ICT Security Manager
(Analyst Programmer 3)

GENERAL JOB SPECIFICATION
Duties and Terms & Conditions of Employment

1. PREAMBLE

Mary Immaculate College is an autonomous, university-level, Catholic College of Education and the Liberal Arts. Founded in 1898, and linked academically with the University of Limerick, MIC is the oldest higher education institution in Limerick. Significant expansion in recent decades has seen the College's offerings expand across two modern campuses, one based in Limerick City and one in Thurles, Co. Tipperary. The student community consists of more than 5,000 learners, participating in fifteen undergraduate degree programmes and several postgraduate programmes extending to PhD/Doctoral level. Academic staff engage in a wide range of academic research areas, and research underpins all teaching and learning at MIC.

MIC seeks to prepare its students for professional excellence and to nurture their capacity to lead flourishing lives.

2. CANDIDATE PROFILE AND SCOPE OF THE POSITION

The College wishes to fill the position of ICT Security Manager on a full-time, permanent contract basis.

The ICT Services Department is responsible for all matters relating to information and communications technology within the College. It supports the enabling of the objectives of the College through strategic alignment, meeting stakeholder needs and maintaining a balance between the realisation of benefits and the optimisation of resources.

The successful candidate will be responsible for cyber security activities for the ICT Services department.

Essential Qualifications & Skills (i.e. those, without which, a candidate would not be able to do the job.)**:**

In order to be considered for this position, candidates must:

1. A Level 8 Degree or higher in a relevant discipline with a minimum of 5 years relevant experience
2. Proven experience in managing cyber security operations, cyber security risk and implementing cybersecurity related technologies and controls.
3. Knowledge and experience in leading cyber security initiatives, organizing staff cyber security training, and fostering a cyber security-conscious culture including implementing cyber security posture improvements.
4. Expertise and experience in handling cyber security incidents/breaches, forensic analysis, recovery plans and cyber security audits.
5. Knowledge and experience of GDPR, ISO 27001, NIST frameworks, and other relevant cyber security regulations.

6. Experience in assessing evolving cyber security threats and adjusting cyber security strategies accordingly.
7. Extensive knowledge and experience of all cyber security connected technologies including firewalls, network security, encryption, mobile device management, intrusion detection systems, endpoint security and data loss prevention.
8. Experience in leading, communicating effectively, and collaborating with a wide variety of stakeholders, both internal and external, in relation to cyber security.
9. Focus on achieving results with a commitment to completing tasks on time and to a high standard.
10. Have completed a CISSP (Certified Information Systems Security Professional), a CISM (Certified Information Security Manager), or a CEH (Certified Ethical Hacker) course.

Cuirfear fáilte roimh iarratais ó dhaoine go bhfuil dearcadh dearfach acu i leith na Gaeilge.
Applications are welcome from people who have a positive outlook to Irish.

3. JOB DESCRIPTION

Reporting Relationship

The appointee is required to carry out the duties set out below, under the general direction of the Director of ICT, to whom they report, and to whom they are responsible for the performance of these duties in the first instance.

The appointee will report through the Director of ICT to the College President and/or to other such College Officers as the President may designate from time to time. The appointee will liaise with the Vice Presidents, Deans, Heads of Departments, Course Leaders and other College personnel and with relevant College bodies in carrying out the duties attaching to the post. The reporting relationship may be subject to review from time-to-time, in line with service needs and developments in the College.

Duties and Responsibilities

- Ensure overall ICT compliance with regulatory cyber security requirements through proactive planning, communication, ownership and relationships.
- Continuously expand and maintain up-to-date ICT cyber security policies, standards and guidelines, ensuring implementation across projects, college systems, services and departments.
- Regularly monitor, audit and report on cyber security risks and develop measures and controls through a cyber security posture improvement plan to prevent data breaches and unauthorised access.
- Conduct regular cyber security audits and risk assessments and make/implement recommendations for improvements.
- Provide technical leadership in the use of cutting-edge cyber security technologies and tools, including AI-driven threat detection, and SOC/SIEM systems.
- Ensure audit trails, system logs and other monitoring data sources are reviewed periodically and comply with policy requirements.
- Constantly monitor networks and systems for vulnerabilities.
- Manage and investigate cyber security incidents including investigations, forensics and take responsibility for any resultant actions.
- Provide ongoing training and education for staff to promote a culture of cyber security awareness and vigilance.

- Ensure that the proper protections are in place to provide for the confidentiality, integrity and availability of computer resources including ensuring that an ICT disaster recovery plan is in place and tested.
- Keep up to date with emerging technologies, cyber security trends, and best practices.
- Work with key stakeholders, including MIC's Data Protection Officer.

The duties and responsibilities as listed are broadly defined and are not exhaustive. The performance of the entire range of duties is not necessarily confined to any one individual, as the work requires that the staff function in a flexible manner, and work together as a team. The College retains the right to assign new duties and/or to re-assign staff to other areas of the College, in response to service needs.

4. TERMS AND CONDITIONS

General

All persons employed will sign an appropriate contract, which will contain terms and conditions of the employment. A job description is given to all applicants for employment and this will form part of the contract documentation.

Place of Work

The appointee's normal place of work will be Mary Immaculate College, Limerick. The College reserves the right to require the appointee to work from any other location. It is a requirement of the College that the appointee must reside within a reasonable distance of the College.

MIC operates a blended working policy, which offers scope for the post holder to combine office attendance with remote working, subject to the provisions of the policy.

Exclusivity of Service and Outside Work

The person appointed will be required to devote their full-time attention and abilities to their duties during their working hours in the College and to act in the best interest of the College at all times. Therefore, for as long as the successful applicant is working in the College, they may not, without the prior written consent of the Vice President Administration and Finance (VPAF), be actively engaged or concerned in any way, either directly or indirectly, in any other business or undertaking where this is or is likely to be in conflict with the College's interests or the performance of the duties that the person has been employed for.

The appointee will not, during their tenure of office, undertake paid outside work unless they have received the permission of the VPAF of Mary Immaculate College to undertake such work on the terms and conditions as agreed for the particular undertaking in question. In every case, it is the duty of the appointee to seek in writing the prior permission of the VPAF. It is also the duty, in every case, of the appointee to inform the person or body for whom the work is being undertaken, that the work is being conducted in a private capacity and that the College cannot in any circumstances be responsible for such work.

Probationary Period

The appointment is subject to satisfactory completion of the standard 6-month probationary period. The probationary period may be extended at the discretion of the College but will not in any case exceed 11 months. Absences during the period of probation will extend the probationary period. Performance and

conduct during the probationary period will be reviewed through a process of assessment meetings. Termination of the appointment during the probationary period, for any reason or no reason, will be at the discretion of the College. The disciplinary procedure will not apply to a dismissal during probation where the probationary employee has been employed by MIC for less than 12 months.

Hours of Attendance

The full-time working hours are 35 hours per week.

The normal hours of duty are Monday to Thursday, 9:00 am to 05:00 pm, with a 1-hour unpaid lunch break each day and Friday, 9.00 am to 4.45 pm with a 45-minute unpaid lunch break. However, the duties attaching to the position are such that the post holder may be required to work evenings/weekends on occasion to accommodate service needs. Subject to College policy, the post holder may avail of "Time-Off-In-Lieu (TOIL)" or overtime where working hours exceed the contract hours per week.

The College reserves the right to adjust starting and finishing times or days of duty to meet service needs.

Salary

The Salary scale for this position has been approved by the Department of Further and Higher Education, Research, Innovation and Science and the Higher Education Authority in line with Government Policy on Public Sector remuneration. The rate of remuneration may be adjusted from time to time in line with Government pay policy. The appointment will be made on the salary scale at a point in line with current Government Pay Policy. New entrants to the Civil or Public Sector, as defined in Circular 18/2010, will commence on the first point of the salary scale.

The grade for the post of ICT Security Manager is Analyst Programmer 3. With effect from 1st March 2025 the annual salary scale for the grade of Analyst Programmer 3 is:

€64,945; €76,488; €80,589; €83,425; €87,583; €91,741; €95,885; €100,027; €104,170

Increments are awarded in line with national pay agreements.

Salary will be paid on a monthly basis on the 25th of each month, or the previous Friday if 25th falls on a weekend, using the Paypath facility. Payment of salaries and wages are subject to statutory deductions, i.e. Income Tax (PAYE), Superannuation Contributions, Pay Related Social Insurance (PRSI) and Universal Social Charge (USC)

Superannuation

New entrants to the public service will be required to participate in the Single Public Service Pension Scheme and pay Superannuation contributions at the appropriate rates in accordance with the provisions of the Public Service Pensions (Single Scheme and Other Provisions) Act, 2012. Details of this scheme can be obtained from the College's website.

All other eligible appointees are automatically included in the Colleges' of Education Pension Scheme on taking up appointment. In compliance with the Colleges of Education Pension Scheme, deductions amounting to 6.5% are made from salary. Details of the regulations concerning the Colleges' of Education Pension Scheme may be obtained from the College's Human Resources Office.

The appointee will be required to pay Additional Superannuation Contribution (ASC) under the provisions of the Public Service and Pensions Act 2017.

Appointees who commenced employment in the public service between 1st April 2004 and 31st December 2012 and have not had a break in employment of greater than 6 months will have no mandatory retirement age. All other appointees will have a mandatory retirement age of 70.

Pension Abatement

If an appointee has previously been employed in the Civil or Public Service and that appointee is entitled to or in receipt of a pension from the Civil or Public Service or where a Civil/Public Service pension comes into payment during the appointee's re-employment that pension will be subject to abatement in accordance with Section 52 of the Public Service Pensions (Single Scheme and other Provisions) Act 2012.

In applying for this position, the applicant is acknowledging that they understand that the abatement provisions, where relevant, will apply. It is not envisaged that the College will support an application for an abatement waiver in respect of appointments to this position.

Annual Leave

The annual leave entitlement for this grade is 30 working days per leave year. Annual leave should be taken when students are off campus and the taking of leave must have the prior approval of the relevant Line Manager.

Public Holidays are granted in accordance with the provisions of the Organisation of Working Time Act, 1997.

Sick Leave

Employees who have a minimum 3 months' continuous employment with the College may be granted sick pay subject to the terms of the Public Service Sick Leave Scheme. Sick pay is contingent on full cooperation and compliance with the College's absence management procedures.

Confidentiality

In the course of working in Mary Immaculate College, the person appointed may have access to or hear information concerning staff and/or students and/or the functioning and the business of the College. Such information acquired in the course of employment with the College, including any aspect of the College's responsibilities or operations, is considered to be confidential information. On no account must information concerning students, staff or other College business be divulged or discussed except in the performance of normal duties and, unless authorised to do so, this information shall not be communicated to a third party. In addition, records must never be left in a manner that unauthorised persons can obtain access to them and must be kept in safe custody when no longer required.

Health & Safety

Mary Immaculate College attaches the highest regard to the safety, health and welfare of its employees. It is the duty of each employee to take reasonable care to protect the health and safety of themselves and of other people in the workplace. Each employee must comply with all health and safety policies and procedures in operation in Mary Immaculate College and familiarise themselves with the Safety Statement.

Employees are obliged to wear any PPE (Personal Protective Equipment) that they may be provided with and no person shall intentionally or recklessly interfere with or misuse any appliance, protective clothing or other equipment provided in the workplace for health and safety purposes. Employees are statutorily/legally obliged to ensure that any accidents/incidents which may occur are reported promptly to the Health and Safety Officer on the MIC Accident/Incident Report Form.

College Policies, Rules and Regulations

The College is a Public Sector employer and is bound by National Agreements. It is also bound by regulations, circulars and directives issued on behalf of Government by the Department of Finance, the Department of Education, the Department of Further and Higher Education, Research, Innovation and Science and the Higher Education Authority.

Employees are at all times subject to the provisions of the Code of Conduct for Staff, College policies, rules and regulations. These policies include but are not confined to Disciplinary & Grievance Policies, Dignity at Work, Examination Rules & Regulations, Policy on Responsible Computing and Use of Information Technology Facilities. All employees are required to familiarise themselves with the contents of Policies and Procedures, available on the College's Staff Portal.

Termination of Employment

At least 2 calendar months' written notice is required to resign this post.

On the termination of employment but before departing from the College, staff members are required to return to the College all books, reports, memoranda, correspondence, papers, records, reports, files including data held on electronic files, computer disks, electronically recorded discs, and any other documentation, and all other property, including office keys, belonging to the College or relating to its business or affairs which are in the possession of a staff member or under their control when the employment is terminated.

5. APPLICATION AND SELECTION PROCESS

Method of Selection for Recommendation

Shortlisting
An expert group will convene to conduct shortlisting of applicants, measured against pre-determined criteria.

The criteria that will be used to shortlist candidates for this appointment are:

- A Level 8 Degree or higher in a relevant discipline with a minimum of 5 years relevant experience.
- Proven experience in managing cyber security operations, cyber security risk and implementing cybersecurity related technologies and controls.
- Knowledge and experience in leading cyber security initiatives, organizing staff cyber security training, and fostering a cyber security-conscious culture including implementing cyber security posture improvements.
- Expertise and experience in handling cyber security incidents/breaches, forensic analysis, recovery plans and cyber security audits.
- Have completed a CISSP (Certified Information Systems Security Professional), a CISM (Certified Information Security Manager), or a CEH (Certified Ethical Hacker) course.

Normally, the number of applications received for a position exceeds that required to fill the position. While a candidate may meet the eligibility requirements of the competition, if the numbers applying for the position are such that it would not be practical to interview everyone, the College may decide that a limited number will be called to interview. This is not to suggest that other candidates are necessarily unsuitable to undertake the job, rather that there are some candidates, based on their application, appear to be better qualified and/or have more relevant experience. It is incumbent, therefore upon the applicant, to ensure that all relevant information is included in their application and that they clearly identify how they meet the specified candidate criteria.

The selection process may include an aptitude assessment of one or more of the essential competencies for the post.

Interview
A recommendation for appointment will be made by an Interview Board. The appointment will be based on this recommendation, except where considerations of health or an unsuitable record in previous employment warrants a departure. A panel will be formed from which the post of **ICT Security Manager** appointments may be filled during the life of the panel (12 months).

Candidates must produce satisfactory documentary evidence of all training and experience claimed by them, if required.

Pre-Employment Health Assessment

For the purpose of satisfying requirements as to health, successful candidates, before being appointed, may be required to participate in pre-employment health screening.

Garda Vetting

Successful applicants may be required to participate in Garda vetting. Specific instruction on this process will be given at the appropriate time. Applicants who do not comply with the College's requirements in this regard will be excluded from consideration for appointment. Applicants who have resided outside Ireland for a cumulative period of 36 months or more over the age of 18 years must furnish a Foreign Police Clearance (FPC) from the country or countries of residence. Please note that any costs incurred in this process will be borne by the applicant.

Applicants Outside European Economic Area (EEA)

Mary Immaculate College welcomes applications from candidates outside the EEA, however such applicants should familiarise themselves with relevant Government policy before making an application. Further information from the Department of Enterprise, Trade and Employment is available here: Economic migration policy - DETE (enterprise.gov.ie)

Making of Applications

Applications must be submitted on an official application form in typed format. Handwritten or incomplete applications will not be accepted. Application forms for this post may be downloaded from the Mary Immaculate College website. www.mic.ul.ie/about-mic/vacancies. Applications must be submitted by e-mail to recruitment@mic.ul.ie with the subject **ICT Security Manager** no later than:

2pm on Wednesday, 3rd July 2025

The Human Resources Office will acknowledge receipt of your application by sending an email to the email address provided. Please be sure to check Spam and Junk folders as it may be redirected here by your account preferences. If you do not receive an acknowledgement of your application form within 2 working days, please contact hr@mic.ul.ie.

Late applications will not be accepted.

The College will not be responsible for any expenses, including travelling expenses, which candidates may incur in connection with their candidature.

Any attempt by a candidate either personally or through any other person, on their behalf, to canvass or otherwise influence the outcome of the selection/interview process in their favour will lead to disqualification from the competition. Any representations made on behalf of a candidate, without their knowledge will be ignored.

Mary Immaculate College is an equal opportunities employer. Mary Immaculate College holds an Athena SWAN Bronze Institution award in recognition of our commitment to advancing equality and opportunity for all in higher education.

June 2025