

Role Profile

Title: IT Manager/Senior IT Specialist - Service Desk & Cybersecurity

Reporting To: Head of Finance

Purpose of the Role

The IT Manager will have full responsibility for end-user support and infrastructure security including management of high-volume Level 1 & 2 service desk and end-user support requirements to ensure rapid incident resolution and high user satisfaction.

The IT Manager will implement and manage of robust cybersecurity frameworks to protect organisational assets and will translate complex technical issues for non-technical stakeholders. The incumbent will ensure IT operations are aligned with and support business continuity and the achievement of relevant key organisational objectives.

It is imperative that the person filling this role works collaboratively with and across all functions of the organisation.

Cheshire Ireland strives to ensure that all people using our services are supported to live their best possible life. It is critical that all Cheshire Ireland staff perform their roles in a manner that is consistent with Cheshire Ireland's core values of Excellence, Partnership, Learning, Integrity and Respect.

Key Responsibilities

Service Desk & End-User Support (Level 1 & 2 Management)

Incident & Request Management: Oversee the entire lifecycle of support tickets, ensuring Level 1 issues resolved - password resets, hardware troubleshooting, software installation efficiently, and Level 2 escalations involving system configuration and network connectivity.

SLA Adherence: Monitor and report on Key Performance Indicators KPIs such as First Call Resolution, Average Handle Time, and Ticket Backlog to ensure Service Level Agreements are met or exceeded.

User Experience: Implement feedback loops and survey mechanisms to continuously improve the end-user experience and reduce friction caused by technical issues.

Hardware & Asset Management: Manage software licensing and the lifecycle of end-user hardware laptops, desktops, mobile devices, ensuring secure provisioning, maintenance, and decommissioning.

Cyber Security Operations

Security Awareness & Training: Develop and deliver regular security training for all staff, focusing on phishing simulation, password hygiene, and social engineering defence - turning end-users into the "first line of defence".

Access Control & IAM: Enforce the Principle of Least Privilege - PoLP and manage Identity and Access Management - IAM to ensure users have only the access necessary for their roles.

Endpoint Protection: Oversee the deployment and maintenance of Endpoint Detection and Response solutions, antivirus software, and patch management to secure all endpoints managed by the service desk.

Incident Response: Serve as a key member of the incident response team, handling security events from detection - via Level 1/2 alerts through containment and remediation.

Infrastructure & Operations

System Administration: Oversee the maintenance of core business systems, including Microsoft 365/Exchange, Active Directory/Azure AD, and file servers, ensuring high availability and security.

Backup & Disaster Recovery: Implement and test backup solutions to ensure data integrity and rapid recovery in the event of ransomware attacks or hardware failures.

Compliance: Ensure IT operations comply with relevant industry standards e.g., GDPR, HIPAA, ISO 27001 by maintaining documentation and audit trails.

Vendor Management: Manage relationships with external IT vendors, suppliers, and the Level 3 IT service provider, ensuring the effective delivery of systems and services, monitoring performance, and resolving issues in a timely manner.

Collaboration & Relationship Management

Participate in project working groups where input of IT skills and knowledge is relevant or required to ensure successful outcomes.

Liaise and collaborate cross-functionally to generate and maintain positive relationships and to role model the Cheshire Ireland core value of Partnership.

Culture

Act as a champion of Cheshire Ireland core values, role modelling and fostering a culture of continuous improvement, reflective practice, on-going learning and partnership.

Essential Skills & Qualifications

Educated to degree level with at least 4 years of experience in similar role

Service Desk experience

Endpoint Management Microsoft Intune - Endpoint Manager & Windows Autopilot

Security Tools Microsoft Defender - Defender for Endpoint/Identity, and Security Awareness Training, MFA - Duo, MS Authenticator

Infrastructure Active Directory - On-Prem & Azure AD/Entra ID , Microsoft 365 Suite, Exchange Online, Group Policy, Basic Networking DNS, DHCP, TCP/IP, Firewall fundamentals

Operating Systems Windows 10/11 and Windows Server 2016/2019/2022, iOS, Android

IT Service Management: ITIL Foundation - essential for understanding Level 1/2 workflows.

Cybersecurity: CompTIA Security+, or CISSP.

Platform Specific: Microsoft 365 Certified: Endpoint Administrator Associate or Microsoft Certified: Security, Compliance, and Identity Fundamentals.

Strong communication skills both verbal and written and able to effectively communicate and influence others at all levels.

Excellent interpersonal skills with the demonstrable ability to build relationships internally and externally.

In possession of the necessary documentation to work and live in the Republic of Ireland and able to speak and write English fluently.

A clean driving licence and willing to travel for work on a regular basis and outside of normal working hours when required. Access to car essential.

Desirable Skills & Experience

Service Desk Optimisation: Restructured the Level 1/2 support workflow, reducing average ticket resolution time within a time period.

Security Implementation: Lead the organisation migration to a Zero Trust security model, including the implementation of Multi-Factor Authentication MFA for all 300+ users and the deployment of an EDR solution across all endpoints.

Ransomware Prevention: Proactively identified a gap in backup procedures during a routine audit, reconfigured the backup strategy and implemented backups, successfully preventing data loss during a subsequent cyber-attack or attempt.

Policy Development: Engage and review all IT related policies on regular basis or when an incident triggers such review. Regularly review company's Acceptable Use Policy AUP and Incident Response Plan, bridging the gap between IT operations and legal/compliance requirements.

Artificial Intelligence: Knowledge of emerging technologies, including AI, and the ability to identify practical opportunities to apply them to improve business operations and service delivery.

Cybersecurity Frameworks: Knowledge and practical experience of cybersecurity frameworks, such as NIST Cybersecurity Framework and/or ISO 27001.

Demonstrated Behaviours & Personal Attributes

Motivated by strong personal values that are aligned to the core values of Cheshire Ireland. Sets a personal example that reinforces Cheshire Ireland's reputation and standards.

Exhibits a high personal drive for excellence and holds self accountable for consistently high-quality performance and results.

Models open communication and information-sharing, consistently keeping all stakeholders engaged and informed.

Demonstrates ability to collaborate with colleagues cross-functionally and uses influence positively and skilfully to find common ground in order to achieve organisational goals.

Uses experience, technical expertise, and established standards and methods to analyse and solve problems and exercises sound judgment about when to act and when to escalate issues to the next level of expertise.

Adept at evaluating, planning, and prioritising own work, creating efficient workflows to manage multiple activities and using time and resources effectively to deliver results on or before deadline.

Understands and supports the need for change and continuous process improvements.

Demonstrates the desire and ability to grow own capabilities by seeking out and engaging in challenging learning opportunities that enhance contribution to the organisation and advance professional and career development.

Flexibility & Additional Duties

The nature of this role requires flexibility and mobility. The role-holder will be required to travel to Cheshire Ireland sites at regular intervals. From time to time this will mean travel outside of normal working hours. All employees must be prepared to undertake additional tasks from time to time as assigned by the organisation.

This role profile is subject to periodic review and may be amended as necessary to meet evolving organisational needs.