POSITION DESCRIPTION

Name:	Jorge Silveira
Commencement / Last Date Reviewed:	May 2019
Reviewed By:	Director Information Management / CIO
EBA:	Victorian Public Health Sector (Health & Allied Services, Managers & Administrative Workers) Single Enterprise Agreement 2016 - 2020

ORGANISATIONAL STRUCTURE

Position Title	**Role / Team**	**Area**	**Direct Reports**
Computer Network and Systems Engineer	ICT Operations & Cybersecurity	Information Management	NIL
Location	**EBA Classification**	**Reports To**	**Professional Accountability**
Wangaratta	HS2 - HS4	ICT Operations and Cybersecurity Team Leader	ICT Operations and Cybersecurity Team Leader

OUR VISION

To Be Recognised Leaders in Rural Health Care

OUR VALUES

CARING **EXCELLENCE** **RESPECT** **INTEGRITY** **FAIRNESS**

POSITION PURPOSE

The primary role of the **Computer Network and Systems Engineer** is to support Northeast Health Wangaratta (NHW) and partners with the provision of ICT infrastructure and cybersecurity services, Level 1 and Level 2 support as part of an ICT service management model.

The **Computer Network and Systems Engineer** plays a key role in responding to incidents and service requests in an effective, efficient and timely manner. The role is responsible for the supporting, monitoring and management of all ICT assets, their configuration, documentation, change management, commissioning and decommissioning. It includes patching, security, backups, disaster recovery, and compliance with regulations, standards and controls as per organisation policy.

The **Computer Network and Systems Engineer** will use a Service Management Tool to record, log time and respond to requests from users and to escalate calls as appropriate to deliver optimum service and meet established Service Level Agreements (SLAs) and Key Performance Indicators (KPIs).

The **Computer Network and Systems Engineer** will provide remote and on-site support for computer applications and hardware, including but not limited to desktop, tablets, phones, smart-phones, video conferencing units, duress, paging, smart TVs, data projectors, patient entertainment systems, CCTV, notebooks and will be included on the NHW out-of-hours roster.

Work includes a broad range of complex technical or professional activities, in a variety of contexts. The **Computer Network and Systems Engineer** investigates, defines and resolves complex issues, works under general direction within a clear framework of accountability, exercises substantial personal responsibility and autonomy and plans own work to meet given objectives and processes.

The role is essential in supporting a diverse range of Customer environments with the opportunity to participate in relevant projects subject to NHW's strategic and operational priorities.

RESPONSIBILITIES AND MEASURES OF SUCCESS IN THE ROLE

The following table breaks down the key performance areas of responsibility for the incumbent. Measurements for performance areas will be agreed to with the Reporting Manager

PERFORMANCE AREA	RESPONSIBILITY
Core Role	**Manage Solutions Identification and Build** - Evaluates new system software, reviews system software updates and identifies those that merit action. - Ensures that system software is tailored to facilitate the achievement of service objectives. - Plans the installation and testing of new versions of system software. Investigates and coordinates the resolution of potential and actual service problems. - Advises on the correct and effective use of system software. - Develop solution components progressively in accordance with detailed designs following development methods and documentation standards, quality assurance (QA) requirements, and approval standards. - Ensure that all control requirements in the business processes, supporting ICT applications and infrastructure services, services and technology products, and partners/suppliers are addressed. - Install and configure solutions and integrate with business process activities. - Implement control, security and audit ability measures during configuration, and during integration of hardware and infrastructural software, to protect resources, ensure availability and data integrity. - Update the services catalogue to reflect the new solutions. - Develop and execute a plan for the maintenance of solution and infrastructure components. Include periodic reviews against business needs and operational requirements **Manage Change Acceptance and Transitioning** - Prepare for business process, ICT service data, application and infrastructure migration as part of the organisation's development methods, including audit trails and a recovery plan should the migration fail. **Monitor infrastructure** - Monitor the infrastructure and related events. - Store sufficient chronological information in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations. - Maintain measures for protection against environmental factors. Install specialised equipment and devices to monitor and control the environment. **Manage Problems** - Investigate and diagnose problems using relevant subject management experts to assess and analyse root causes. - As soon as the root causes of problems are identified, create known-error records and an appropriate workaround, and identify potential solutions. - Identify and initiate sustainable solutions addressing the root cause, raising change requests via the established change management process if required to resolve errors. Ensure that the personnel affected are aware of the actions taken and the plans developed to prevent future incidents from occurring. **Manage Security Services** - Implement and maintain preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam). - Ensure that endpoints (e.g., laptop, desktop, server and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements of the information processed, stored or transmitted. - Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party. - Using intrusion detection tools, monitor the infrastructure for unauthorised access and ensure that any events are integrated with general event monitoring and incident management.

	Manage Operations - Co-ordinate and execute the activities and operational procedures required to deliver internal and outsourced applications and ICT services to the organisation, including the execution of pre-defined standard operating procedures and the required monitoring activities. **Manage Continuity** - Maintain availability of business-critical information (manage backup, business continuity and disaster recovery arrangements). **Manage Service Requests and Incidents** Perform service desk support activities as required. **General** - Perform other tasks as required.
	KPI - Adhere to the organisation values and demonstrates in every day actions and behaviours - Evaluation and testing for hardware and software follows a structure process, is documented and presented to management - Migration plans are developed, communicated and agreed with management, with clear process to rollback if required - ICT infrastructure is monitored and events actioned within timeframes specified by the organisation - Problems are clearly documented and followed through their resolution within timeframes specified by the organisation or its partners - ICT infrastructure is monitored for security vulnerabilities and remediated within timeframes specified by the organisation or its partners - Backup and disaster recovery activities are fully documented and up to date for each service provided to the organisation or its partners - Service Desk requests are attended to or escalated as per Service Level Agreements (SLAs), including the logging of all service desk requests - Maintain high level of confidentiality on all issues relating to the organisation, Customers and work colleagues - Treat everyone with respect & equality, whilst being responsive to their needs - Active contribution to Continuous System Improvement (CSI) activities - Keep infrastructure up to date with patching (within 1 month of approval) - Attendance to workshops as requested - Implementation and maintenance of DHHS/NIST Cybersecurity controls - 100% response to on-calls when rostered
Partnerships	- Provide ICT Service Desk services to NHW's partners as required
	KPI - Meet Service Level Agreement (SLA) Compliance Rate of 100%
Quality & Safety	- Prioritise requests with higher impact to clinical and corporate areas - Provide regular updates to achieve full resolution of issue
	KPI - High impact, high risk requests are prioritised over non-critical requests
Employee Obligations- OHS	- Participate in the development of a safe and healthy workplace. - Comply with instructions given for their own safety and health and that of others, in adhering to safe work procedures. - Co-operate with management in its fulfilment of its legislative obligations. - Take reasonable care to ensure their own safety and health and that of others, and to abide by their duty of care provided for in the legislation. - To report any injury, hazard or illness immediately, where practical to their supervisor. - Not place others at risk by any act or omission. - Not wilfully or recklessly interfere with safety equipment.

WORKING RELATIONSHIPS

INTERNAL
- NHW Staff Members
- NHW Contractors

EXTERNAL
- NHW partners
- Hume Rural Health Alliance
- Department of Health and Human Services

SPECIFIC SKILL REQUIREMENTS / QUALIFICATIONS / QUALITIES

Essential

- Can do attitude
- A high level of organisation, responsibility, self-motivation and personal commitment
- Information technology degree or substantial demonstrated experience
- ITIL Certification or demonstrated advanced knowledge of ITIL or COBIT processes
- Demonstrated experience with backup technologies such as Veeam and/or Commvault
- Demonstrated experience with Asset Management Tools, such as ForeScout
- Demonstrated experience migrating domain controllers to contemporary versions
- Demonstrated experience configuring firewalls/UTMs/Switches/Routers
- Demonstrated experience migrating Microsoft Exchange servers to contemporary versions
- Demonstrated experience with AD architecture and GPO deployment
- Minimum 3 years' experience in applications and ICT level 2/3 support - preferably in the Health industry
- Excellent interpersonal (written-verbal), customer service aptitude and negotiation skills
- Strong track record of managing client/end-user expectations and maintaining operational relationships
- Excellent documentation skills
- Experience with virtualization/remote access technologies such as VMware, Hyper-V, Citrix, Remote Desktop
- Experience using PowerShell
- Demonstrated experience with thin client deployment and management
- Strong ability to resolve complex problems and incidents
- Demonstrated experience in identifying and driving process continual improvement initiatives
- Ability to deal with high pressure situations and work under pressure
- Experience using a (ITIL) compliant Service management Tool and adhering to formalised change management controls
- Be part of an on-call roster

Desirable

- MCSA/MCSE or equivalent
- VMware Certification
- ITIL Certification
- Healthcare Experience
- CISCO Certification
- CISA / CSX Nexus Certification
- Understanding of Health Informatics

All staff must have and remain current for continued employment the following:
- A current National Police Check (renewed every 3 years)
- A current Working with Children Check (renewed every 5 years)
- Statutory Declaration for applicable workers who have lived overseas

Standards of Behaviour

	Above the line Our staff will always:	Below the line Our staff will not:
Caring	Show compassion to all people Demonstrate empathy and understanding Work as part of the team Mentor others Provide encouragement to others Care for others the way they would like to be cared for themselves	Be disrespectful Be self-centered Have inappropriate conversations with others Display rudeness
Excellence	Commit to the NHW Hardwiring Excellence expectations Have the courage to question what we do Persevere to do the best job they can Strive continuously to improve Be professional and enthusiastic Maintain customer focus	Give up Demonstrate a 'can't-do' attitude Accept mediocrity Be unreliable Pass the buck Ignore feedback given by patients or colleagues
Respect	Maintain confidentiality and privacy Listen to others and accept differences Be punctual Respond courteously Greet all people by saying hello, smiling and introducing themselves Be culturally informed and sensitive Respect diverse opinions	Be sarcastic Bully, harass or display aggression Be judgmental Withhold information Contribute to rumours Leave an untidy workplace
Integrity	Be open and honest Lead by example Be responsible and accountable for their own actions Stand up and take action Escalate issues or behaviors of concern	Be arrogant Be dishonest Be hypocritical Avoid responsibility Allow unacceptable behavior
Fairness	Demonstrate consistency Treat people equally Be considerate and understanding Be collaborative and collegiate	Discriminate against others Demonstrate favoritism and exclusion Refuse to assist others with their workload

Acknowledged By Employee

Name _____ Date _____

Signature _____