners is valuable.
- **Web Application Security**: Professionals should be familiar with securing web applications. Understanding common web vulnerabilities (such as Cross-Site Scripting, Cross-Site Request Forgery, and SQL injection) and implementing security controls are essential.
- **Cloud Security**: As organizations adopt cloud services, practical experience in securing cloud environments (e.g., AWS, Azure, Google Cloud) is necessary. This involves configuring access controls, encryption, and monitoring.
- **Security Policies and Compliance**: Understanding regulatory requirements (e.g., GDPR, HIPAA, PCI DSS) and implementing security policies is essential. Professionals should know how to conduct security

audits and ensure compliance.

- **Certification in Cyber Security:** A certification in Cyber Security would also be desirable.

(e) Competencies

It is desirable that the candidates can demonstrate competency under the following headings:

(i) Management & Change

- Ability to think and act strategically to ensure functional responsibility is properly aligned with corporate policies and strategies, and organisational goals.
- Clear understanding of political reality and context of local authority operations.
- Ability to embed good governance practices into day-to-day activities, practices and processes.
- Ability to develop and maintain positive and productive professional relationships both internally and externally to the local authority.
- Effectively manage change, foster a culture of creativity in employees, overcome resistance to change and develop new ways to work effectively.

(ii) Delivering Results

- Acts decisively and makes timely, informed and effective decisions.
- Pinpoints critical information and address issues logically.
- Develops operational and team plans having regard to corporate priorities operational objectives and available resources.
- Establishes high quality service and customer care standards.
- Allocates resources effectively to deliver on operational plans.
- Identifies and achieves efficiencies.
- Ensures compliance with legislation regulation and procedures.

(iii) Performance through People

- Effectively manages the performance of individuals and teams to achieve operational plan targets and objectives.
- Leads by example to motivate staff in the delivery of high-quality outcomes and customer service.
- Develops staff potential.
- Manages underperformance or conflict.

- Understands the value of effective communications at all levels within the organization.
- Actively listen to others.
- Demonstrates high level of verbal and written communication skills.
- Fosters and maintains productive working relationships within the organisation and with relevant stakeholders externally.

(iv) Personal Effectiveness

- Initiative and creativity.
- Enthusiasm and positivity about the role.
- Resilience and Personal Well-Being.
- Personal Motivation.
- Understands the importance of corporate governance.
- Ability to work under pressure and to lead effectively during potential security incidents
- Commitment to integrity & good public service values.
- Understanding the structures and environment within which the local authority sector operates and the role of an I.S. Project Leader in this context.

Candidates at interview must achieve a minimum 50% of the total marks available in each of the competencies to qualify for inclusion on a panel.

4. Particulars of the Post

a) General

Donegal County Council proposes to create a panel of qualified candidates for the position of IS Project Leader – Cyber Security from which it will fill any vacancies permanent or temporary that may arise.

b) Probation

Successful candidates shall be required to be on probation for an initial period, as determined by the Council. This period may be extended at the discretion of the Council.

c) Remuneration

The current annual salary-scale is €58,252 minimum to max LSI2 €75,728 (as per Circular EL 10/2024).
Holders of the post will be paid at the appropriate point on the salary scale in accordance with the relevant Department Circular.
New entrants will commence on the minimum point of the scale.

d) Base
The base for the post of IS Project Leader shall be the County House Lifford or any other such location as determined by the Council and will depend on the particular area and service to which the post holder is assigned.

The role of IS Project Leader may involve some travel, with some involving overnight stays and associated costs covered by the appropriate allowances.

e) Residence
Holders of the post shall reside in the district in which their duties are to be performed or within a reasonable distance thereof.

f) Working Hours
The normal hours of work will be 35 hours per week. The Council reserves the right to alter the hours of work from time to time.

Annual leave allowance will be in accordance with Circular LG(P) 07/2011. Maximum 30 days for all applicants.

g) Requirement to Drive
Candidates shall be required:

- to possess a full current category B Driving Licence.
- to have their own vehicle available for use while performing their duties and the associated costs will be covered by the appropriate allowances.

h) Citizenship Requirements
Eligible candidates must be, on the latest date for receipt of completed application forms; (a) A citizen of the European Economic Area (EEA). The EEA consists of the Member States of the European Union, Iceland, Liechtenstein and Norway; or (b) A citizen of the United Kingdom (UK); or (c) A citizen of Switzerland pursuant to the agreement between the EU and Switzerland on the free movement of persons; or (d) A non-EEA citizen who is a spouse or child of an EEA or UK or Swiss citizen and has a stamp 4 visa; or (e) A person awarded international protection under the International Protection Act 2015 or any family member entitled to remain in the State as a result of family reunification and has a stamp 4 visa or (f) A non-EEA citizen who is a parent of a dependent child who is a citizen of, and resident in, an EEA member state or the UK or Switzerland and has a stamp 4 visa.

i) Conflicts of Interest

The post holder shall not engage in any gainful occupation, other than as an employee of a local authority, to such an extent as to impair the performance of his or her duties as an employee of a local authority or in any occupation which might conflict with the interests of the local authority, or which might be inconsistent with the discharge of his duties as a local authority employee.

j) Garda Vetting

Candidates for the post of Front of House Senior Administrator are subject to Garda Vetting. Prior to appointment, candidates must undergo and satisfactorily complete the Garda Vetting process.

5. Recruitment Process

a) Application Form

- Applications must be made on the official application form and all sections of the form must be fully completed.
- **Please do not submit a CV with your application**. Only information contained in the application form will be considered when assessing a candidate's suitability for the post.
- Applications must be submitted as an e mail attachment in either Word or PDF format only **by email only** to vacancies@donegalcoco.ie
- Applications must be received by the deadline specified on the form.
- Applications that are late, lost or delayed will not be considered unless official evidence showing that the application was sent within the timeframe can be produced.

b) Short Listing

Candidates may be short-listed for interview on the basis of information supplied. In the event of a short-listing exercise being required, an Expert Panel will convene to examine and assess the application forms against a set of pre-determined criteria, based on the requirements of the job. It is therefore in your own interest to provide a detailed and accurate account of your qualifications and experience on the application form.

Where it is considered, by reason of the number and standard of applications received, that it would be reasonable not to admit all candidates to the interview, only persons likely to attain at the interview a standard sufficient for selection and recommendation for appointment shall be called for interview.

c) Right to Information and Review

The Council is committed to offering feedback and information to candidates. Any candidate who wishes to do so may request to have a decision or the

process reviewed. Any such request must be submitted in writing, stating the grounds of the request and this must be submitted to the Human Resources Department, Three Rivers Centre, Lifford, Co. Donegal within five working days of the date of notification of a relevant decision.

d) Confidentiality

Subject to the provisions of the Freedom of Information Act 2014, applications will be treated in strict confidence.

e) Other

Appointments to the Council are subject to satisfactory checks with regard to references, qualifications, medical examinations, and Garda Vetting, as applicable.

f) Canvassing Will Disqualify

Any attempt by a candidate (or by any persons acting on their behalf) to canvass or otherwise influence any officer of the Council (or persons nominated by it to interview or examine applicants) in the candidate's favour, either directly or indirectly, by means of written communication or otherwise, will automatically disqualify the applicant for consideration for the position.

g) General Data Protection Regulation

Donegal County Council is committed to protecting your personal data and we comply with our obligations under the Data Protection Acts, 1988 – 2018, and the General Data Protection Regulation.

- **Basis for Processing your Personal Information**

The basis for processing your personal data is to process your application for the position you have applied for with Donegal County Council under the Terms of the Employment (Information) Act 1994 and Human Resources Department policies and procedures.

When your application form is received, we create a computer record in your name, which contains much of the personal information you have supplied on your application form. This personal record is used solely in processing your candidature. You are entitled to obtain at any time, a copy of information about you, which is kept on record.

- **Sharing of Information**

Outside of the relevant recruitment team, the information provided in your application form will only be shared for progressing the competition for which you have applied for, with a designated shortlisting and/or interview board.

If, following the competition, you are deemed a qualified candidate and offered a position; the information provided in your application form will form part of your Personnel File.
Furthermore, should you be offered a position and subsequently confirm your interest in the position, the information provided on your application form will be used to request service records and employment references.

- **Storage period**

Your application will be retained for two years from the date a panel for this position is formed. Applications that are not progressed to interview stage will be destroyed post competition.
Donegal County Council's Privacy Statement can be assessed at:
www.donegalcoco.ie