Job Description

Role Information

Job Title	Senior IT Infrastructure Lead
Directorate (and Team)	Digital (Technology Services)
Location (supported by Hybrid Working)	Birmingham
Full Time or Part Time	Full time

Company Overview

Ardent is the UK's leading provider of land, consent management and stakeholder engagement services to support major infrastructure and regeneration projects from concept to delivery.

We are Project Managers, Chartered Surveyors, Engagement specialists and Land Referencers, based in London, Birmingham, Warrington, Leeds, Glasgow and Dublin and supporting projects throughout the UK and Ireland.

Established in 1992, we are a high-growth business with a client portfolio that includes some of the biggest players across our four core sectors of transport, renewables, utilities and regeneration.

We are passionate about delivering life-improving change for communities and future generations and we are proud to play a key role in facilitating and delivering the UK and Ireland's net zero and growth agendas, improving connectivity, enabling the repurposing of high streets and town centres and delivering new homes.

We are problem-solvers that are outcome focused working collaboratively with our clients to provide strategic advice and services that identify and mitigate risks, deliver efficiencies, delivering buildable consents and then implementing those consents to positively change people's lives and the world that we live in.

Role Purpose

Our Ardent purpose is - Delivering life improving change for communities and future generations.

- Own Ardent's technology infrastructure and the full co-managed toolset: hold and safeguard the top-level administrative access to every platform, and govern the MSP's operation within it
- Act as the technical gatekeeper for change: approve or reject MSP-proposed changes to security policies, configurations, patching schedules, and platform settings through the agreed change control process
- Verify MSP performance on the toolset — patch compliance, backup integrity, vulnerability remediation, security notifications — rather than accepting reported figures at face value
- Own the escalation decision: determine when an issue exceeds 1st line scope and warrants calling off MSP 3rd line professional services (time-and-materials), scope those engagements, and validate the resulting invoices
- Own vendor and licensing relationships for the toolset, with all licence costs paid by Ardent directly

Area	% Effort
M365 / Azure / Identity	30%
Security & Compliance	25%
Supplier & MSP Governance	15%
Infrastructure Projects	15%
Major Incidents / Escalations	10%
Documentation & Standards	5%

Values Alignment & Shared Commitment

The 3rd Line Infrastructure Lead is an ambassador of the Ardent values, promoting a culture of integrity, collaboration and excellence, inspiring a commitment to inclusivity, change and innovation.

Ardent Values

- Thirst for knowledge - We embrace every opportunity to learn, grow and continuously improve
- Own it - We do what we say we will do. We own our individual actions, are accountable for them, and take pride in adding value
- Be the difference - Focus energy to make things happen. Go beyond process. Stand up, Stand out
- Enjoy the journey - Have fun, be engaged and be proud to be Ardent
- Adapt - We drive change and innovation to deliver growth and new opportunities in an ever-changing world

Key Accountabilities, Responsibilities & Outcomes

Accountabilities and / or Responsibilities
• Act as Ardent's senior internal technical authority for infrastructure, cloud, identity, security, networking, backup, disaster recovery, and core technology services. • Design, implement, manage, support, and continually improve enterprise infrastructure platforms, including Microsoft Azure, Microsoft 365, virtual environments, storage, servers, network services, and cloud resources. • Ensure infrastructure services remain secure, resilient, scalable, supportable, and aligned to business requirements, technical standards, and future-state architecture principles. • Own and maintain infrastructure lifecycle plans, technology refresh roadmaps, capacity planning, storage and licence forecasting, and annual infrastructure budget inputs. • Act as technical owner for Microsoft 365 services, including Exchange Online, Teams, SharePoint Online, OneDrive, licensing optimisation, and service configuration standards. • Administer and govern Entra ID, Active Directory, Conditional Access, MFA, role-based access controls, identity governance, privileged access, and identity security controls.

- Hold, safeguard, and periodically test Ardent's top-level administrative access to co-managed platforms, including ITSM, RMM, EDR, email security, vulnerability scanning, patch management, backup and recovery, Microsoft 365/Azure, identity platforms, DNS/DHCP/IPAM, network monitoring, documentation platforms, and PAM/PIM solutions.
- Maintain break-glass credentials for all critical systems, ensuring they are held securely, independently of suppliers, and tested in line with governance requirements.
- Provision, review, and revoke MSP and supplier administrator access using named accounts, least-privilege controls, quarterly access reviews, and audit evidence for privileged activity.
- Enforce the agreed co-management framework, ensuring no undisclosed administrator accounts, no unauthorised supplier-side copies of Ardent data, and no new or replaced tooling without Ardent approval.
- Execute supplier access-removal processes during contract change, service transition, or exit, ensuring supplier accounts are removed within agreed timescales and written certification is obtained.
- Administer Microsoft Defender and associated security tooling, monitor and respond to security alerts, support security incident response, and work with external security providers or SOC partners where required.
- Lead vulnerability management and remediation activity, including assessment of scan findings, prioritisation of fixes, coordination with suppliers, and validation of remediation against agreed SLAs.
- Maintain Cyber Essentials Plus aligned technical controls, support audit and compliance activity, conduct technical risk assessments, and develop security hardening standards and technical baselines.
- Manage firewalls, network infrastructure, secure connectivity, SD-WAN, VPN, Wi-Fi, WAN services, DNS changes, and network monitoring, including troubleshooting complex network issues and reviewing proposed network changes.

- Own backup, recovery, and disaster recovery arrangements, including backup monitoring, restore testing, DR documentation, RPO/RTO targets, recovery procedures, technical runbooks, and business continuity testing support.
- Act as the highest internal technical escalation point for complex incidents, major incidents, problem investigations, and supplier escalations, including root cause analysis and implementation of permanent fixes.
- Act as Ardent's technical lead during P1 incidents and security incidents, coordinating internal teams, MSP resources, vendors, and independent security support where required.
- Support ITIL-aligned incident, problem, change, request, and major incident processes, including participation in major incident reviews, lessons learned activities, and continual service improvement.
- Review, approve, challenge, or reject MSP-proposed technical changes, including changes to identity controls, patching schedules, maintenance windows, DNS, firewall rules, network configuration, backup schedules, retention settings, and security policies.
- Produce, review, and maintain high-level and low-level technical designs, technical standards, architecture principles, service documentation, CMDB records, risk registers, dependency registers, and technical roadmaps.
- Own Ardent's technical standards, including security baselines, naming conventions, network architecture principles, cloud configuration standards, and infrastructure design principles, ensuring suppliers operate in line with them.
- Independently verify MSP reporting against source tool data, including patch compliance, backup success, restore testing, vulnerability remediation, security notifications, SLA performance, and service credit evidence.
- Prepare technical input for monthly service reports, quarterly service reviews, governance forums, supplier performance reviews, and service improvement plans.
- Provide technical oversight of MSPs, vendors, and third-party suppliers, including validation of technical recommendations, review of contractual performance, challenge of proposed solutions, and escalation of supplier issues.

- Assess escalated issues to determine root-cause ownership and whether resolution sits with the MSP core service, MSP professional services, a vendor, or internal action.
- Scope, commission, and technically supervise MSP 3rd line professional services engagements, including review of Statements of Work, validation of delivered outcomes, and invoice checks against agreed scope and time records.
- Evaluate supplier recommendations where existing tools or platforms are considered unfit for purpose, run vendor selection where required, and support Ardent-owned procurement decisions.
- Support supplier onboarding, service transition, exit planning, knowledge transfer, and documentation assurance so critical knowledge remains documented, current, and owned by Ardent.
- Approve supplier-proposed SOPs and own the Ardent-side SOP approval workflow, ensuring the combined SOP library remains accurate, version-controlled, complete, and suitable for audit or supplier exit.
- Manage toolset vendor relationships and licensing activity, including renewals, true-ups, support contracts, vendor escalations, and direct cost visibility for Ardent-owned services.
- Lead infrastructure, identity, security, networking, cloud, and service improvement workstreams within transformation programmes, including cloud migrations, infrastructure modernisation, automation, and operational efficiency initiatives.
- Support mergers, acquisitions, office relocations, due diligence activity, and other business change initiatives by providing technical assessment, risk input, infrastructure planning, and implementation support.
- Identify opportunities to reduce MSP dependency, strengthen internal capability, improve resilience, enhance governance, automate repeatable activity, and improve the overall quality of Technology Services delivery.

Key Competencies, Skills & Experience

Competency, Skills & Experience	Essential/Desirable
5+ years in infrastructure engineering, including significant time at 3rd line level	Essential
Deep hands-on Microsoft 365 and Azure/Entra ID administration, including conditional access, Intune, and tenancy security	Essential
Strong networking knowledge: firewalls, switching, Wi-Fi, DNS/DHCP, VPN/remote access	Essential
Hands-on experience administering an RMM platform and an EDR/endpoint protection platform	Essential
Experience with backup platforms and demonstrable involvement in restoration testing / DR exercises	Essential
PowerShell scripting for administration and automation	Essential
Experience operating formal change control and privileged access management in a production environment	Essential
Experience managing or working within an outsourced/MSP arrangement — ideally on the client side of a co-managed model	Essential
ITIL v4 Foundation certification	Desirable
Strong commercial judgement: able to scope, challenge, and validate professional services work and invoices	Essential
Microsoft certifications (e.g. AZ-104, MS-102, SC-300)	Desirable
Security certifications (e.g. Security+, CISMP) or SIEM/SOC exposure	Desirable
Experience holding a technical lead role in an MSP transition or re-tender	Essential
Vendor and licensing management experience	Essential

Key Working Relationships

MSP 3rd Line / Professional Services teams	Per engagement — scoping, supervision, and acceptance of project and escalation work
EUC Lead (internal)	Daily/weekly — build standards, stack enrolment, tooling issues affecting provisioning
People Leader	Weekly — budget, risk, contract performance, and service credit decisions
Toolset and infrastructure vendors	As needed — licensing, renewals, support escalations
Auditors / compliance	Periodic — access reviews, Cyber Essentials Plus evidence, DR test records

Success Measures (First 12 months)

Measure	Target / Indicator
Co-management access governance	Quarterly privileged access reviews completed and documented; zero undisclosed admin accounts found at audit
Change control	100% of MSP changes to security policy, patching, DNS, and network config pass through documented approval; zero unauthorised changes detected
MSP performance verification	Monthly independent verification of patch compliance, backup tests, and vulnerability

	remediation completed and evidenced; discrepancies raised at service review
3rd line call-off discipline	100% of professional services engagements have an approved scope before work starts; invoices validated against time records with zero unchallenged variances
DR readiness	DR test completed within [6] months of contract go-live, with findings tracked to closure
Exit readiness	Documentation platform assessed as complete at [6]-month review — MSP exit would require only access removal
Security posture	Cyber Essentials Plus certification maintained; critical vulnerabilities remediated within contractual SLA

What we offer

We are a purpose, and values led business with a strong focus on personal growth and opportunities to contribute to impactful infrastructure and regeneration projects across the UK and Ireland, living our purpose in delivering life improving change for communities and future generations.

We promote a supportive and collaborative culture, where our people are empowered through coaching, hybrid working, and a healthy work-life balance. Our commitment to professional development is clear, from supporting early-career professionals to enabling progression through professional qualifications and continuous learning, living our Thirst for Knowledge value. We provide purposeful work, which includes our contributions to the UK's net zero agenda and community regeneration, and seek people who value the opportunity to solve complex challenges in a culture that thrives on innovation.

We're a fast-growing business with a culture centered on learning, innovation, and opportunity. Through our company-wide coaching programme, we empower our people with faster, personalised career development, a deeper connection to our culture and values, and greater ownership of their progression.

We're looking for curious, ambitious individuals who thrive in a dynamic, purpose-driven environment, where learning, openness, trust, and collaboration are at the heart of everything we do. We also know the importance of enjoying the journey, which is why we value social connection and having fun along the way.

We offer a comprehensive benefits package designed to support the health and wellbeing, engagement, and work-life balance of our team. From day one, our people have access to hybrid working, 25 days of annual leave (with options to buy or carry over), enhanced maternity and paternity pay, and a company pension scheme.

We provide Benenden Health Care, offering mental health support, 24/7 GP services, physiotherapy, optical and dental cover, and personal accident protection (depending on level). Additional benefits include the Cycle to Work scheme, electric car leasing, recognition awards, long service leave, and a discretionary annual bonus scheme, all designed to ensure our people feel valued and supported.

We're proud to be an equal opportunities employer, and we're passionate about creating a workplace where you're empowered to bring your authentic self to work every day.

We are committed to building a diverse, inclusive team where everyone belongs. We welcome talent from all backgrounds and actively encourage applications from underrepresented groups.

If you're ready to grow with a business that's scaling rapidly and making a real impact, you're in the right place!.

To apply or learn more about this opportunity, please submit your CV to **recruitment@ardent-management.com**