

Job Description

Job Title: Infrastructure Security Engineer
Team: IT
Reports to: Director of IT
Date: September 2025



the muckle way

Purpose of Role

Help design and lead delivery of the firm's overall endpoint management and security approach

Core Responsibilities:

- Day-to-day administration and management of Microsoft 365 services including **Entra ID (Azure AD)**, **Intune**, **Exchange Online**, **SharePoint Online** and **Teams**.
- Deployment and management of **Intune** policies, including:
 - Device compliance and configuration profiles for **Windows**, **Android** and **iOS** devices.
 - Lead the transition to Intune cloud-only **Autopilot** deployments.
 - Support the migration of on-prem **Group Policy** settings to **Intune** using modern management best practices.
 - Software and app deployment (**Win32 / MSI / Store apps**).
- Support vulnerability management processes including:
 - Patching of critical third-party software (e.g. **Veeam Backup and Replication** and **VMware vSphere / ESX**).
 - Assessment and remediation of **Common Vulnerabilities and Exposures (CVEs)** across the enterprise environment.
- Administration and maintenance of **SentinelOne** and **NinjaOne** endpoint management tools.
- **FortiGate** firewall configuration, rule management and troubleshooting.
- Assist in defining and executing the organisation's security strategy, policies and best practices.
- Run the firm's relationship with **Arctic Wolf**. This will include participation in monthly security hardening workshops with their technical experts.

Knowledge / Skills / Experience:

- Proven experience with **Microsoft Intune** and **Microsoft 365 administration** (minimum 3 years preferred).
- In depth understanding of **Microsoft Group Policy (GPO)**
- Strong knowledge of:
 - **PKI infrastructure** (certificates, internal/external CA and lifecycle management).
 - **Networking principles** including:
 - Segmentation and Isolation (VLANs, DMZ)
 - Secure Protocols (HTTPS/SSH)
 - Authentication and Encryption (RADIUS, PKI Infrastructure, VPN/IPSec)
 - NAT and firewall rules.
- Proficiency in **PowerShell scripting** for:
 - **Intune Automation** (Detection/Remediation/Platform scripts)
 - Deployment and automation tasks across Windows environments.
- Comfortable with both **Windows and Linux CLI** environments.
- Experience administering endpoint protection and remote monitoring / management (RMM) platforms (e.g. **SentinelOne** and **NinjaOne**).
- Practical understanding of patch management best practices across hybrid infrastructure.
- Exceptional written and communication skills.
- Ability to work independently and lead initiatives in a fast-paced environment.
- Comfortable challenging accepted norms for business benefit.
- Analytical and solution-focused approach to security challenges.
- A want to stay current with emerging threats, technologies and best practices.

Desirable Skills:

- Experience with **Zero Trust** principles and implementations.
- Hands-on knowledge of **multi-factor authentication (MFA)** and **conditional access policies**.
- Exposure to **identity governance**, **least privilege access models**, and **role-based access control (RBAC)**.
- Familiarity with cloud security standards (e.g. **CIS Benchmarks**).
- Experience working in a **Cyber Essentials Plus** certified environment.
- A full driving licence.
- Formal IT certification / qualification to 'A' level or above.

N.B. The duties and responsibilities in this job description are not exhaustive.



Trust



Teamwork



Responsibility



Care

Our Values & Behaviours

Trust

We trust each other to do the right thing

- Respect and treat each other fairly
- Be honest, open and transparent
- Be yourself and empower others to do what they do well
- Value and recognise each other

Teamwork

We are one team and work selflessly for each other

- Be aware of your impact on others
- Be clear about what you expect from others
- Plan, organise and prioritise your time
- Coach others to be their best
- Support and delegate to others
- Work hard for the collective, not for individual gain

Responsibility

We are self-starters and take responsibility for how we work together and communicate

- Be positive and enthusiastic
- Communicate – listen, ask questions and share knowledge
- Embrace feedback
- Challenge ourselves and others to deliver success
- Have great conversations, including the difficult ones

Care

We care about our people, clients and community

- Help and look out for each other
- Understand, support and learn from each other
- Be proactive and make a difference
- Be kind to yourself and others