Technical Specifications

Support and Maintenance

1. Introduction

This document outlines the specifications for the provision of support and maintenance services for the networked environment at Sefateng. The service provider is expected to deliver comprehensive support to ensure continuous and reliable operation of network systems critical to the mining operations. The scope includes maintaining network infrastructure, hardware, and associated software systems.

2. Scope of Work

The service provider shall deliver the following services:

1. **Network Infrastructure Support:**
    - Support for routers, switches, firewalls, and wireless access points.
    - Regular monitoring and performance tuning of the network.
    - Configuration and change management.
2. **Server and Storage Support:**
    - Maintenance of physical and virtual servers, including updates and patch management.
    - Backup and disaster recovery management.
3. **End-User Support:**
    - Assistance with network connectivity issues for workstations, laptops, and other devices.
    - Support for network printing and shared resources.
4. **Software and Application Support:**
    - Maintenance of network-dependent applications, including updates and troubleshooting.

- Support for communication and collaboration tools.

5. **Security Management:**
    - Monitoring and management of network security devices.
    - Incident response and mitigation for network security events.

3. Service Level Agreement (SLA)

The following response times and time to repair targets must be met by the service provider:

Category	Response Time	Time to Repair	Remarks
Critical Systems	30 minutes	4 hours	Includes core network components affecting mining operations.
High Priority	1 hour	8 hours	Includes servers, storage systems, and business-critical applications.
Medium Priority	2 hours	16 hours	Includes non-critical applications, network peripherals, and user issues.
Low Priority	8 hours	48 hours	Minor issues not affecting core operations.

4. Contingency Planning

The service provider must develop and maintain a contingency plan to ensure minimal downtime for key systems. The plan should include:

1. **Redundancy and Failover Mechanisms:**
    - Implementation of redundant network paths for critical infrastructure.
    - Configuration of failover systems for servers and key applications.
2. **Disaster Recovery Planning:**
    - Regular backups and verification of restore procedures for critical data and configurations.

- Documentation of disaster recovery procedures, including roles and responsibilities.

3. **Business Continuity Planning:**
    - Identification of essential services and personnel required to maintain operations during outages.
    - Development of alternative communication channels and work arrangements.
4. **Testing and Validation:**
    - Scheduled testing of contingency plans at least annually.
    - Documentation of test results and corrective actions.

5. Reporting and Documentation

The service provider must maintain comprehensive documentation for the following:

1. **Network Architecture and Configuration:**
    - Up-to-date diagrams and configurations for all network components.
2. **Incident Reports:**
    - Detailed reports for each incident, including root cause analysis and corrective actions taken.
3. **Performance and Uptime Reports:**
    - Monthly reports on network performance, including uptime, response times, and resolution times.
4. **Change Management Records:**
    - Documentation of all changes made to the network, including approvals and implementation details.

6. Personnel Requirements

The service provider must assign qualified personnel with experience in managing complex networked environments, including:

1. **Network Engineers:**

- Certified professionals (e.g., Microsoft, CompTIA) with experience in network design and troubleshooting.

2. **System Administrators:**
   - Experienced in server management, virtualization, and storage systems.
3. **Support Technicians:**
   - Skilled in providing end-user support and resolving hardware and software issues.

7. Health, Safety, and Environmental Compliance

The service provider must adhere to all health, safety, and environmental regulations specific to the mining industry. This includes:

1. **Site Safety Training:**
   - Mandatory training for all personnel before commencing work on-site.
2. **Safety Equipment:**
   - Provision of necessary personal protective equipment (PPE) for all personnel.
3. **Environmental Considerations:**
   - Adherence to regulations regarding electronic waste disposal and minimization of environmental impact.

8. Evaluation Criteria

The tender submissions will be evaluated based on the following criteria:

1. **Technical Capability:**
   - Demonstrated experience in managing similar environments.
2. **Response and Repair Times:**
   - Ability to meet or exceed the SLA requirements.
3. **Contingency Planning:**
   - Robustness and completeness of the proposed contingency plans.
4. **Cost:**

- Competitive pricing in line with the scope of services provided.

5. **Compliance:**
    - Adherence to industry standards and regulatory requirements.

9. Submission Requirements

All submissions must include:

1. **Company Profile and Experience:**
    - Overview of the company, including past projects relevant to the mining sector.
2. **Technical Proposal:**
    - Detailed description of the approach to delivering the services outlined in this document.
3. **Financial Proposal:**
    - Breakdown of costs, including any optional services and associated fees.
4. **References:**
    - Contact information for at least three clients with similar environments.

10. Conclusion

The selected service provider will play a crucial role in ensuring the stability and efficiency of Sefateng's networked environment. Their ability to provide high-quality support and proactive maintenance is vital to the ongoing success of mining operations.