

Role title	Head of IT Infrastructure	Grade	Senior Leader / Head of Function
Reports to	Finance & IT Director	Location	CSO, Darlington (Hybrid) with travel to homes and regional offices
Job family	Finance & IT Directorate	Job Code	
Role Purpose			
The Head of IT Infrastructure leads HCI's retained IT Infrastructure & Support function and is the senior service owner for the hybrid retained / outsourced operating model across the 146-home estate. The role owns IT service delivery and MSP governance for the outsourced technical layers — End User Computing (EUC), infrastructure, network, cloud, the cyber managed service, emergency out-of-hours cover, L3 technical escalation and major infrastructure projects. The internal office-hours support desk operates as the business-facing front door and service owner, led by this role. Emergency out-of-hours P1/P2 coverage is delivered by the MSP and governed by this role. This is a governance-and-accountability role. The postholder sets standards, owns service outcomes, governs the MSP, leads the service team, preserves internal controls and holds the MSP to account against the Statement of Works.			
Main Activities			
Service Delivery and MSP Governance • Own IT service delivery and vendor governance for the outsourced MSP covering EUC, infrastructure, network, cloud, the cyber managed service, emergency out-of-hours cover, L3 technical escalation and major infrastructure projects • Hold the MSP to account against the Statement of Works, SLA/KPI framework, service improvement plan, reporting obligations, compliance-evidence calendar and escalation matrix • Chair the monthly MSP service review; escalate and resolve persistent service failures, SLA breaches, handbacks and commercial concerns • Ensure the MSP does not define HCI's technical direction unchecked by routing material designs, changes and exceptions through the joint Technical Design Authority • Work with Procurement and Finance on MSP contract performance, renewal, retendering and commercial governance Internal Office-Hours Service Desk Leadership • Lead, develop and performance-manage the retained internal support desk of five IT Support Analysts, operating as the office-hours front door and service owner for care homes and central functions • Own the office-hours support model: intake, triage, prioritisation, escalation to the correct internal or MSP resolver group, user communications and backlog management • Define and monitor internal service desk KPIs including first response, first-contact resolution, triage accuracy, escalation completeness, aged backlog, CSAT and tickets per analyst • Validate service desk capacity against empirical demand — ticket volume, escalation rate, identity workload, site complexity and MSP handbacks — to confirm whether retained analyst capacity is sufficient			

Emergency Out-of-Hours Governance

- Govern and accept the MSP emergency out-of-hours P1/P2 coverage model, ensuring procedures, contact routes, acknowledgement targets and handover arrangements are documented, tested and contractually enforceable
- Ensure every out-of-hours incident is logged, reconciled into the shared ticket process and handed back to the internal desk on the next working day, and that major or cyber incidents are escalated to HCI's named accountable owners

Identity, Access and Network Administration Governance

- Own governance of Active Directory / Microsoft Entra ID, identity lifecycle, group policy, privileged access, access reviews and access-control evidence
- Line-manage the Network / Infrastructure Administrator; ensure the MSP backup model for this role is documented, tested and operationally credible, and own that governance and testing

Cyber Managed-Service Oversight

- Govern the MSP-managed cyber service, ensuring operational cyber activity is performed effectively while HCI retains accountability, risk acceptance and control ownership
- Own technical cyber governance and evidence, ensuring MSP reporting covers EDR coverage, vulnerability status, patch compliance, alert triage, incident response and threat posture, with clear escalation and decision rights

Assurance, Resilience and Compliance

- Own infrastructure standards, disaster recovery and business continuity governance, testing DR/BCP plans regularly with the MSP
- Own infrastructure and access-related SOX IT General Controls (ITGC) evidence, and support DSPT, Cyber Essentials and audit-evidence requirements to the agreed calendar
- Act as the senior internal escalation point for major infrastructure, network, cyber or support incidents affecting care operations

Qualifications and Skills Required

	Essential	Desirable
Qualifications and knowledge	Significant senior IT infrastructure or service-delivery leadership experience in a large, multi-site organisation operating a hybrid in-house / outsourced model Proven track record governing MSPs or outsourced IT providers, including SLA/KPI management, escalation, reporting, service improvement and commercial governance Strong understanding of Active Directory, Microsoft Entra ID, identity lifecycle, group policy, privileged access and access governance Experience governing cyber security services delivered by an external provider while retaining internal accountability and risk acceptance Knowledge of Cyber Essentials, DSPT, GDPR and CQC digital-governance requirements	Understanding of SOX ITGC or equivalent audit and internal-control frameworks Care, health or similarly regulated multi-site sector background ITIL v4 Foundation or higher; relevant infrastructure/security certifications

	Experience of disaster recovery, business continuity and major-incident governance	
Skills	Service delivery and MSP governance at expert level Support desk leadership and ITIL-aligned incident/request/problem/change management Identity and infrastructure governance Cyber-service oversight and governance Major-incident leadership and escalation Technical Design Authority participation and decision-making	
Experience	Experience leading an internal IT service desk, with strong ITIL-aligned incident, request, problem, change and major-incident management	
Personal attributes	Commitment to HCI's core values: Quality, Innovation, Compassion, Integrity and Respect Ownership mindset with accountability for service delivery and governance outcomes Strong stakeholder management and escalation discipline Strategic and analytical approach to problem-solving	
Special features		
Enhanced DBS disclosure required DVLA licence check required Full-time, 40 hours per week Office-hours office-based role with hybrid flexibility, plus travel to homes and regional offices Direct reports: IT Support Analysts (x5) and Network / Infrastructure Administrator (x1)		
Dimensions:		