ICT Specialist – Network & Systems
Salary: R1 003 890 xv R1 182 534 per annum

(Ref. 2025/02/02)

Key purpose:

Responsible for administration (installations, setup, configurations and maintenance) of the Agency's networks, server-farm, computer systems, and computers applications. Implementation of Information Technology policies, Information Security mechanism and IT risk management.

Key output:

Network Design, update and maintain the Agency's IT Architecture (LANs, WANs, and wireless networks, including servers, routers, hubs, switches and other hardware); Integrate VOIP systems on the Agency network; Design and implement Server infrastructure; Monitors the server on a 24 hours basis; Make recommendation to management on the state of the ICT infrastructure; Lead network infrastructure projects and sub-projects in accordance with IT and project management frameworks and guidelines; Monitor and test network performance and provide network performance statistics and reports; Practice network asset management, including maintenance of network component inventory and related documentation and technical specifications information; Create and maintain documentation as it relates to network configuration, network mapping, processes, and service records; Practice network asset management, including maintenance of network component inventory and related documentation and technical specifications information; Provide 3rd line support

Systems Administration

Configuration and support of the Agency's website and Intranet; Configuration of SharePoint system; and Maintenance, creation of users and management of Exchange 2010 and AD.

Governance, Security and Planning

Assist in drafting of Standards, Policies to govern the IT function Involved in evaluation, planning, PoC, testing and implementation of various security related products such as representative on Microsoft Patch Council and role in patch management, approval, testing and distribution; Documentation of technical specifications and DR requirements; Ensure a project management approach to all activities is maintained; Provide technical assistance in the selection, configuration and maintenance of anti-virus, anti-spy ware, patch management and host-based protection of servers, workstations and network devices; Installation,

configuration and support on anti-virus, software to protect the Agency's data and systems; Plan design, implementation and support of new Technologies; Problem management; Backups of data and systems according to the approved Backup Policies and Procedures; Change management; Monitoring of events and alerts, as well as escalation and investigation around them; Perform root-cause analysis for all IT incidents and record on the Service Desk system; Develop, implement and maintain policies, procedures, and associated training plans for network administration, usage, and disaster recovery; Implement monitoring and improvement activities to ensure compliance with both internal security policies and applicable laws and regulations; Implement adequate IT security controls, processes and systems to ensure effective detection and management of IT security risks; Assume overall responsibility for setting policies, standards, procedures and guidelines to ensure the protection of the organization's information technology assets such as data, information, software, and hardware; Conduct research on network products, services, protocols, and standards to remain abreast of developments in the security industry.

Project Management

Delivery according to agreed project scope of work; Maintain high standard of project implementation; Follow up on users after projects were implemented; and ensure all assigned projects are completed within the Project SLA

Essential Knowledge, Skills, and Competencies Required

The incumbent must have the following competencies:

Experience with the following technologies: Thorough knowledge of Microsoft technologies, Windows Server 2008 or higher (design, Installation, configuration and admin), Active Directory and Exchange Server 2010 (design, Installation, configuration and admin), Disaster Recovery planning, implementation and testing, SharePoint, (Design, Installation, configuration and admin), Routers, Switches, (Design, Installation, configuration and admin), ISA/Forefront Firewalls, wireless technology, Thorough knowledge of VMware virtualization technology is essential, TCP/IP, DNS, DNS, WSUS and DHCP configuration, Knowledge of SAN devices (design, Installation, configuration and administration), Backup technologies, A good working knowledge of network vulnerability assessment and remediation, A good working knowledge of encryption mechanisms, Knowledge of Blade Server technologies; Must be able to stay abreast with latest ICT technologies and advice ICT and USAASA Management; Team player; Oral and written communication; Must be able to stay abreast of the latest IT technology; Knowledge of COBIT governance, ITIL service management, Project Management, SDLC, and Enterprise Architecture frameworks essential; Knowledge of Information Security Management and Risk Management; Code B driver's license; and Willingness to work abnormal hours, including weekends and public holidays.

Requirements:

- Matric
- NQF level 7 National Diploma or Degree in IT
- Specialization in Network Engineering or Computer Networking or Computer Software or computer Systems Engineering, enterprise architecture and IT Infrastructure management.
- CompTIA A+
- A+, N+, and MCSE 2008 with AD 2008 and Exchange Server 2007 or higher

- CCNA, CNE or IT related diploma will be advantageous
- ITIL V3 and Cobit Essentials
- Minimum of 4 to 7 years ICT experience in the whereby at least 4 years is in the similar role.

Closing Date: 14 March 2025

Please forward your applications and CV (with two recent referees) to **recruitment@usaasa.org.za** or hand deliver to Building 1, Thornhill Office Park, 94 Bekker Street, Vorna Valley, Midrand, 1685. To view the full advert visit **www.usaasa.org.za**

Enquiries: Sharonne Scheepers (Recruitment & Selection) Tel. (011 564 1653)

Note: Correspondence will be limited to short-listed candidates only. If you have not been contacted within 3 (three) months of the closing date of the advertisement, kindly regard your application as unsuccessful. Short-listed candidates must be prepared to consent and be subjected to necessary security vetting.