SOUTH DUBLIN COUNTY COUNCIL

(Comhairle Chontae Atha Cliath Theas)

Information Security Analyst

The Role

The Information Security Analyst will be in the first line of defence for the Council against cyber threats. The successful candidte will be responsible for identifying and preventing cyber threats affecting or having the potential to affect the Council as well as maintenance of IT Security Management procedures and processes. They will be expected to meticulously analyse security systems, uncover vulnerabilities, and together with more senior staff develop strong strategies to counter security threats. Their work will be critical to ensuring that the Council can operate securely and effectively in today's digital landscape.

The Information Security Analyst is a critical member of the organisation's cybersecurity team, responsible for providing advanced security expertise and leadership to protect the organisation's digital assets and infrastructure. In this role, the Information Security Analyst serves as a subject matter expert, guiding the implementation and maintenance of robust security controls, incident response procedures, and forensic analysis capabilities.

As a seasoned cybersecurity professional, the Information Security Analyst plays a pivotal role in ensuring the organisation's security posture remains strong and resilient against evolving cyber threats. They are responsible for overseeing the administration, diagnostics, and ongoing support of the organisation's networking and cybersecurity infrastructure, ensuring that all necessary security measures are in place to safeguard digital government services.

The Information Security Analyst is also a key contributor to the development and maintenance of the organisation's security documentation, including policies, procedures, and incident response plans. They work closely with cross-functional teams to design, develop, and implement new network and cybersecurity solutions, leveraging their deep technical expertise and industry knowledge to identify and evaluate the most effective security technologies and strategies.

In addition to their technical responsibilities, the Information Security Analyst serves as a trusted advisor and resource for end-users, providing first-line support and guidance on cybersecurity best practices. They also contribute to the organisation's overall security posture by conducting risk assessments, developing security awareness campaigns, and participating in vulnerability assessments and penetration testing.

The Information Security Analyst plays a pivotal role in safeguarding the organisation's digital assets, ensuring the confidentiality, integrity, and availability of critical systems and data. Their expertise, leadership, and commitment to continuous improvement are essential in maintaining the organisation's resilience against evolving cyber threats.

Qualifications

Character

Candidates will be of good character.

Health

Each candidate must be in a state of health such as would indicate a reasonable prospect of ability to render regular and efficient service.

Education, Training, Experience

Each candidate must, on the latest date for receipt of completed application forms have –

(A) 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 3 years directly relevant, recent ICT hands-on experience from your employment to date

OR

(B)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 4 years directly relevant, recent ICT hands-on experience from your employment to date*

OR

(C) A Level 7 NFQ major award qualification in a relevant computing discipline ***and*** at least 4 years directly relevant ICT hands-on experience from your employment to date*.

OR

(D) A level 6 NFQ major award qualification in a relevant computing discipline and at least 5 years directly relevant ICT hands-on experience from your employment to date*

And

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.

Highly Desirable

NFQ Level eight Qualification in Computer Studies or an equivalent accredited certified IT qualification.

The Ideal Candidate

The ideal candidate for the Information Security Analyst role should possess many of the following qualifications, skills, and experience:

1. Technologies:
   The Information Security Analyst role requires a deep understanding of the organisation's robust security infrastructure, which includes amongst others the following key technologies:
   - Microsoft Security Platforms: The organisation has invested in a comprehensive suite of Microsoft security solutions, providing advanced threat protection and identity management capabilities. Familiarity with the Microsoft Security Center and associated workspaces would be a distinct advantage.
   - Juniper Networks: The organisation's network is fortified by Juniper Networks, ensuring secure and reliable connectivity across the entire ecosystem.
   - ClearPass Authentication: The organisation has implemented ClearPass to provide robust access control and policy management, further strengthening the security of the network.
   - CryptoSpike Ransomware Protection: The organisation has deployed CryptoSpike to detect and respond to sophisticated ransomware threats.
   - QRadar SIEM: The organisation utilises QRadar as part of a managed Security Operations Center (SOC) and Security Information and Event Management (SIEM) solution for monitoring and responding to security incidents.

Candidates with experience and expertise in these or similar enterprise-grade security technologies will be well-positioned to excel in the Cyber Security Senior Analyst role.

2. Incident Response and Forensic Analysis:
    - Extensive experience in incident response, including identifying, monitoring, and reporting suspicious activity, as well as containing incidents, eradicating threats, and conducting post-incident analysis.
    - Proficiency in digital forensic analysis, including collecting, preserving, and analysing digital evidence related to cybersecurity incidents.
    - Strong problem-solving and critical thinking skills to effectively investigate and respond to security incidents.
3. Cybersecurity Infrastructure Management:
    - Expertise in administering, diagnosing, and providing ongoing support for the organisation's networking and cybersecurity infrastructure, including configuring and managing network devices, monitoring for suspicious activity, and identifying and resolving security vulnerabilities.
    - Thorough understanding of networking, network security technologies, such as firewalls, intrusion detection/prevention systems, and security information and event management (SIEM) tools.
    - Ability to implement and maintain appropriate security measures to protect digital government services, including security controls, security awareness training, and security control testing.
4. Security Documentation and Solution Development:
    - Demonstrated experience in contributing to the development and maintenance of security documentation, such as security policies, procedures, and incident response plans.
    - Proficiency in participating in the design, development, and implementation of new network and cybersecurity solutions, including researching and evaluating new security products and technologies, assisting with deployment and configuration, and providing training and support.
    - Strong technical and analytical skills to research, evaluate, and implement effective security solutions.
5. Continuous Learning and Collaboration:
    - Proven commitment to staying up-to-date on the latest cybersecurity threats and trends, and the ability to share this knowledge with the organisation.

- Excellent communication and interpersonal skills to provide first-line support to end-users and collaborate with cross-functional teams.
- Ability to contribute to the overall security posture of the organisation, including conducting risk assessments, developing security awareness campaigns, and participating in vulnerability assessments and penetration tests.

6. Information Security Management System (ISMS) Implementation:
    - Experience in assisting with the implementation and maintenance of the organisation's ISMS, including developing and implementing security controls, maintaining security incident records, and reporting on the organisation's security posture.
    - Familiarity with security frameworks and standards, such as NIST, ISO, and NIS2, to ensure the ISMS aligns with industry best practices.

Overall, the ideal candidate for the Information Security Analyst role should possess a strong technical background in cybersecurity, a deep understanding of incident response and digital forensics, expertise in managing and securing complex IT infrastructures, and the ability to collaborate effectively with cross-functional teams. They should also demonstrate a commitment to continuous learning and a proactive approach to enhancing the organisation's overall security posture.

Key competencies / skills

- Management and Change
- Delivering Results
- Performance through People
- Personal Effectiveness
- Local Government Knowledge and Understanding

Candidates are requested to give an example of a situation which highlights the behaviour, skills and attitude that underpin effective performance in these areas and which demonstrates their suitability to meet the challenges of this role. Candidates should ensure the example used clearly demonstrates their ability in this area and that the scale and scope of the example given is appropriate to the post and level of the post.

Particulars

The office is wholetime, permanent and pensionable.

Salary

€55,090 - €56,405 - €58,006 - €61,019 - €62,819 (max) - €65,055 (1st LSI) - €67,304(2nd LSI)

Entry point to this scale will be determined in accordance with Circulars issued by the Department of Housing, Planning, Community and Local Government.

The salary shall be fully inclusive and will be determined from time to time. Holders of the office will pay to South Dublin County Council any fees or other monies (other than their inclusive salary) payable to or received by them by virtue of their office or in respect of service which they are required by or under any enactment to perform.

Rate of remuneration may be adjusted from time to time in line with Government Policy.

Duties

The duties will be such as will be assigned by the local authority from time to time, and will include the duty of deputising for other officers of the local authority when required.
The duties will also include such duties as may be assigned in relation to the area of any other local authority.

The duties may include:-

- Incident Response: assisting with incident response and forensic analysis as necessary. Incident response is the process of responding to and recovering from a cybersecurity incident. This may include:
  - Identifying, monitoring, and reporting suspicious activity.
  - Containment: Containing the incident to minimize the impact.
  - Eradication: Removing the malware or attacker from the system.
  - Recovery: Restoring the system to normal operation

- Post-incident analysis: Analysing the incident to improve security posture.

- Forensic Analysis: Forensic analysis is the process of collecting, preserving, and analysing digital evidence related to a cybersecurity incident. This may include:
  - Collecting digital evidence: This may include logs, files, network traffic, and other data from the affected system.
  - Preserving digital evidence: This ensures that the evidence is not altered or destroyed.
  - Analysing digital evidence: This involves using forensic tools to identify, extract, and interpret the evidence.
  - Reporting on digital evidence: This may include creating a report that summarizes the findings of the analysis.

- Assist with the administration, diagnostics, and ongoing support for the organisation's networking and cyber security infrastructure. This includes tasks such as:
  - Configuring and managing network devices (routers, switches, firewalls)
  - Monitoring network traffic for suspicious activity
  - Identifying and resolving security vulnerabilities
  - Responding to security incidents

- Provide support to ensure that all necessary and appropriate security measures are in place to protect digital government services implemented by the organisation. This includes tasks such as:
  - Implementing security controls based on risk assessments
  - Conducting security awareness training for employees
  - Testing the effectiveness of security controls

- Contribute to the development and maintenance of security documentation. This includes tasks such as:
  - Writing and updating security policies and procedures
  - Creating and maintaining security incident response plans
  - Documenting security testing results

- Completing incident reporting documentation

- Participate in the design, development, and implementation of new network and cyber security solutions. This may include tasks such as:
  - Researching and evaluating new security products and technologies
  - Assisting with the deployment and configuration of new security solutions
  - Providing training and support for new security solutions

- Stay up-to-date on the latest cybersecurity threats and trends. This includes tasks such as:
  - Reading security news and blogs
  - Attending cybersecurity conferences and training
  - Participating in online cybersecurity communities

Additional Duties:

- Provide first-line support to end users with their cybersecurity needs. This may include tasks such as:
  - Answering questions about security policies and procedures
  - Helping users to implement or adhere to organisation security measures.
  - Advising users on how to protect their devices from cyber threats

- Contribute to the overall security posture of the organisation. This may include tasks such as:
  - Conducting risk assessments
  - Developing security awareness campaigns
  - Participating in or conducting vulnerability assessments and penetration tests

- Contribute to the implementation and maintenance of the organisation's Information Security Management System (ISMS). This may include tasks such as:
  - Assisting with the development and implementation of security controls
  - Maintaining records of security incidents and corrective actions
  - Reporting on the organisation's security posture,

- Such other duties as may be assigned from time to time.

Superannuation

The provisions of the Local Government (Superannuation) (Consolidation) Scheme 1998 may apply.

Persons who become pensionable officers who are liable to pay the Class A rate of PRSI contribution will be required, in respect of their superannuation contribution, to contribute to the local authority as follows:
1.5% of their pensionable remuneration
plus
3.5% of net pensionable remuneration
(i.e. pensionable remuneration less twice the annual rate of social insurance old age contributory pension payable at the maximum rate to a person with no adult dependent or qualified children).

Persons who become pensionable officers who are liable to pay the Class D rate of PRSI contribution will be required, in respect of their superannuation contribution, to contribute to the local authority at the rate of 5% of their pensionable remuneration.

The provisions of the Spouses and Children's / Widows & Orphans Contributory Pension Scheme will continue to apply.

New entrants will be admitted to the Single Public Service Pension Scheme with effect from the date of appointment. The scheme is contributory and provides pension, retirement gratuity, death gratuity and survivors benefits. To qualify for a pension the successful candidate must have served a minimum of two years employment in a Local Authority.

2024 Rates and Thresholds

Local Government Superannuation Scheme members

- €0.00 to €34,500 0%
- €34,500 to €60,000 10%
- Over €60,000 10.5%

Single Public Sector Pension Scheme members

- €0.00 to €34,500 0%
- €34,500 to €60,000 3.33%
- Over €60,000 3.5%

Residence

Holders of the office will reside in the district in which their duties are to be performed or within a reasonable distance thereof, as determined by South Dublin County Council.

Citizenship

Critical Skills Occupations

Candidates must, by the date of submission of application form, have a Critical Skills Employment Permit (stamp 1G). Candidates should ensure that the post they are applying for is included in the Critical Skills Occupations List

Non-Critical Skills Occupations

Candidates must, by the date of submission of application form, be:

1. A citizen of the European Economic Area (EEA). The EEA consists of the Member States of the European Union, Iceland, Liechtenstein and Norway;
   or
2. A citizen of the United Kingdom (UK);
   or
3. A citizen of Switzerland pursuant to the agreement between the EU and Switzerland on the free movement of persons;
   or
4. 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
5. 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

6. 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.

In the case of **relief positions** advertised by the Council, a person awarded a stamp 2 Visa (student visa) is allowed to work to a maximum of 20 hours work per week.

Outside employment

The position is whole-time, and the employee may not engage in private practice or be connected with any outside business which would interfere with the performance of official duties.

Retirement age

There is no mandatory retirement age for new entrants to the public service as defined in the Public Service Superannuation (Miscellaneous Provisions) Act 2004.

Anyone who is not a new entrant to the public service, as defined in the Public Service Superannuation (Miscellaneous Provisions) Act 2004, is subject to a compulsory retirement age of 70 years or as determined in accordance with Department Circulars and in line with Government Policy.

The maximum retirement age for new entrants as defined by the Public Service Pensions (Single Scheme and other Provisions) Act 2012 is 70 years.

Incentivised Scheme for Early Retirement (ISER)

It is a condition of the Incentivised Scheme for Early Retirement (ISER) as set out in Department of Finance Circular 12/09 that retirees, under that Scheme, are debarred from applying for another position in the same employment or the same sector. Therefore, such retirees may not apply for this position.

Hours of Work

The successful candidates normal hours of work will be 35 hours per week.

The Council reserves the right to alter your hours of work from time to time.

Annual Leave

Annual leave entitlement for the position of Information Security Analyst is 30 days.

Probation

Where a person is permanently appointed to South Dublin County Council, the following provisions will apply -

(a) there will be a period after appointment takes effect, during which such a person will hold the position on probation;
(b) such period will be one year but the Chief Executive may, at his discretion, extend such period;
(c) such a person will cease to hold the position at the end of the period of probation unless during this period the Chief Executive has certified that the service is satisfactory;
(d) the period at (a) above may be terminated on giving one week's notice as per the Minimum Notice and Terms of Employment Acts;
(e) there will be assessment(s) during the probationary period;

Officers who have already completed a probationary period with another Local Authority will not be obliged to serve probation with South Dublin County Council.

Recruitment

Selection will be by means of a competition based on an interview conducted by or on behalf of the Council.

Interview may be face to face or conducted through Microsoft Teams and will be at the discretion of the Council.

South Dublin County Council reserves its right to shortlist candidates in the manner it deems most appropriate which may include desktop shortlisting and / or preliminary interviews.

Shortlisting will be on the basis of information supplied on the application form and the likely number of vacancies to be filled. It is therefore in your own interest to provide a detailed and accurate account of your qualifications and experience on the application form, and to fully complete the competency questions where applicable.

A panel may be formed on the basis of such interviews. Candidates whose names are on a panel and who satisfy the Council that they possess the qualifications declared for the post and that they are otherwise suitable for appointment may, within the life of the panel, be appointed as appropriate vacancies arise. The life of the panel will be for a period of one year from the date of its formation.

The Council will not be responsible for any expenses a candidate may incur in attending for interview.

For the purpose of satisfying the requirement as to health, it will be necessary for successful candidates to undergo a medical examination by a qualified medical practitioner to be nominated by the Council.

Appointment will also not proceed without the Council obtaining two satisfactory references from responsible persons know to but not related to the candidate. A responsible person should be a person under whom the candidate has serviced in employment, or in the case of relevant voluntary work a person who has held a supervisory position. At least one of references must be from a current employer.
.

South Dublin County Council will require persons to whom appointments are offered to take up such appointments within a reasonable period of time as determined by the Council. If they fail to take up appointment within such period or such longer period as the Council in its absolute discretion may determine, the Council will not appoint them.

Garda Vetting will be sought prior to appointment in accordance with the National Vetting Bureau Act 2012 - 2016.

A candidate who is found to be ineligible at any stage of the competition will not be further considered. Provision of inaccurate, untrue or misleading information will lead to disqualification from the competition, withdrawal of employment or dismissal.

A candidate who does not attend for interview when and where required by the Council will have no further claim to consideration.

Only applications received electronically through the Council's e-Recruitment system will be accepted and must be received no later than **midnight on Thursday, 3rd October 2024.**

Applicants should hold themselves in readiness for interview any time after the closing date.

Interview results will be available on www.sdcc.ie

South Dublin County Council is an equal opportunities employer.
Canvassing will automatically disqualify.