

Role title	Network/Infrastructure Administrator	Grade	IT Specialist / Senior Technical Officer
Reports to	Head of IT Infrastructure	Location	DSO Darlington
Job family	Finance & IT Directorate	Job Code	
Role Purpose			
The Network / Infrastructure Administrator is HCI's office-hours retained technical specialist for identity, access, network and infrastructure administration, reporting to the Head of IT Infrastructure. The role owns day-to-day Active Directory / Microsoft Entra ID administration, provides second-line technical escalation above the IT Support Analysts, and acts as the internal technical liaison with the MSP for network and infrastructure matters. The role operates during office hours only. The MSP provides emergency out-of-hours P1 / P2 coverage, and the MSP also backs up this role for AD / Entra ID, access continuity, network / infrastructure escalation and emergency cover, removing the single point of failure. The postholder is the internal technical control point that keeps identity and infrastructure knowledge in-house.			
Main Activities			
Active Directory & identity management • Administer HCI's hybrid AD / Entra ID environment: users, security groups, organisational units, group policy, conditional access and directory synchronisation health. • Manage the identity lifecycle, including complex joiner, mover and leaver cases, role changes and processing of sensitive / privileged accounts. • Own privileged access controls and support regular access reviews and privileged-access reviews. • Conduct AD hygiene reviews — stale-account clean-up, orphaned-object removal and password-policy compliance — and resolve identity, authentication and sync issues escalated from the service desk. Network & infrastructure liaison • Act as HCI's internal technical liaison with the MSP for network and infrastructure matters: WAN / LAN, firewalls, switching, Wi-Fi and site connectivity across the estate. • Monitor MSP-provided performance and availability reporting; escalate degradation or recurring issues with complete diagnostic information. • Support new home openings and site changes, and review MSP network / infrastructure documentation, diagrams and change records for completeness. • Note: major infrastructure delivery, cyber operations, emergency out-of-hours response and final vendor governance sit with the MSP and the Head of IT Infrastructure, not this role. MSP backup & second-line escalation • Own the internal side of the documented MSP backup arrangement for AD / Entra ID, access continuity, network / infrastructure escalation and emergency cover, ensuring the MSP has the access, runbooks and break-glass procedures needed to act as backup. • Participate in annual and post-change testing of the MSP backup model.			

- Provide second-line technical escalation above the IT Support Analysts for complex EUC, application, connectivity and identity issues, working with the MSP where infrastructure-level intervention is required.

Cyber, compliance & service desk enablement

- Support the MSP-managed cyber service by keeping identity, endpoint and infrastructure information accurate for security monitoring, vulnerability management and incident response, with risk acceptance remaining with HCI.
- Support SOX ITGC, DSPT and Cyber Essentials evidence relating to identity, access, availability and infrastructure controls.
- Contribute technical input to the joint Technical Design Authority and change control for identity, network and infrastructure changes.
- Provide service desk enablement and quality-assure the IT Support Analysts' routine AD / access tasks (starters, leavers, password resets), coaching on escalation quality and diagnostic capture.

Qualifications and Skills Required

	Essential	Desirable
Qualifications and knowledge	Significant experience in network/infrastructure administration with strong Active Directory and hybrid AD/Entra ID expertise Practical experience of identity lifecycle, group policy, security groups, conditional access and privileged access management Experience supporting hybrid Microsoft environments, including Microsoft 365 and directory synchronisation Working knowledge of network fundamentals (WAN, LAN, Wi-Fi, DNS, DHCP, firewalls) sufficient to liaise with outsourced MSP Experience acting as technical liaison with third-party MSP or IT partner within hybrid retained/outsourced model Understanding of privileged access, access reviews, audit evidence and ITGC requirements	Microsoft/networking/security certifications (e.g. MS-102, AZ-104, Network+, Security+)
Skills	Identity and access administration at expert level Advanced MSP liaison and third-party partner management Infrastructure troubleshooting and technical escalation Second-line support and complex technical problem solving Coaching and service desk enablement	Cyber security awareness and compliance knowledge
Experience	Second-line technical support experience and ability to coach first/second-line analysts	Care, health or similarly regulated multi-site sector experience

	Awareness of cyber security controls, Cyber Essentials, DSPT and GDPR	
Personal attributes	Commitment to HCI's core values: Quality, Innovation, Compassion, Integrity and Respect Strong attention to detail, especially regarding security and compliance Collaborative approach to working with internal and external teams	
Special features		
Enhanced DBS disclosure required DVLA licence check required Office hours role (40 hours per week) with occasional travel to homes and regional offices		
Dimensions:		