**SINGLE CORPORATE SERVICES - DIGITAL**

|  |  |  |
| --- | --- | --- |
| **Job title:**  | Network Technical Architect  | ***To be completed by HR*** *Job Reference Number* *CORP SCS DIG 001**Band 7*  |
| **Reporting to:**  | Technical Delivery Manager |
| **Accountable to:**  | Associate Director IT  |
| **Pay Band:**  | Band 7 |

As part of the Single Corporate Service, this role provides a service across both Isle of Wight NHS Trust and Portsmouth Hospitals University NHS Trust.

The intention for the existing primary work locations to remain unchanged as there is no desire to change base locations unnecessarily. However, as the single corporate service will be delivered across both organisations, individuals may be required to undertake business travel from time to time. The staff mobility local agreement will apply.

For our leaders managing staff across multi-site locations, they will need to be visible and provide in person leadership. The arrangements and frequency will be agreed locally.

**Job purpose**

Play a technical role in the provision of effective, efficient and fully integrated ICT operational services that maximise their availability and integrity for end-users and optimise the value gained by the Trust from its investment in IT by:

1. Designing multiple network architectural models with varying complexities ensuring business strategy and processes are considered in translation to IT solutions.
2. Ability to operate across organisation and computer technology ‘silos’ to drive common approaches across the Trust enterprise network architecture.
3. Acting as champion for the department’s ITIL processes, providing professional guidance in and execution of Incident, Change, Release, Problem, Performance, and Availability Management.

**Organisational Chart**



**Specific Core Functions**

**Network Design and Hosting**

1. Working alone on complex network infrastructure and modifications to existing network components, or with partners, vendors or colleagues on enterprise systems. Specifies user/system technical requirements, including the overall management of the network implementation and transition into both the Operational Service and Data Centre.
2. Participate in projects including, but not limited to network design, product design, network expansions and Data Centre Scale outs.
3. Designs and completes detailed analysis of network solutions (fixed and wireless) which meet security standards and are resilient in the event of disaster.
4. Designs and executes network test plans, to verify correct operation of implementations.
5. Documents all work using required standards, methods and tools, including internal tools where appropriate.
6. Prepares and maintains operational documentation for relevant network equipment within the Trusts Data Centres. Advises other ICT staff on the correct and effect use of network related system software.
7. Collects network and application performance data to monitor new and existing services either against their published service level agreements or to aid in the defining of these service level agreements. Monitors both resource usage and failure rates of installed equipment and provides feedback to IT Operations Infrastructure Team.
8. Gathers performance statistics from the hosted network devices and application systems to enable recommendations for the tuning of applications and Infrastructure. Initiate network parameters to maximize throughput and efficiencies.
9. Provide the Infrastructure Architects with design support and implementation expertise required to aid in the successful deployment and transition of new services.

**Software and Hardware Installation**

1. Initiates network device software builds ready for loading onto the target hardware. Held within a configuration management standard arrangement, conducts a series of tests and records the details of any failures.
2. Installs or removes network hardware and/or software, using installation instructions and tools, follows agreed standards. Adheres to the ICT Change and Release Management Process for all software and hardware changes.
3. Reports details of all Core network related hardware/software items that have been installed and removed so that configuration management records can be updated.
4. Contributes, as required, to the development of installation procedures and standards.
5. Produces test specifications as required for testers to follow, carries out fault diagnosis relating to extreme complex problems as part of installations, reporting the results of the diagnosis in a clear and concise manner.
6. Adheres to the ICT Change and Release Management Process for all software and hardware changes.
7. Reports details of all network hardware/software items that have been installed and removed so that configuration management records can be updated.
8. Contributes, as required, to the development of installation procedures and standards.

**Infrastructure Developments/Innovation**

1. Contribute high-level specialist expertise to the development and innovation of network related technical strategies and wider ICT strategies as appropriate.
2. Manage the successful implementation of new or modified network elements within approved ICT development projects to meet project timescale and budgetary targets.
3. Keep abreast of ICT developments and technologies in order to effectively carry out the duties of the post and make recommendations for bringing benefits to our customers and improving service delivery.

**ITIL Processes**

**Change & Release Management**

1. Initiate the production of schedules of requests for change (RFC) for managing changes to the live infrastructure.
2. Initiate the provision of awareness material to customers and IT users to explain the purpose, impact and if required the risk assessment of technical changes.
3. Initiate the preparation of software and hardware implementation procedures with test plans, fall back contingency plans.
4. Installs and tests new versions of system software.

**Problem Management**

1. Conduct trend analysis resulting in the identification of complex faults within the Digital Infrastructure, create workarounds and implement a permanent fix to the root cause.
2. Conduct major problem reviews with the intention of identifying what went wrong, right and what can be done to improve the response in the future. Outcome of the review should also identify how to prevent the reoccurrence of the major problem.
3. Maintain the Digital Problem Management Information database, to demonstrate the effectiveness of the process, impact of the problem resolution, outstanding known errors, workaround, and contribution to the annual service improvement programme.
4. Advise and train other Digital operational staff on the best available workaround for incident resolution to known errors.

**Incident Management**

1. Following agreed procedures, provides advice on systems, and Digital services as part of the incident resolution.
2. Provides an effective interface between Digital Users and service providers, including external commercial suppliers where applicable.
3. Ensures incidents resolution are documented, external commercial supplier progress checking, and ensuring all relevant diagnosis information is provided to external commercial suppliers for error resolution and incident analysis.
4. Enables the Digital Operations Department in meeting the performance management programme by influencing the delivery model for meeting KPIs for incident management.
5. Provides information on updates and known errors to colleagues within Digital Operations.
6. Interprets highly complex technical or procedure manuals on behalf of non technical Digital Users and colleagues within Digital Operations.
7. Provides routine training for colleagues within Digital Operations in incident diagnosis, resolution, known solutions and changes in availability.

**Security**

1. Sets security policies and influences Digital Users in defining their needs for new access rights and privileges.
2. Analyse network traffic patterns and responds to security issues.
3. Provide advanced level technical support for network related security products.
4. Provides professional advice for enquires related to clinical information and personal information security.
5. Provides professional technology subject matter expertise advice to the department’s business contingency planning.

**Other**

1. Maintain personal and professional development to meet the changing demands of the job, participate in appropriate training activities and encourage and support staff development and training.
2. Participate in a Rota system for on-call services.
3. Provide cross matrix support across the three operational functions within Digital Operations, Operations Centre, Service Operations & Infrastructure Services.
4. Other tasks as directed by the Technical Delivery Manager.

**Key Responsibilities**

***Communication and Working Relationships***

* The post holder will be providing and receiving complex, sensitive or contentious information orally, in writing or electronically to inform work colleagues, patients, clients, carers, the public or other external contacts. The communication will include;

(a) Providing and receiving complex, sensitive or contentious routine information where persuasive, motivational, negotiating, training, empathic or re-assurance skills or where there are barriers to understanding

(b) providing and receiving complex or sensitive information,

**Analytical and Judgement**

* Judgements involving highly complex facts or situations, which require the analysis, interpretation, and comparison of a range of options.

***Planning and organising***

* Planning and organisation of a broad range of complex activities or programmes, some of which are ongoing, which require the formulation and adjustment of plans or strategies.

**Physical Skills**

* Developed physical skills, advanced keyboard use – accuracy important

***Patient Client Care***

* Incidental patient contact

***Policy and Service Development***

* The post holder will propose policy to service changes, impact beyond own area.

***Financial Management***

* Safe use of equipment other than equipment used personally

***Management/Leadership***

* The post holder is responsible for day-to-day supervision or co-ordination of staff within the Technical Delivery Team. They will deal with work allocation and daily responsibility for the monitoring or supervision of one or more groups of staff.

***Information Resources***

* The post holder is responsible for the management and development of information systems across the organisation as the major job responsibility.

***Research and development***

* Regularly undertake equipment testing, including applications and hardware
* Responsible, as an integral part of the job, for initiating (which may involve securing funding) and developing R&D programmes or activities, which support the objectives of the broader organisation.

***Freedom to Act***

* The post holder is guided by general health, organisational or broad occupational policies, but in most situations the post holder will need to establish the way in which these should be interpreted.

***Physical effort***

* A combination of sitting, standing, and walking with little requirement for physical effort. There may be a requirement to exert light physical effort for short periods.

***Mental effort***

* There is a frequent requirement for intense concentration.

***Emotional Effort***

* Exposure to distressing or emotional circumstances is rare, or occasional indirect exposure to distressing or emotional circumstances.

***Working conditions***

* Occasional exposure to unpleasant working conditions.

**Person Specification**

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** | **Essential** | **Desirable** | ***How criteria will be assessed*** |
| **Qualifications** | * Masters level qualification or equivalent in computer science or related field.
* Technical accreditation in at least two or more of the following; CCNA\CCNA Data Centre, CCNP, CCP-N, VCP.
* ITIL Foundation Certificate.
* Evidence of continuing professional development.
 | * PRINCE2 Practitioner Certificate.
* Cisco Certified Design Associate (CCDA).
* Cisco Certified Network Associate- Wireless (CCNAW)

OR Aruba Networking Associate Certified  | Application / Interview |
| **Experience**  | * At least five years experience working in a tiered, enterprise scale, Data Center network.
* Strong grasp of TCP/IP, routing, switching, and routing protocols including OSPF.
* Advanced knowledge of Cisco, Netscaler and Checkpoint hardware and software.
* Strong grasp of Load Balancers, and firewalls.
* Experience of VMware and Citrix virtualized networking or Aruba networking.
* In depth knowledge of virtualized Windows environments.
* Excellent understanding of Cisco Nexus technology.
* Advanced hands on configuration skills with network devices.
* Advanced troubleshooting of network connectivity and routing issues.
* Management of network Incidents.
* Management of Events and Alerts.
* Advanced technical management of escalations from teams and other departments.
* Advanced theoretical and enterprise knowledge across two or more information technology platforms: Database administration, Server Virtualisation, Desktop Virtualisation, Data & Voice Networking, Messaging, Storage Area Networks, Security, Mobility, Server & Peripheral Hardware.
* Significant experience of IT Service Management, Incident Management, Problem Management, Change
* Significant experience in leading highly complex technical problems to resolution, including managing external suppliers.
* Significant experience in project delivery of technical projects.
* Experience in assisting with report writing, being operating procedures, options appraisals, risk analysis, user guides.
 |  | Application / Interview |
| **Knowledge**  | * Solid in-depth experience of supporting, administering and designing enterprise networks
* Cisco CCNP/CCIE or Aruba CX
* Desktop and Server virtualisation technologies experience
* Must be able to demonstrate experience and high level knowledge of support, administration and design.
* Cisco core products including routing, switching, hardware, support, fibre.
* Working in Microsoft Active Directory Infrastructure environments and Microsoft Windows desktop operating systems and office application environments
* Storage technologies
* Working with Virtualisation Server & desktop technologies, preferably VMWare, HyperV & Citrix or Aruba CS..
* Network security and protection systems such as Extranet design, encryption, firewalls, certificates, mail & web filtering, AV, NAC.
* NAS / SAN storage infrastructures e.g. NetApp/EMC
* Deployment and use of monitoring tools (e.g. Solarwinds) for proactive infrastructure management
* Networking skills (switching, routing, VLANs, PoE, WLAN)
* Extensive knowledge of maintaining and troubleshooting networks
* Experience of building, managing and maintaining high availability networks with Cisco devices
* Experience of Checkpoint Firewalls, VPN and IPSec tunnel configuration and management
* Experience of implementing network monitoring solutions
* Experience of managing and maintaining load balancing equipment
 | * Experience of Cisco ASA, configuration and management
* Experience of Cisco APIC-EM and software defined networking
* Experience of Aruba CX
 | Application / Interview |

**Compliance statement to expected organisational standards.**

To comply with all Trust Policies and Procedure, with particular regard to

* Risk Management
* Health and Safety
* Confidentiality
* Data Quality
* Freedom of Information
* Equality Diversity and Inclusion
* Promoting Dignity at Work by raising concerns about bullying and harassment
* Information and Security Management and Information Governance
* Counter Fraud and Bribery

The Trust has designated the prevention and control of healthcare associated infection (HCAI) as a core patient safety issue. As part of the duty of care to patients, all staff are expected to:

Understand duty to adhere to policies and protocols applicable to infection prevention and control.

* Comply with key clinical care policies and protocols for prevention and control of infection at all time; this includes compliance with Trust policies for hand hygiene, standards (universal) infection precautions and safe handling and disposal of sharps.
* All staff should be aware of the Trust’s Infection Control policies and other key clinical policies relevant to their work and how to access them.
* All staff will be expected to attend prevention and infection control training, teaching and updates (induction and mandatory teacher) as appropriate for their area of work, and be able to provide evidence of this at appraisal.
* To perform your duties to the highest standard with particular regard to effective and efficient use of resources, maintaining quality and contributing to improvements.
* Ensure you work towards the Knowledge and Skills Framework (KSF) requirements of this post. KSF is a competency framework that describes the knowledge and skills necessary for the post in order to deliver a quality service.
* Your behaviour will demonstrate the values and vision of the Trust by showing you care for others, that you act professionally as part of a team and that you will continually seek to innovate and improve. Our vision, values and behaviours have been designed to ensure that everyone is clear about expected behaviours and desired ways of working in addition to the professional and clinical requirements of their roles.
* Ensure you adhere to and work within local and national safeguarding children legislation and policies including the Children Act 1989 & 2004 , Working Together to Safeguard Children 2013, 4LSCB guidance and the IOW Safeguarding Policy.
* Ensure you adhere to and work within the local Multiagency safeguarding vulnerable adults policies and procedures
* Ensure that you comply with the Mental Capacity Act and its Code of Practice when working with adults who may be unable to make decisions for themselves,
* Ensure that you maintain personal and professional development to meet the changing demands of the job, participate in appropriate training activities and encourage and support staff development and training.
* Respect the confidentiality of all matters that they may learn relating to their employment and other members of staff.  All staff are expected to respect conform to the requirements of the Data Protection Act 1998, including the responsibility to ensure that personal data is accurate and kept up to date
* If your employment is to a post that requires you to be registered with a professional body, the continuation of your employment is conditional upon you continuing to be registered with the appropriate professional body. The Trust will require evidence of current registration.
* Proactively, meaningfully and consistently demonstrate the Trust Values in your every day practice, decision making and interactions with patients and colleagues.
* Perform any other duties that may be required from time to time.
* Contribute to the IT Departments on-call rota and if required, maintain required skills, experience and resource levels allowing for hospital digital 24/7 services.

This job description may be altered, from time to time, to meet changing needs of the service, and will be reviewed in consultation with the post holder.