Registration number: LR2/6/6/1
275 Kent Avenue, Ferndale, Randburg 2125
PO Box 2578, Randburg
+27 (0) 861 664 226
www.mibco.org.za

REQUEST FOR PROPOSAL (RFP)

FULLY MANAGED SECURE NETWORK AND CYBERSECURITY SERVICE (SNAAS)

Including

- Next Generation Firewall (NGFW)
- Secure SD-WAN
- Zero Trust Network Access (ZTNA)
- Security Service Edge (SSE)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)
- Remote Browser Isolation (RBI)
- User and Entity Behaviour Analytics (UEBA)
- Hybrid Data Centre and Azure Security
- Managed Security Services

RFP REFERENCE NUMBER

MIBCO/ICT/2026/007

ISSUE DATE

28 July 2026

CLOSING DATE

28 August 2026 **Extended to 11 September 2026**

CONTRACT PERIOD

36 Months

1. INTRODUCTION

The Motor Industry Bargaining Council (MIBCO) hereby invites suitably qualified service providers to submit proposals for the provision of a Fully Managed Secure Network and Cybersecurity Service.

MIBCO is seeking a strategic technology partner capable of designing, implementing, supporting and operating a modern enterprise cybersecurity and secure networking platform on a managed service basis.

The proposed solution shall replace MIBCO's existing Cisco Meraki security and SD-WAN environment which has reached end-of-life and shall provide enhanced cybersecurity, secure connectivity, Zero Trust capabilities and regulatory compliance support.

The successful bidder shall assume responsibility for the ongoing operation, maintenance, support, lifecycle management and continuous improvement of the solution during the contract term.

MIBCO's objective is to procure security and connectivity outcomes rather than individual technology products.

2. BACKGROUND

The Motor Industry Bargaining Council (MIBCO) is a bargaining council as envisaged in the Labour Relations Act, with the mission to create and maintain peace and stability within the South African motor industry.

MIBCO provides services to approximately 21,000 employers and over 300,000 employees operating within the South African motor industry.

MIBCO currently employs approximately 340 employees and operates nationally through a network of regional and satellite offices.

MIBCO has adopted the NIST Cyber Security Framework as its primary cybersecurity framework and operates an internal Security Operations Centre (SOC).

The organisation is increasingly dependent on:

- Cloud services
- Remote work capabilities
- Secure third-party access
- Secure digital services
- Cybersecurity resilience
- Compliance with regulatory requirements

As a result, MIBCO requires a modern, scalable and secure networking and cybersecurity platform capable of supporting current and future business requirements.

3. CURRENT ENVIRONMENT

Site Distribution

Site Type	Quantity
Main Offices	6
Satellite Offices	15
Total Sites	21

User Population

User Category	Number
Employees	324
Contractors and Third Parties	90
Potential Remote Users	324
Concurrent Remote Access Users	329

Branch Distribution

Location	Users
Randburg	125
Cape Town	45
Pretoria	45
Pinetown	50
Port Elizabeth	23
Bloemfontein	21
Remaining Branches	1–2 Users Each

Current Network Infrastructure

Existing Firewall Platform

- Cisco Meraki MX67
- Cisco Meraki MX100
- Cisco Meraki MX105

Existing Services

- Cisco Meraki SD-WAN
- Cisco Meraki Secure Connect
- Fibre WAN Connectivity
- Local Internet Breakout at All Branches

Current Microsoft Environment

Identity

- Microsoft Entra ID

Endpoint Management

- Microsoft Intune

Endpoint Security

- Microsoft Defender for Endpoint

Disaster Recovery

- Microsoft Azure South Africa

Current Security Operations Environment

SOC Platforms

- Wazuh
- Grafana
- Ollama
- N8N

4. CURRENT ARCHITECTURE

Production Environment

MIBCO operates a primary physical data centre located in Randburg.

This facility hosts:

- Core Business Applications
- Authentication Services
- Infrastructure Services
- Management Services
- Security Services
- Operational Databases

The Randburg data centre serves as MIBCO's primary production environment.

Disaster Recovery Environment

MIBCO maintains a Disaster Recovery environment hosted within Microsoft Azure South Africa.

The Azure environment supports:

- Disaster Recovery Services
- Application Recovery
- Infrastructure Recovery
- Business Continuity Services
- Secure Replication

Architecture Requirement

The proposed solution shall support a hybrid architecture consisting of:

- Randburg Data Centre
- Azure Disaster Recovery Environment
- Regional Offices
- Satellite Offices
- Remote Employees
- Third-Party Users

Solutions relying solely on cloud-delivered security controls without appropriate protection of the physical data centre environment may be rejected.

5. PROJECT OBJECTIVES

The objectives of this procurement are to:

Modernise Infrastructure

Replace the existing end-of-life Cisco Meraki environment.

Improve Cybersecurity

Reduce organisational cyber risk through modern cybersecurity controls.

Implement Zero Trust

Implement identity centric Zero Trust security principles.

Improve Visibility

Enhance monitoring, reporting and threat visibility.

Improve Compliance

Support MIBCO's regulatory and governance obligations.

Improve Security Operations

Enhance integration with the MIBCO Security Operations Centre.

Improve User Experience

Provide secure and reliable connectivity for branch, mobile and remote users.

Support Hybrid Architecture

Provide consistent security controls across:

- Physical Data Centre
- Azure Disaster Recovery Environment
- Branch Offices
- Remote Workforce

Support Future Growth

Provide a scalable architecture capable of supporting future business requirements.

6. RFP OBJECTIVES

The successful bidder shall provide a fully managed service including:

Design

- Discovery Workshops
- Solution Design
- Security Architecture Design
- Migration Planning

Supply

- Hardware

- Software
- Licensing
- Subscriptions

Implementation

- Installation
- Configuration
- Testing
- Migration

Operations

- Monitoring
- Maintenance
- Incident Management
- Problem Management
- Change Management

Support

- OEM Support
- Vendor Management
- Escalation Management
- Service Reporting

Lifecycle Management

- Firmware Updates
- Software Updates
- Security Updates
- Hardware Replacement
- Technology Refresh

7. CONTRACTING MODEL

Mandatory Contracting Requirement

This procurement shall be based on a fully managed Security Network as a Service (SNaaS) model.

MIBCO is procuring a business outcome and managed service and not solely hardware or software components.

The service provider shall be responsible for the design, implementation, support and operation of the proposed solution throughout the contract period.

Ownership of hardware may remain with the service provider provided that all contractual obligations and service level requirements are met.

8. MODULAR PROCUREMENT MODEL

Procurement Principle

MIBCO reserves the right to procure the solution in phases based on available budget, organisational priorities and strategic requirements.

The proposed architecture must therefore be modular, scalable and capable of incremental expansion without redesign.

All costs shall be separated into modules.

Phase 1 – Core Foundation

Mandatory Security and Networking Platform

Includes:

- NGFW
- SD-WAN
- IPS
- IDS
- Malware Protection
- DNS Security
- Azure Integration
- Reporting Platform

Phase 2 – Zero Trust

Includes:

- ZTNA
- Device Posture Assessment
- Identity-Based Controls
- Contractor Access Controls
- Just-In-Time Access

Phase 3 – Security Service Edge

Includes:

- Secure Web Gateway
- CASB
- Remote Browser Isolation

Phase 4 – Advanced Security Controls

Includes:

- Data Loss Prevention
- UEBA
- AI-Assisted Security Analytics
- Advanced Threat Protection

Modular Pricing Requirement

Bidders shall provide individual pricing for every module.

MIBCO reserves the right to:

- Award all modules.
- Award selected modules.
- Defer modules.
- Implement modules during future budget periods.

Failure to provide modular pricing may result in disqualification.

9. SCOPE OF WORK

9.1 Overview

MIBCO requires a suitably qualified service provider to design, supply, implement, migrate, operate, manage, maintain and continuously improve a fully managed Secure Network and Cybersecurity Service (SNaaS) across all MIBCO locations.

The successful bidder shall assume full accountability for delivering a secure, resilient, scalable and highly available solution that supports MIBCO's business operations, cybersecurity objectives, regulatory obligations and future growth requirements.

The proposed solution shall replace the existing Cisco Meraki environment and provide a modern enterprise architecture capable of supporting:

- Physical Data Centre operations.
- Microsoft Azure Disaster Recovery operations.

- Branch connectivity.
- Remote users.
- Contractor access.
- Zero Trust security controls.
- Advanced cybersecurity capabilities.
- Future modular expansion.

The service provider shall provide all resources, skills, technologies, software, subscriptions, hardware, implementation services and support services necessary to deliver the required outcomes.

9.2 Existing Environment Migration

The successful bidder shall perform a complete migration from the existing Cisco Meraki environment.

The migration shall include but not be limited to:

Existing Infrastructure

- Cisco Meraki MX67
- Cisco Meraki MX100
- Cisco Meraki MX105
- Cisco Meraki SD-WAN
- Cisco Meraki Secure Connect

Migration Activities

The bidder shall:

- Conduct a detailed discovery and assessment of the current environment.
- Document the existing architecture.
- Document all existing firewall policies.
- Document all SD-WAN configurations.
- Document all VPN configurations.
- Document all Internet breakout configurations.
- Document all security policies.
- Document all routing configurations.
- Document all Azure connectivity configurations.

The bidder shall provide:

- Migration Strategy.
- Detailed Migration Plan.
- Migration Runbook.
- Testing Plan.
- User Acceptance Testing Plan.
- Cutover Plan.
- Rollback Plan.
- Hypercare Support Plan.

No migration activity shall take place without approved rollback procedures.

9.3 Network and Security Architecture Design

The successful bidder shall perform a complete architecture review and design exercise.

The design shall include:

Current State Assessment

- Network Infrastructure
- Security Infrastructure
- Branch Connectivity
- Internet Connectivity
- Azure Connectivity
- Identity Services
- Remote Access Services
- Third-Party Access

Future State Design

The future architecture shall include:

- Secure SD-WAN
- Next Generation Firewall
- Zero Trust Architecture
- Secure Cloud Integration
- Security Service Edge Components

- Disaster Recovery Integration
- Security Monitoring Integration

The bidder shall provide:

- High-Level Design (HLD)
- Low-Level Design (LLD)
- Security Architecture Diagram
- Logical Architecture Diagram
- Physical Architecture Diagram
- Azure DR Architecture Diagram
- Branch Architecture Diagram

9.4 Data Centre Security Services

The successful bidder shall secure MIBCO's primary Data Centre located in Randburg.

The solution shall provide:

Perimeter Protection

- Next Generation Firewalling
- Layer 7 Security Controls
- Intrusion Prevention
- Intrusion Detection
- Malware Protection
- DNS Security
- URL Filtering

Internal Security Controls

- East-West Traffic Inspection
- Internal Segmentation
- Identity-Based Segmentation
- DMZ Protection
- Administrative Network Segmentation

Data Centre Segmentation

The solution shall support segmentation of:

Network Zone	Required
Users	Yes
Servers	Yes
Domain Controllers	Yes
Management Networks	Yes
Backup Infrastructure	Yes
Storage Networks	Yes
DMZ	Yes
Guest Networks	Yes
Security Tooling	Yes

9.5 Azure Disaster Recovery Security Services

The successful bidder shall provide integrated security services for MIBCO's Microsoft Azure South Africa Disaster Recovery environment.

The solution shall support:

Azure Connectivity

- Azure Virtual WAN
- Azure VPN Gateway
- Site-to-Site VPN
- Route Integration
- Secure Replication

Azure Security Controls

- Security Policy Extension
- Azure Workload Visibility
- Azure Segmentation
- Secure DR Connectivity
- DR Access Control

Consistent Security Controls

The solution shall ensure that security policies can be consistently applied across:

- Randburg Data Centre
- Azure DR Environment
- Branch Offices
- Remote Users

9.6 Secure SD-WAN Services

The bidder shall provide a fully integrated Secure SD-WAN solution.

The solution shall support all MIBCO locations.

Core Requirements

- Application Aware Routing
- Dynamic Path Selection
- SLA-Based Routing
- WAN Optimisation
- Path Monitoring
- Link Monitoring
- Local Internet Breakout

Connectivity Requirements

The solution shall support:

- Branch to Branch Connectivity
- Branch to Data Centre Connectivity
- Branch to Azure Connectivity
- Branch to Internet Connectivity

The architecture shall support future branch additions without fundamental redesign.

9.7 Zero Trust Network Access (ZTNA)

The bidder shall provide a comprehensive Zero Trust access solution.

The solution shall replace traditional VPN-based remote access wherever possible.

Mandatory Capabilities

- Identity-Based Access

- Continuous Verification
- Device Trust Validation
- Least Privilege Access
- Context-Aware Access Controls
- Risk-Based Access Controls

Microsoft Integration

The solution shall integrate with:

- Microsoft Entra ID
- Microsoft Active Directory
- Conditional Access
- Microsoft MFA
- Microsoft Intune

Device Posture Validation

The solution shall validate:

- Defender Status
- Real-Time Protection Status
- Malware Signature Currency
- BitLocker Encryption Status
- Intune Compliance
- Operating System Patch Status

9.8 Third-Party Access Services

The successful bidder shall provide secure access controls for approximately ninety (90) contractors and third-party users.

The solution shall support:

- Contractor-Specific Access Controls
- Application-Based Access
- Time-Limited Access
- Approval-Based Access
- Just-In-Time Access

- Access Monitoring
- Session Recording
- Session Logging

9.9 Security Service Edge (SSE) Services

The solution shall include Security Service Edge capabilities.

Secure Web Gateway (SWG)

The solution shall provide:

- URL Filtering
- Web Threat Protection
- SSL Inspection
- Category Controls
- Malware Prevention

Cloud Access Security Broker (CASB)

The solution shall provide:

- SaaS Visibility
- SaaS Risk Assessment
- Shadow IT Discovery
- SaaS Governance Controls

Remote Browser Isolation (RBI)

The solution shall provide:

- Browser Isolation
- Unknown Website Isolation
- High-Risk Website Isolation

9.10 Data Loss Prevention Services

The proposed solution shall include Data Loss Prevention capabilities.

DLP controls shall support:

- Web Traffic
- Email Traffic
- SaaS Applications

- Microsoft 365
- Azure Storage
- Endpoint DLP Requirements

The bidder shall describe:

- DLP Detection Methods
- DLP Policy Framework
- DLP Reporting Capabilities
- DLP Incident Management

9.11 User and Entity Behaviour Analytics (UEBA)

The bidder shall provide behaviour analytics capabilities.

The solution shall support:

- User Behaviour Analytics
- Entity Behaviour Analytics
- Insider Threat Detection
- Anomaly Detection
- Risk Scoring
- Behaviour-Based Alerting

9.12 Security Operations Centre Integration

The proposed solution shall integrate with MIBCO's Security Operations Centre.

Existing Platforms

The solution shall support integration with:

- Wazuh
- Grafana
- Ollama
- N8N

Integration Methods

The solution shall support:

- REST APIs
- Syslog

- JSON
- Webhooks
- STIX/TAXII

Security Operations Requirements

The solution shall support:

- Incident Response
- Threat Intelligence Integration
- Threat Hunting
- Automated Workflows
- Security Orchestration

9.13 Reporting and Dashboard Requirements

The successful bidder shall provide comprehensive reporting capabilities.

Minimum reporting requirements include:

Executive Reporting

- Security Posture Reports
- Risk Exposure Reports
- Compliance Reports
- Service Availability Reports

Operational Reporting

- Incident Reports
- Threat Reports
- Capacity Reports
- Utilisation Reports

Technical Reporting

- Security Events
- Threat Prevention Statistics
- Policy Change Reports
- Device Health Reports

Reports shall be available on-demand and through scheduled delivery.

9.14 Managed Services

The successful bidder shall provide a fully managed service.

Minimum managed services shall include:

Monitoring

- 24x7 Monitoring
- Health Monitoring
- Performance Monitoring
- Security Monitoring

Service Management

- Incident Management
- Problem Management
- Change Management
- Configuration Management

Lifecycle Management

- Firmware Upgrades
- Security Updates
- Patch Management
- License Management

Vendor Management

- OEM Escalations
- Warranty Management
- Technology Roadmap Reviews

9.15 Training and Knowledge Transfer

The bidder shall provide:

Training

- Administrator Training
- Operations Training
- Security Operations Training

Knowledge Transfer

- Architecture Walkthroughs
- Operational Procedures
- Support Procedures

Documentation

- High-Level Design
- Low-Level Design
- As-Built Documentation
- Configuration Documentation
- Operating Procedures

9.16 Deliverables

The successful bidder shall deliver, at minimum:

Project Deliverables

- Project Charter
- Project Plan
- Risk Register
- Communications Plan

Technical Deliverables

- High-Level Design
- Low-Level Design
- Security Architecture
- Migration Plan
- Rollback Plan

Operational Deliverables

- Support Procedures
- Escalation Procedures
- Service Reporting Templates
- SLA Documentation

Completion Deliverables

- As-Built Documentation

- Training Material
- Knowledge Transfer Documentation
- Operational Acceptance Report
- Project Closure Report

9.17 Future Expansion Requirements

The proposed solution shall support future expansion of:

- Branch Offices
- Remote Users
- Contractors
- Security Services
- Bandwidth Requirements
- Cloud Services

The bidder shall provide pricing schedules allowing MIBCO to expand the environment in future budget periods without requiring replacement or redesign of the core architecture.

10. TECHNICAL REQUIREMENTS

10.1 General Technical Requirements

The proposed solution shall be an enterprise-grade platform suitable for a nationally distributed organisation operating within a regulated environment.

The solution shall support:

- 21 sites.
- 324 employees.
- 90 contractors and third-party users.
- 329 concurrent remote access users.
- Randburg Primary Data Centre.
- Microsoft Azure Disaster Recovery Environment.
- Future growth in users, sites and services.

The proposed architecture shall be designed for a minimum operational lifespan of five (5) years without requiring fundamental redesign.

The bidder shall provide a detailed architecture demonstrating:

- Current state assumptions.

- Proposed target architecture.
- Data Centre architecture.
- Azure DR architecture.
- Branch architecture.
- Remote access architecture.
- Security architecture.
- Management architecture.

10.2 Solution Architecture Requirements

The proposed solution shall provide a unified architecture incorporating:

- Next Generation Firewall.
- Secure SD-WAN.
- Zero Trust Network Access.
- Security Service Edge.
- Threat Prevention.
- Identity-Based Security.
- Security Operations Integration.

The proposed architecture shall:

- Minimise complexity.
- Minimise management overhead.
- Provide central management.
- Support future expansion.
- Support integration with Microsoft technologies.

The architecture shall support:

Architecture Component	Required
Randburg Data Centre Security	Yes
Azure DR Security	Yes
Branch Security	Yes
Mobile Workforce Security	Yes

Contractor Security	Yes
Centralised Policy Management	Yes
Centralised Logging	Yes
Centralised Reporting	Yes

10.3 Next Generation Firewall (NGFW) Requirements

The proposed solution shall provide enterprise-class Next Generation Firewall functionality.

Firewall Controls

Mandatory features:

- Stateful inspection.
- Layer 3 firewalling.
- Layer 4 firewalling.
- Layer 7 firewalling.
- Deep packet inspection.
- Application-aware policies.
- User-aware policies.
- Identity-aware policies.
- Dynamic Access Control.
- Policy-based routing.

Application Visibility

The solution shall provide:

- Real-time application visibility.
- Application classification.
- Application risk scoring.
- Application-based enforcement.
- Application reporting.

10.4 Threat Prevention Requirements

The solution shall provide integrated threat prevention capabilities.

Mandatory Threat Prevention Features

- Intrusion Prevention System (IPS).
- Intrusion Detection System (IDS).
- Anti-Malware Protection.
- Anti-Ransomware Protection.
- Botnet Protection.
- Command and Control Protection.
- Exploit Prevention.
- Threat Intelligence Integration.
- Advanced Threat Protection.

Threat Prevention Requirements

The bidder shall describe:

- Detection methodology.
- Prevention methodology.
- Update frequency.
- Global threat intelligence capabilities.
- AI-assisted threat detection capabilities.

10.5 SSL/TLS Inspection Requirements

The proposed solution shall provide SSL/TLS inspection capabilities.

Mandatory Support

- TLS 1.3 inspection.
- Inbound SSL inspection.
- Outbound SSL inspection.
- Selective SSL bypass.
- Certificate-based controls.

Performance Requirements

The bidder shall provide verified throughput figures for:

- Firewall throughput.
- Threat prevention throughput.

- SSL inspection throughput.

The quoted figures shall be based on real-world security services enabled.

Marketing throughput figures will not be accepted.

10.6 Secure SD-WAN Requirements

The proposed solution shall provide fully integrated Secure SD-WAN capabilities.

SD-WAN Features

Mandatory capabilities:

- Dynamic path selection.
- WAN path monitoring.
- Link quality monitoring.
- Packet loss monitoring.
- Latency monitoring.
- Jitter monitoring.
- Application-aware routing.
- SLA-based routing.
- Automatic failover.
- Traffic steering.

Branch Requirements

The solution shall support:

- Main offices.
- Satellite offices.
- Branch expansion.
- Local Internet breakout.

WAN Connectivity

The proposed solution shall support:

- Fibre connectivity.
- IPSEC connectivity.
- Secure branch-to-branch communication.
- Branch-to-Data Centre communication.

- Branch-to-Azure communication.

10.7 Zero Trust Network Access (ZTNA) Requirements

The proposed solution shall provide Zero Trust Network Access capabilities.

Mandatory Capabilities

- Identity-based access.
- Device-based access.
- Application-based access.
- Context-aware access.
- Continuous verification.
- Continuous trust evaluation.
- Least privilege access.
- Risk-based access controls.

Authentication Integration

Mandatory support:

- Microsoft Entra ID.
- Multi-Factor Authentication (MFA).
- Conditional Access.
- Single Sign-On (SSO).

Remote Access

The solution shall support:

- Remote employees.
- Contractors.
- Third-party suppliers.
- Mobile users.

The bidder shall describe how traditional VPN reliance will be reduced through ZTNA capabilities.

10.8 Device Posture Assessment Requirements

The proposed solution shall support device trust verification.

Mandatory Validation Controls

The solution shall validate:

- Microsoft Defender operational status.
- Real-time protection status.
- Malware signature currency.
- BitLocker status.
- Intune compliance.
- Domain membership.
- Operating system patch compliance.

Preferred Controls

The solution should support:

- Secure Boot validation.
- TPM validation.
- Device Risk Scoring.

10.9 Identity and Access Management Requirements

The solution shall support identity-centric security controls.

Mandatory Integration

- Microsoft Entra ID.
- Microsoft Active Directory
- Microsoft Conditional Access.
- Microsoft MFA.
- Microsoft Intune.

Mandatory Identity Features

- Role-based access control.
- Granular permissions.
- Dynamic access policies.
- User risk evaluation.
- Device risk evaluation.
- Access auditing.

10.10 Security Service Edge (SSE) Requirements

The proposed solution shall support Security Service Edge services.

Secure Web Gateway (SWG)

Mandatory capabilities:

- URL filtering.
- Content filtering.
- SSL inspection.
- Malware inspection.
- Acceptable-use enforcement.

Cloud Access Security Broker (CASB)

Mandatory capabilities:

- SaaS visibility.
- Shadow IT detection.
- SaaS risk assessment.
- Application governance.
- SaaS access controls.

Remote Browser Isolation (RBI)

Mandatory capabilities:

- Browser isolation.
- High-risk website isolation.
- Malware isolation.
- Safe browsing enforcement.

10.11 Data Loss Prevention (DLP) Requirements

The proposed solution shall provide integrated Data Loss Prevention capabilities.

Data Protection Scope

The solution shall support:

DLP Area	Required
Web Traffic	Yes
Email Traffic	Yes
SaaS Applications	Yes

Microsoft 365	Yes
Azure Storage	Yes
Endpoint DLP	Yes

Data Classification

The solution should support:

- Personal Information.
- Financial Information.
- Confidential Information.
- Custom Data Types.

Incident Response

The solution shall support:

- Alerting.
- Blocking.
- Quarantine.
- Workflow escalation.
- Incident reporting.

10.12 User and Entity Behaviour Analytics (UEBA)

The proposed solution shall provide behaviour analytics capabilities.

Mandatory Features

- User behaviour monitoring.
- Entity behaviour monitoring.
- Risk scoring.
- Behavioural baselines.
- Anomaly detection.
- Threat detection.

Detection Use Cases

The solution shall support detection of:

- Insider threats.

- Account compromise.
- Privilege abuse.
- Unusual access patterns.
- Suspicious data movement.

10.13 Micro-Segmentation Requirements

The solution shall support internal segmentation and Zero Trust segmentation principles.

Network Segmentation Requirements

The following network zones shall be capable of being independently secured:

Security Zone	Required
User Networks	Yes
Server Networks	Yes
Domain Controllers	Yes
Backup Infrastructure	Yes
Storage Systems	Yes
VoIP Infrastructure	Yes
Management Networks	Yes
DMZ Networks	Yes
Guest Networks	Yes
Security Platforms	Yes

Identity-Based Segmentation

The solution shall support:

- User-based segmentation.
- Group-based segmentation.
- Role-based segmentation.
- Dynamic segmentation.
- Policy-driven segmentation.

10.14 Logging and Reporting Requirements

The solution shall provide comprehensive logging capabilities.

Logging Requirements

The solution shall log:

- Security events.
- Firewall events.
- Authentication events.
- Administrative actions.
- Configuration changes.
- Access control activity.
- Threat prevention activity.

Retention Requirements

Requirement	Duration
Online Log Retention	30 Days
Archived Log Retention	5 Years

Export Requirements

The solution shall support:

- Syslog.
- API export.
- Webhooks.
- SIEM integration.

10.15 Security Operations Integration Requirements

The solution shall integrate with the following platforms:

SOC Environment

- Wazuh.
- Grafana.
- Ollama.
- N8N.

Integration Methods

Mandatory support:

- REST APIs.
- JSON.
- Syslog.
- Webhooks.
- STIX/TAXII.

SOC Capabilities

The solution shall enable:

- Security monitoring.
- Threat hunting.
- Security orchestration.
- Automated workflows.
- Incident response.

10.16 Administration and Management Requirements

The proposed solution shall provide centralised management.

Mandatory Administrative Features

- Single management interface.
- Role-based administration.
- Multi-factor authentication.
- Single sign-on.
- Just-in-Time administration.
- Privileged Access Management integration.
- Audit trails.

Audit Requirements

Audit logs shall include:

- Administrative activities.
- Policy changes.
- User activities.

- Configuration modifications.
- System events.

Audit logs shall be immutable and tamper resistant.

10.17 Performance Requirements

The proposed solution shall support the following minimum performance requirements.

Data Centre Requirements

Requirement	Minimum
Internet Bandwidth	2 Gbps
Security Inspection Throughput	1 Gbps
Threat Prevention Throughput	1 Gbps
SSL Inspection Throughput	1 Gbps

Performance Validation

The bidder shall provide:

- Product datasheets.
- Independent performance validation.
- Published throughput figures.
- Throughput with applicable security services enabled.

10.17.1 Performance Benchmark Requirements

Purpose

To ensure fair and objective comparison of vendor responses, all performance figures submitted by bidders shall be based on measurable, real-world operating conditions and not on theoretical, laboratory or marketing throughput values.

The bidder shall clearly state the test methodology, assumptions and feature sets enabled during benchmarking.

MIBCO reserves the right to request independent verification of any quoted performance figures.

Performance Testing Principles

All quoted performance figures shall be based on the following security services being enabled simultaneously:

- Application Control
- Intrusion Prevention System (IPS)

- Anti-Malware
- Threat Prevention
- DNS Security
- SSL/TLS Inspection
- URL Filtering
- Logging
- Reporting

The solution shall not be benchmarked using basic packet forwarding or firewall-only throughput.

Data Centre Performance Benchmarks

Minimum Performance Requirements

Performance Metric	Minimum Requirement
Stateful Firewall Throughput	5 Gbps
NGFW Throughput	2 Gbps
Application Control Throughput	2 Gbps
Threat Prevention Throughput	1 Gbps
SSL/TLS Inspection Throughput	1 Gbps
IPS Throughput	1 Gbps
IPSEC VPN Throughput	1 Gbps
Concurrent Sessions	2,000,000
New Sessions per Second	50,000
Site-to-Site VPN Tunnels	100
Remote Access Sessions	500

Design Requirement

The proposed platform shall be sized at no less than:

- 30% growth capacity.
- 30% bandwidth growth.
- 30% user growth.

The proposed architecture shall not exceed 70% average utilisation under normal operating conditions.

Branch Appliance Performance Benchmarks

Main Regional Offices

Applies to:

- Randburg
- Pretoria
- Cape Town
- Pinetown
- Port Elizabeth
- Bloemfontein

Minimum requirements:

Performance Metric	Minimum Requirement
NGFW Throughput	1 Gbps
Threat Prevention	500 Mbps
SSL Inspection	500 Mbps
SD-WAN Throughput	1 Gbps
IPSEC Throughput	500 Mbps

Small Branch Offices

Minimum requirements:

Performance Metric	Minimum Requirement
NGFW Throughput	200 Mbps
Threat Prevention	100 Mbps
SSL Inspection	100 Mbps
SD-WAN Throughput	200 Mbps

Secure Remote Access Benchmarks

The solution shall support:

Requirement	Minimum
Concurrent Remote Users	329
Contractor Users	90
Simultaneous ZTNA Sessions	500
MFA Transactions	Unlimited
Device Posture Assessments	Real Time

The bidder shall confirm whether additional infrastructure is required to support growth beyond these values.

Azure Disaster Recovery Performance Benchmarks

The solution shall support:

Requirement	Minimum
Site-to-Site Connectivity	1 Gbps
Replication Traffic Inspection	1 Gbps
Failover Security Inspection	1 Gbps
Security Policy Replication	Real Time
Log Synchronisation	Real Time

The bidder shall provide evidence of successful deployment of the proposed architecture within Microsoft Azure.

Logging Performance Benchmarks

The solution shall support:

Requirement	Minimum
Log Retention Online	30 Days
Log Archive Retention	5 Years
Security Event Processing	10,000 EPS
Log Export Delay	Less than 1 Minute
Dashboard Refresh Interval	Less than 60 Seconds

Availability Benchmarks

The bidder shall commit to the following minimum service levels:

Service	Minimum Target
Managed Service Availability	99.9%
Management Portal Availability	99.9%
Security Services Availability	99.9%
SD-WAN Services Availability	99.9%

Incident Response Benchmarks

Severity	Response Time	Restoration Objective
Critical	30 Minutes	4 Hours
High	1 Hour	8 Hours
Medium	4 Hours	24 Hours
Low	1 Business Day	Best Effort

Reporting Benchmark Requirements

The bidder shall provide:

Monthly Reports

- Service Availability
- Incident Statistics
- Threat Prevention Statistics
- Security Trends
- Capacity Utilisation
- SLA Compliance

Quarterly Reports

- Technology Health Assessment
- Cybersecurity Posture Assessment

- Capacity Forecast
- Technology Roadmap Recommendations
- Risk Assessment Update

Performance Validation Requirements

All bidders shall complete the following table.

Annexure B.1 – Performance Benchmark Declaration

Requirement	Manufacturer Specification	Independent Test Result	Proposed Value
Firewall Throughput			
NGFW Throughput			
Threat Prevention Throughput			
SSL Inspection Throughput			
Concurrent Sessions			
New Sessions Per Second			
SD-WAN Throughput			
VPN Throughput			
Remote Users Supported			
Log Processing Rate			

Mandatory Requirement

Failure to disclose the performance impact of enabling:

- IPS
- SSL Inspection
- Threat Prevention
- Application Control
- Sandboxing

shall result in the associated performance figure being disregarded during evaluation.

Evaluation Guidance

For adjudication purposes, vendors will be scored higher where:

- Published benchmark figures are independently verified.
- The proposed architecture provides greater headroom above MIBCO's stated requirements.
- Security services are enabled without significant degradation of throughput.
- Capacity planning demonstrates support for future growth without hardware replacement.

10.17.2 Performance Headroom Requirements

The proposed solution shall not be sized solely for current requirements.

The solution must provide sufficient capacity to support future growth.

Minimum growth assumptions:

Growth Area	Required Headroom
Users	30%
Remote Users	30%
Contractors	30%
Internet Bandwidth	30%
Azure Workloads	30%
Security Events	30%

10.17.3 Performance Benchmark Scoring Matrix

The adjudication committee may use the following guideline during evaluation.

Performance Response	Score Guidance
Meets minimum benchmark only	Acceptable
Exceeds benchmark by 10–25%	Good
Exceeds benchmark by 25–50%	Very Good
Exceeds benchmark by >50%	Excellent
Independent testing provided	Additional merit

Real-world NGFW performance provided	Additional merit
Uses marketing throughput only	Penalty

10.17.4 Mandatory Performance Declaration

Each bidder shall submit a signed declaration confirming:

1. Performance figures are based on security features enabled.
2. SSL/TLS inspection throughput is disclosed.
3. IPS throughput is disclosed.
4. Threat prevention throughput is disclosed.
5. Application control throughput is disclosed.
6. Figures are not based on theoretical packet forwarding rates.
7. Performance degradation caused by enabling security features has been disclosed.

Failure to disclose performance impacts shall result in the affected performance figures being excluded from evaluation.

Disqualification Criteria:

Any proposal that only provides firewall throughput, switching throughput or packet forwarding throughput without disclosing Next Generation Firewall throughput, IPS throughput, Threat Prevention throughput and SSL/TLS inspection throughput shall be deemed non-compliant and may be disqualified.

10.18 Future Expansion Requirements

The proposed solution shall support future expansion without major redesign.

The solution shall support future growth of:

- Users.
- Branches.
- Contractors.
- Cloud Services.
- Security Services.
- Internet Bandwidth.
- Azure Workloads.

The bidder shall clearly identify:

- Scalability limits.

- Licensing dependencies.
- Expansion requirements.
- Additional hardware requirements.
- Additional subscription requirements.

10.19 Mandatory Technical Deliverables

The successful bidder shall deliver:

Architecture Deliverables

- High-Level Design (HLD).
- Low-Level Design (LLD).
- Security Architecture.
- Azure Architecture.
- Disaster Recovery Architecture.
- Network Segmentation Design.

Technical Deliverables

- Implementation Plan.
- Migration Runbook.
- Cutover Plan.
- Rollback Plan.
- Test Plan.
- Validation Report.

Operational Deliverables

- As-Built Documentation.
- Configuration Documentation.
- Administrator Guide.
- Operational Procedures.
- Escalation Procedures.
- Support Documentation.

11. SECURITY REQUIREMENTS

11.1 Security Objectives

The proposed solution shall provide enterprise-grade cybersecurity controls designed to:

- Reduce MIBCO's cyber risk exposure.
- Protect business-critical systems and data.
- Support a Zero Trust security model.
- Support regulatory compliance obligations.
- Detect, prevent and respond to cyber threats.
- Secure remote access.
- Secure cloud services.
- Protect sensitive member and financial information.
- Support Security Operations Centre (SOC) activities.

The bidder shall explain how the proposed solution supports these objectives.

11.2 Security Architecture Requirements

The proposed solution shall provide a defence-in-depth security architecture.

The architecture shall include multiple layers of protection across:

- Users
- Devices
- Networks
- Applications
- Data
- Cloud Services
- Identity Services
- Datacentre Services
- Azure Services

The bidder shall provide architecture diagrams demonstrating how the proposed controls work together.

11.3 Next Generation Firewall Security Controls

The solution shall provide integrated Next Generation Firewall capabilities.

Mandatory capabilities include:

- Layer 7 Application Awareness
- User Awareness
- Device Awareness
- Policy-Based Enforcement
- Content Inspection
- URL Filtering
- Application Control
- Threat Prevention
- Identity-Based Security Policies

The solution shall provide visibility and enforcement at:

- User level
- Device level
- Application level
- Network level

11.4 Intrusion Detection and Prevention

The solution shall provide integrated IDS and IPS functionality.

Mandatory capabilities:

- Signature-Based Detection
- Behaviour-Based Detection
- Protocol Analysis
- Exploit Detection
- Vulnerability Detection
- Prevention Controls

The bidder shall describe:

- Threat update frequency
- Signature update process
- Intelligence feed sources
- Detection effectiveness

11.5 Advanced Threat Prevention

The solution shall provide advanced threat prevention capabilities.

Mandatory controls:

- Anti-Malware
- Anti-Ransomware
- Anti-Botnet
- Command-and-Control Detection
- Zero-Day Detection
- Advanced Threat Analysis

The proposed solution shall provide:

- Automated threat identification
- Automated prevention
- Automated alerting
- Security event correlation

11.6 Malware Analysis and Sandboxing

The solution shall provide sandboxing capabilities.

Mandatory functionality:

- Dynamic Malware Analysis
- File Reputation Analysis
- Zero-Day Threat Analysis
- Behavioural Analysis

- Real-Time Verdicting

The bidder shall describe:

- Sandboxing methodology
- Threat intelligence integration
- Detection effectiveness

11.7 DNS Security

The solution shall provide DNS security controls.

Minimum requirements:

- DNS Threat Detection
- DNS Tunnelling Detection
- Malicious Domain Blocking
- Known Threat Blocking
- Command and Control Blocking
- DNS Analytics

The bidder shall describe:

- Threat intelligence sources
- Update frequency
- DNS enforcement methods

11.8 URL Filtering and Web Security

The solution shall provide URL filtering and web security controls.

Mandatory functionality:

- Category-Based Filtering
- Reputation-Based Filtering
- Malicious Website Detection
- Phishing Protection
- Acceptable Use Enforcement

- SSL/TLS Inspection

The solution shall support custom URL categories.

11.9 SSL/TLS Inspection Security

The proposed solution shall support comprehensive encrypted traffic inspection.

Mandatory capabilities:

- TLS 1.3 Inspection
- HTTPS Inspection
- Selective Decryption
- Certificate-Based Controls
- Policy-Based Decryption

The bidder shall disclose:

- SSL inspection throughput
- SSL inspection limitations
- Performance impact

11.10 Threat Intelligence Requirements

The proposed solution shall integrate with global threat intelligence services.

Mandatory capabilities:

- Threat Feed Integration
- Reputation Services
- IOC Feeds
- Threat Correlation
- Automated Threat Updates

The bidder shall describe:

- Source of threat intelligence
- Update frequency
- Intelligence sharing mechanisms

11.11 MITRE ATT&CK Alignment

The solution shall support mapping of security events to the MITRE ATT&CK framework.

Mandatory capabilities:

- ATT&CK Mapping
- ATT&CK Reporting
- ATT&CK Visualisation
- Threat Triage Support
- Threat Hunting Support

The bidder shall demonstrate how security events are correlated against ATT&CK techniques.

11.12 Data Loss Prevention (DLP)

The proposed solution shall provide enterprise-grade Data Loss Prevention capabilities.

The solution shall support:

DLP Area	Required
Web Traffic	Yes
Email Traffic	Yes
SaaS Applications	Yes
Microsoft 365	Yes
Azure Storage	Yes
Endpoint DLP	Yes

Mandatory capabilities:

- Data Classification
- Data Discovery
- Policy Enforcement
- Data Exfiltration Prevention

- Incident Management
- Reporting

11.13 Cloud Access Security Broker (CASB)

The solution shall provide CASB functionality.

Mandatory capabilities:

- SaaS Visibility
- SaaS Risk Assessment
- Shadow IT Discovery
- Application Governance
- Data Protection Controls
- User Activity Monitoring

The bidder shall explain how CASB integrates with Microsoft 365 and Azure.

11.14 Secure Web Gateway (SWG)

The solution shall provide Secure Web Gateway functionality.

Mandatory capabilities:

- Secure Internet Access
- Content Filtering
- Malware Protection
- URL Filtering
- SSL Inspection
- Threat Detection

11.15 Remote Browser Isolation (RBI)

The solution shall provide browser isolation capabilities.

Mandatory functionality:

- Isolation of Unknown Sites
- Isolation of High-Risk Sites

- Malware Containment
- Safe Browsing

The bidder shall explain:

- User experience impact
- Deployment options
- Policy enforcement capabilities

11.16 User and Entity Behaviour Analytics (UEBA)

The proposed solution shall include UEBA capabilities.

Mandatory capabilities:

- Behaviour Profiling
- Risk Scoring
- Anomaly Detection
- Insider Threat Detection
- Account Compromise Detection

The solution shall support:

- User Risk Scores
- Device Risk Scores
- Alert Prioritisation

11.17 Identity-Aware Security

The solution shall support identity-centric security principles.

Mandatory integrations:

- Microsoft Entra ID
- Microsoft Active Directory
- Conditional Access
- MFA
- Intune

Mandatory capabilities:

- User-Based Policies
- Group-Based Policies
- Dynamic Policies
- Identity-Aware Firewalling

11.18 Security Analytics and Reporting Requirements

The proposed solution shall provide advanced security analytics capabilities to support security monitoring, threat detection, incident response, compliance reporting and executive decision-making.

Security Event Correlation

The solution shall correlate events from multiple sources including:

- Firewall Events
- SD-WAN Events
- ZTNA Events
- Authentication Events
- Microsoft Entra ID Events
- Microsoft Defender Events
- Endpoint Events
- Azure Events
- CASB Events
- DLP Events

The bidder shall describe event correlation capabilities.

Threat Intelligence Correlation

The solution shall correlate security events against:

- Global Threat Intelligence Feeds
- Known Indicators of Compromise (IoCs)
- Known Malicious IP Addresses
- Known Malicious Domains
- Threat Intelligence Platforms

The solution should automatically enrich security events with external threat intelligence.

User Risk Analytics

The solution shall provide:

- User Risk Scoring
- User Behaviour Analysis
- Privileged User Monitoring
- Anomalous User Behaviour Detection
- Compromised Account Detection

Example use cases:

- User downloading unusual volumes of data.
- User accessing systems outside normal working hours.
- User accessing unusual applications.
- Credential compromise indicators.

Entity Risk Analytics

The solution shall provide risk scoring for:

- Devices
- Applications
- Servers
- Network Segments
- Cloud Services

The solution shall identify high-risk entities requiring investigation.

Machine Learning and AI Analytics

The proposed solution should provide:

- Behavioural Baseline Modelling
- Anomaly Detection
- AI-Assisted Threat Detection
- Emerging Threat Detection
- Threat Prediction

The bidder shall describe:

- AI model usage.
- Learning methodology.
- False-positive reduction mechanisms.

MITRE ATT&CK Analytics

The solution shall support:

- MITRE ATT&CK Mapping
- ATT&CK Dashboards
- ATT&CK Visualisation
- ATT&CK-Based Detection Rules

The solution should assist security analysts in identifying:

- Initial Access Techniques
- Privilege Escalation Attempts
- Persistence Mechanisms
- Lateral Movement Activities
- Data Exfiltration Attempts

Threat Hunting Analytics

The solution should assist Security Operations personnel with:

- Threat Hunting
- Historical Analysis
- IOC Searching
- Behavioural Analytics
- Investigation Workflows

The bidder shall describe available threat hunting capabilities.

Dashboard Requirements

The solution shall provide role-based dashboards.

Executive Dashboard

Must provide:

- Overall Security Posture
- Top Risks
- Security Trends
- Compliance Status
- Business Impact View

Security Operations Dashboard

Must provide:

- Active Threats
- Security Incidents
- Threat Intelligence
- User Risks
- Device Risks

Infrastructure Dashboard

Must provide:

- Firewall Health
- SD-WAN Health
- Performance Metrics
- Capacity Metrics
- Service Availability

Compliance Analytics

The solution shall provide analytics supporting:

- POPIA
- PCI-DSS
- NIST CSF
- ISO 27001
- FSCA Requirements
- PFA Requirements

Reports shall be exportable in:

- PDF
- Excel
- CSV

SOC Integration Analytics

The solution shall support:

- Wazuh Integration
- Grafana Dashboards
- API-Based Reporting

- Webhook Integration
- N8N Automation

The bidder shall explain how data can be consumed by MIBCO's SOC platforms.

Mandatory Security Analytics Demonstration

The bidder shall demonstrate the following during the Proof of Concept:

Analytics Capability	Demonstration Required
Threat Correlation	Yes
User Behaviour Analytics	Yes
Device Risk Analytics	Yes
Threat Intelligence Enrichment	Yes
MITRE ATT&CK Mapping	Yes
Security Dashboards	Yes
Compliance Reporting	Yes
Wazuh Integration	Yes
API Integration	Yes

11.19 Security Logging Requirements

The solution shall log:

- Security Events
- Authentication Events
- Administrative Activities
- Threat Events
- Policy Changes
- Configuration Changes

Log retention requirements:

Requirement	Duration
Online Retention	30 Days
Archived Retention	5 Years

11.20 Security Certifications and Standards

The proposed solution shall support or demonstrate alignment with:

- FIPS 140-2 or FIPS 140-3 Cryptography
- Common Criteria Certification (where available)
- NIST Cyber Security Framework
- ISO 27001 Security Controls

The bidder shall provide supporting evidence.

11.21 Security Response and Incident Management

The proposed solution shall support:

- Threat Detection
- Threat Containment
- Incident Investigation

- Root Cause Analysis
- Security Alerting
- Automated Response Workflows

The bidder shall describe available response automation capabilities and integration options with the MIBCO SOC.

11.22 Security Capability Declaration

The bidder shall complete Annexure A and indicate:

- Comply
- Partially Comply
- Does Not Comply

for every security requirement contained within this section.

Failure to comply with any mandatory security requirement may result in the proposal being deemed non-responsive and excluded from further evaluation.

12. HYBRID DATA CENTRE AND AZURE DISASTER RECOVERY REQUIREMENTS

12.1 Hybrid Architecture Objectives

MIBCO operates a hybrid technology environment consisting of:

- A primary production Data Centre located in Randburg.
- A Disaster Recovery (DR) environment hosted within Microsoft Azure South Africa.
- Twenty-one (21) national offices connected via SD-WAN.
- Remote users.
- Third-party and contractor access.

The proposed solution shall provide a unified security architecture across all environments and shall ensure consistent security controls, visibility, policy management, monitoring and reporting.

The bidder shall demonstrate how the proposed solution supports:

- Hybrid networking.
- Hybrid security.
- Disaster recovery.

- Business continuity.
- Centralised management.
- Policy portability.
- Unified operational visibility.

The bidder shall provide a detailed architecture demonstrating the integration of:

- Randburg Data Centre.
- Azure DR Environment.
- Branch Offices.
- Remote Users.
- Third-Party Users.
- Security Operations Centre.

12.2 Randburg Data Centre Security Requirements

The proposed solution shall provide enterprise-grade protection for MIBCO's primary production Data Centre.

The solution shall support:

Perimeter Security

- Next Generation Firewall protection.
- Application-aware inspection.
- Threat prevention.
- Anti-malware controls.
- SSL/TLS inspection.
- DNS security.
- URL filtering.
- Advanced threat protection.

Internal Security Controls

- East-West traffic inspection.
- Internal segmentation.

- Identity-aware segmentation.
- Server protection.
- Administrative network isolation.

Visibility

The solution shall provide visibility into:

- Server communications.
- Inter-zone traffic.
- User access activity.
- Third-party access activity.
- Administrative activities.
- Security threats.

12.3 Data Centre Segmentation Requirements

The proposed solution shall support logical and security segmentation between critical infrastructure components.

The bidder shall propose segmentation controls for the following zones.

Security Zone	Mandatory
User Network	Yes
Server Network	Yes
Domain Controllers	Yes
Database Servers	Yes
Application Servers	Yes
Storage Infrastructure	Yes
Backup Infrastructure	Yes
VoIP Infrastructure	Yes
Management Networks	Yes
Security Management Platforms	Yes
Guest Networks	Yes
DMZ	Yes

The solution shall support:

- Inter-zone policy enforcement.
- Least-privilege communications.
- Role-based segmentation.
- Identity-based segmentation.
- Micro-segmentation.

The bidder shall provide a proposed segmentation model.

12.4 Azure Disaster Recovery Security Requirements

The solution shall provide integrated security for the Microsoft Azure Disaster Recovery environment.

The proposed architecture shall secure:

- Azure Virtual Networks.
- Azure workloads.
- Azure application services.
- Azure replication services.
- Azure VPN services.
- Recovery infrastructure.

The architecture shall ensure that a disaster recovery event does not reduce the security posture of the organisation.

The bidder shall describe:

- Azure deployment architecture.
- Azure security controls.
- Azure policy enforcement capabilities.
- Azure security monitoring capabilities.

12.5 Azure Connectivity Requirements

The proposed solution shall support secure connectivity between the Randburg Data Centre and Azure South Africa.

Mandatory support shall include:

The bidder shall describe:

- Connectivity design.
- Routing architecture.
- Failover methodology.
- Security controls applied to hybrid connectivity.

12.6 Azure Routing and Integration Requirements

The proposed solution shall integrate securely with Microsoft Azure networking services.

The bidder shall demonstrate support for:

- Dynamic routing.
- Route advertisement.

- Route failover.
- Secure route propagation.
- Integration with Azure routing architecture.

The bidder shall explain how security policies remain effective during:

- Normal operation.
- DR testing.
- Disaster declaration.
- Azure failover events.

12.7 Disaster Recovery Security Requirements

The proposed solution shall support secure disaster recovery operations.

The bidder shall describe how security services are maintained during:

Planned Failover

- Disaster Recovery testing.
- Infrastructure maintenance.
- Planned migration activities.

Unplanned Failover

- Data Centre outages.
- Cybersecurity incidents.
- Infrastructure failures.
- Connectivity failures.

The proposed solution shall maintain:

- Firewall policies.
- Security policies.
- Identity policies.
- Logging.
- Monitoring.

- Threat prevention controls.

during failover operations.

12.8 Security Policy Synchronisation

Security policies shall be consistently enforced across:

- Randburg Data Centre.
- Azure Disaster Recovery Environment.
- Regional Offices.
- Satellite Offices.
- Remote Users.

The proposed solution shall support:

Policy Synchronisation

- Firewall policies.
- Segmentation policies.
- ZTNA policies.
- User access policies.
- Security inspection policies.
- Logging policies.

The bidder shall explain:

- Synchronisation methodology.
- Synchronisation intervals.
- Policy validation controls.
- Policy rollback procedures.

12.9 Secure Replication Traffic Requirements

The proposed solution shall secure all replication traffic between:

- Randburg Data Centre.
- Azure Disaster Recovery Environment.

The bidder shall describe the controls applied to:

Replication Traffic

- Encryption.
- Monitoring.
- Logging.
- Threat Inspection.
- Route Protection.

Encryption Standards

Minimum requirements:

- TLS 1.3.
- AES-256.
- SHA-256.
- Perfect Forward Secrecy.
- IPSEC IKEv2.

The bidder shall indicate whether replication traffic can be inspected without compromising application functionality.

12.10 Hybrid Architecture Management Requirements

The solution shall provide centralised administration and operational management across all environments.

The management platform shall provide:

Centralised Management

- Policy Management.
- Device Management.
- User Management.
- Reporting.
- Threat Monitoring.

Unified Visibility

Visibility shall include:

- Data Centre activity.
- Azure activity.
- Branch activity.
- Remote user activity.
- Threat activity.

The bidder shall demonstrate how administrators can manage all environments through a single management platform.

12.11 Logging and Monitoring Requirements

The proposed solution shall provide unified logging and monitoring across the hybrid environment.

Logging Scope

The solution shall generate and retain logs for:

- Data Centre security events.
- Azure security events.
- SD-WAN events.
- ZTNA events.
- Authentication events.
- Administrative activities.
- Threat prevention activities.

SIEM Integration

The solution shall integrate with:

- Wazuh.
- Grafana.
- N8N.
- Ollama.

Supported methods shall include:

- REST API.
- Syslog.
- JSON.
- Webhooks.
- STIX/TAXII.

Retention Requirements

Requirement	Duration
Online Logs	30 Days
Archived Logs	5 Years

12.12 Disaster Recovery Testing Requirements

The successful bidder shall support periodic Disaster Recovery testing.

The solution shall facilitate:

- Annual DR testing.
- Partial failover testing.
- Full failover testing.
- Recovery validation testing.

The bidder shall provide:

- Test procedures.
- Test plans.
- Test schedules.
- Test reporting templates.

The bidder shall explain how security services remain operational during DR test activities.

12.13 Disaster Recovery Reporting Requirements

The solution shall provide reporting capabilities relating to:

Availability

- Service uptime.
- Service health.
- Connectivity status.

Recovery Performance

- Recovery Time Objective (RTO) achievement.
- Recovery Point Objective (RPO) achievement.
- Failover duration.
- Failback duration.

Security Performance

- Security policy integrity.
- Threat prevention continuity.
- Security event continuity.
- Log retention continuity.

Reports shall be available on-demand and included in monthly operational reports.

12.14 Business Continuity Requirements

The proposed solution shall support MIBCO's business continuity objectives.

The solution shall minimise operational disruption during:

- Cybersecurity incidents.
- Infrastructure failures.
- Network outages.
- Site outages.
- Disaster recovery events.

The bidder shall describe:

- Resilience mechanisms.
- Recovery mechanisms.
- Security continuity controls.

- Operational continuity controls.

12.15 Hybrid Architecture Response Requirements

As part of the proposal submission, bidders shall provide:

Architecture Deliverables

- Current State Understanding Diagram.
- Proposed Future State Architecture Diagram.
- Hybrid Network Architecture Diagram.
- Azure DR Architecture Diagram.
- Security Architecture Diagram.
- Segmentation Architecture Diagram.

Operational Deliverables

The bidder shall describe:

- Management model.
- Security operations model.
- Incident response model.
- DR support model.

Compliance Statement

The bidder shall complete Annexure J – Hybrid Architecture Response Schedule and indicate compliance with every requirement contained within this section.

Failure to adequately address the Hybrid Data Centre and Azure Disaster Recovery requirements may result in the proposal being deemed technically non-compliant and excluded from further evaluation.

13. ZERO TRUST REQUIREMENTS

13.1 Zero Trust Objectives

MIBCO intends to transition from traditional perimeter-based security controls towards a Zero Trust security model.

The proposed solution shall support the principles of:

- Never Trust, Always Verify.

- Assume Breach.
- Least Privilege Access.
- Continuous Verification.
- Identity-Centric Security.
- Device-Centric Security.
- Application-Centric Security.
- Risk-Based Access Control.

The bidder shall describe how the proposed solution enables the adoption and maturation of Zero Trust Architecture across MIBCO.

13.2 Zero Trust Architectural Principles

The proposed solution shall support the following Zero Trust pillars:

Zero Trust Pillar	Mandatory
Identity	Yes
Devices	Yes
Networks	Yes
Applications	Yes
Data	Yes
Infrastructure	Yes
Visibility and Analytics	Yes
Automation and Orchestration	Yes

The bidder shall explain how the solution addresses each pillar.

13.3 Zero Trust Network Access (ZTNA)

The solution shall provide enterprise-grade Zero Trust Network Access capabilities.

The solution shall support secure access to:

- On-Premises Applications.
- Azure Hosted Applications.
- Web Applications.
- Line-of-Business Applications.

- Administrative Platforms.
- Third-Party Access Services.

The proposed solution shall eliminate or significantly reduce reliance on traditional VPN services.

The bidder shall clearly indicate:

- Applications accessible through ZTNA.
- Limitations of the ZTNA solution.
- Licensing dependencies.
- Deployment requirements.

13.4 Identity-Centric Security

Identity shall form the primary security control within the proposed Zero Trust architecture.

The solution shall integrate with:

- Microsoft Entra ID.
- Microsoft Active Directory
- Microsoft Conditional Access.
- Microsoft Multi-Factor Authentication.
- Microsoft Intune.

The solution shall support:

- User-Based Access Policies.
- Group-Based Access Policies.
- Risk-Based Access Policies.
- Role-Based Access Policies.
- Dynamic Access Controls.

The bidder shall explain how identities are continuously evaluated.

13.5 Device Trust and Posture Validation

The proposed solution shall continually verify device trust before and during access sessions.

Mandatory Device Validation Checks

Validation Requirement	Mandatory
Microsoft Defender Operational	Yes
Real-Time Protection Enabled	Yes
Updated Malware Signatures	Yes
BitLocker Enabled	Yes
Intune Compliance	Yes
Operating System Patch Compliance	Yes
Domain Joined or Approved Device	Yes

Preferred Device Validation Checks

Validation Requirement	Preferred
Secure Boot Enabled	Yes
TPM Enabled	Yes
Device Risk Scoring	Yes
Jailbreak Detection	Yes
Root Detection	Yes

Device compliance shall be evaluated continuously and not solely at authentication.

13.6 Continuous Verification

Access decisions shall not be based on a single authentication event.

The proposed solution shall continuously evaluate:

- User Identity.
- Device Health.
- Device Risk.
- User Risk.
- Geographic Location.
- Network Context.

- Application Context.
- Session Behaviour.

The bidder shall explain how session risk is re-evaluated during active sessions.

13.7 Least Privilege Access Controls

The solution shall enforce Least Privilege principles.

The solution shall support:

- Application-Level Access.
- Role-Based Access.
- Temporary Access.
- Granular Authorisation.
- Segmented Access Rights.
- Just-In-Time Access.

Access shall only be granted to resources explicitly authorised for the user.

The solution shall prevent broad network-level access wherever possible.

13.8 Adaptive and Risk-Based Access Controls

The solution shall provide context-aware access decisions.

Risk factors shall include:

- User Identity.
- Device Health.
- Device Compliance.
- User Behaviour.
- Geographic Location.
- Time of Day.
- Authentication Risk.
- Threat Intelligence Indicators.

The solution shall support automatic enforcement actions such as:

- Allow Access.
- Challenge with MFA.
- Restrict Access.

- Read-Only Access.
- Block Access.
- Session Termination.

13.9 Application-Level Access Controls

The solution shall support application-level access rather than network-level access.

The bidder shall demonstrate how users are granted access to:

- Specific Applications.
- Specific Services.
- Specific Workloads.

without exposing entire network segments.

The solution shall support:

- Application Discovery.
- Application Classification.
- Application Access Policies.
- Application Visibility.

13.10 Third-Party and Contractor Access Controls

MIBCO supports contractor and third-party access to business systems.

The proposed solution shall provide:

Contractor Access Controls

- Dedicated Contractor Policies.
- Limited Access Rights.
- Time-Limited Access.
- Expiry-Based Access.
- Approval-Based Access.
- Application-Level Access.

Session Controls

- Session Monitoring.
- Session Recording.
- Session Logging.

- Session Risk Analysis.

The bidder shall describe how third-party users are isolated from internal resources.

13.11 Privileged Access Controls

The proposed solution shall support enhanced protections for privileged users.

Mandatory capabilities:

- Role-Based Administration.
- Just-In-Time Privileged Access.
- Multi-Factor Authentication.
- Administrative Session Logging.
- Administrative Session Monitoring.
- Administrative Activity Auditing.

The bidder shall describe available integrations with Privileged Access Management (PAM) solutions.

13.12 Micro-Segmentation Requirements

The proposed solution shall support micro-segmentation and identity-based segmentation.

The solution shall support segmentation based on:

- User Identity.
- Device Identity.
- Security Group Membership.
- Business Function.
- Risk Level.
- Application.

The bidder shall describe how micro-segmentation is applied within:

- Randburg Data Centre.
- Azure DR Environment.
- Branch Networks.

13.13 Conditional Access Integration

The proposed solution shall integrate with Microsoft Conditional Access.

The bidder shall demonstrate support for:

- Device Compliance Checks.

- User Risk Evaluation.
- Sign-In Risk Evaluation.
- Location-Based Controls.
- Application-Based Controls.
- Session Controls.

The solution shall not require duplication of Conditional Access policies already managed within Microsoft Entra ID.

13.14 Zero Trust Visibility and Analytics

The solution shall provide visibility into:

- User Activity.
- Device Activity.
- Application Usage.
- Access Requests.
- Access Approvals.
- Access Failures.
- Device Compliance Status.
- User Risk Scores.

The bidder shall provide dashboards supporting:

Executive View

- Zero Trust Adoption.
- Access Risk.
- Security Posture.

Security Operations View

- Access Events.
- User Risk.
- Device Risk.
- Threat Indicators.

Administrative View

- Identity Activity.

- Policy Enforcement.
- Compliance Status.

13.15 Zero Trust Automation and Orchestration

The solution should support automation of Zero Trust policy enforcement.

Examples include:

- Automatic Device Quarantine.
- Automatic Session Termination.
- Automatic MFA Enforcement.
- Automatic Access Revocation.
- Automated Incident Response.

The solution shall integrate with:

- Wazuh.
- N8N.
- Microsoft Security Services.

The bidder shall describe available automation capabilities.

13.16 Remote Workforce Security

The proposed solution shall support secure access for remote workers.

The solution shall provide:

- ZTNA Access.
- MFA Enforcement.
- Device Posture Validation.
- Application-Level Access.
- Threat Inspection.
- Secure Internet Access.

Remote users shall receive equivalent security protections regardless of location.

13.17 Zero Trust Compliance Requirements

The bidder shall demonstrate how the proposed solution supports Zero Trust principles aligned with:

- NIST Cybersecurity Framework.
- ISO 27001.

- ISO 27002.
- ISO 27005.
- ISO 27032.
- POPIA.
- PCI-DSS.
- FSCA Requirements.

13.18 Zero Trust Maturity Roadmap

The bidder shall provide a proposed Zero Trust maturity roadmap for MIBCO covering:

Phase 1

- Foundation Controls.
- Identity Integration.
- Device Compliance.

Phase 2

- ZTNA Deployment.
- Application Access Controls.
- Contractor Access Controls.

Phase 3

- Micro-Segmentation.
- Continuous Verification.
- Risk-Based Enforcement.

Phase 4

- Advanced Analytics.
- Automated Response.
- Zero Trust Optimisation.

The roadmap shall indicate expected business outcomes, implementation effort and dependencies.

13.19 Mandatory Bidder Response Requirements

The bidder shall complete the Zero Trust compliance schedule in Annexure A and indicate:

- Fully Compliant.
- Partially Compliant.

- Non-Compliant.

The bidder shall provide supporting evidence for each response.

Failure to comply with mandatory Zero Trust requirements may result in the proposal being considered non-responsive and excluded from further evaluation.

14. IDENTITY, ACCESS CONTROL AND DEVICE POSTURE REQUIREMENTS

14.1 Objectives

The proposed solution shall provide secure, identity-driven access controls aligned with Zero Trust principles.

Identity shall become the primary security control for granting, monitoring and restricting access to MIBCO resources.

The solution shall support:

- Strong authentication.
- Continuous identity validation.
- Device trust verification.
- Risk-based access decisions.
- Least privilege access.
- Secure remote access.
- Secure contractor access.
- Conditional access controls.
- Continuous access governance.

The bidder shall demonstrate how the proposed solution supports identity-centric security across:

- Randburg Data Centre.
- Azure Disaster Recovery Environment.
- Branch Offices.
- Remote Users.
- Mobile Users.
- Contractors and Third Parties.

14.2 Identity Platform Integration

The proposed solution shall integrate with MIBCO's existing identity platform.

Mandatory Integrations

Identity Platform	Mandatory
Microsoft Entra ID	Yes
Microsoft Active Directory	Yes
Microsoft Conditional Access	Yes
Microsoft MFA	Yes
Microsoft Intune	Yes

The bidder shall describe:

- Native integration capabilities.
- Authentication methods supported.
- Synchronisation methods.
- Identity federation options.
- Licensing dependencies.

14.3 Authentication Requirements

The proposed solution shall support strong authentication mechanisms.

Mandatory Authentication Methods

- Multi-Factor Authentication (MFA).
- Single Sign-On (SSO).
- Passwordless Authentication (where supported).
- Certificate-Based Authentication.
- Risk-Based Authentication.

Supported Authentication Factors

The solution should support:

- Microsoft Authenticator.
- Push Notifications.
- FIDO2 Security Keys.
- Certificates.

The bidder shall identify any authentication limitations.

14.4 Single Sign-On (SSO)

The solution shall provide Single Sign-On for:

- Administrative Portals.
- Remote Access Services.
- ZTNA Services.
- Security Management Consoles.
- Cloud Applications.

The bidder shall explain:

- Supported SSO standards.
- Entra ID integration.
- Federation support.

Supported Standards

Standard	Required
SAML 2.0	Yes
OAuth 2.0	Yes
OpenID Connect	Yes
LDAP	Yes
RADIUS	Yes

14.5 Multi-Factor Authentication (MFA)

The solution shall enforce MFA for all privileged and administrative access.

Mandatory MFA Requirements

- Administrative Access.
- Cloud Administration.
- Security Administration.
- Remote Access.
- ZTNA Access.
- Contractor Access.

The solution shall support:

- Adaptive MFA.
- Risk-Based MFA.
- Conditional MFA.

The bidder shall describe available MFA policy options.

14.6 Conditional Access Requirements

The proposed solution shall integrate with MIBCO's existing Microsoft Conditional Access framework.

The solution shall support decisions based on:

- User Identity.
- Device Compliance.
- Device Health.
- Location.
- Sign-In Risk.
- User Risk.
- Application Sensitivity.

Policy Actions

The solution shall support:

- Allow.
- Block.
- Require MFA.
- Require Device Compliance.
- Require Reauthentication.
- Restrict Access.

The bidder shall explain how policy conflicts are managed.

14.7 Device Posture Assessment Requirements

The proposed solution shall provide continuous device posture assessment capabilities.

Device posture assessments shall be performed before and during active sessions.

The solution shall support real-time posture validation.

14.8 Mandatory Device Compliance Checks

The proposed solution shall validate the following minimum controls.

Device Posture Check	Mandatory
Microsoft Defender Running	Yes
Real-Time Protection Enabled	Yes
Defender Signatures Updated	Yes
BitLocker Enabled	Yes
Device Managed by Intune	Yes
Device Compliance Status	Yes
Supported Operating System	Yes
Operating System Patch Compliance	Yes
Domain Joined or Approved Device	Yes

Access decisions shall be capable of being based on these posture validations.

14.9 Preferred Device Compliance Checks

The following capabilities are desirable and may attract additional evaluation points.

Device Posture Check	Preferred
Secure Boot Enabled	Yes
TPM Present	Yes
TPM Enabled	Yes
Device Risk Score	Yes
Vulnerability Assessment	Yes
Jailbreak Detection	Yes
Root Detection	Yes
Endpoint Detection and Response Integration	Yes

14.10 Device Trust Levels

The solution should support multiple trust levels.

Example Device Categories

Device Category	Description
Trusted Device	Fully compliant corporate device
Restricted Device	Partially compliant device
Untrusted Device	Non-compliant device
BYOD Device	Personal device
Contractor Device	Third-party device

The bidder shall explain how access is limited according to trust level.

14.11 Bring Your Own Device (BYOD)

MIBCO permits limited BYOD access.

The proposed solution shall support secure access from personally owned devices.

BYOD Controls

The solution shall support:

- Device Registration.
- Device Validation.
- Device Trust Assessment.
- Application-Level Access.
- Session Controls.
- Data Protection Controls.

The solution shall prevent unrestricted access from unmanaged devices.

14.12 Access Control Requirements

The solution shall support granular access control policies.

Access decisions shall be based on:

- User Identity.
- Group Membership.
- Device Trust.
- Device Compliance.

- Location.
- Risk Score.
- Time of Day.
- Application.

Access Models

The solution shall support:

- Role-Based Access Control (RBAC).
- Attribute-Based Access Control (ABAC).
- Dynamic Access Controls.
- Risk-Based Access Controls.

14.13 Role-Based Access Control (RBAC)

The solution shall support granular role definitions.

Minimum administrative roles shall include:

Role	Required
Security Administrator	Yes
Network Administrator	Yes
SOC Analyst	Yes
Auditor	Yes
Read-Only Administrator	Yes
Service Provider Administrator	Yes

The bidder shall describe how separation of duties is achieved.

14.14 Privileged Access Management (PAM)

The solution shall support integration with Privileged Access Management processes.

The solution shall provide:

- Privileged Session Control.
- Administrative Session Logging.
- Privileged Activity Monitoring.
- Just-In-Time Administration.

- Approval-Based Access.

The bidder shall describe PAM integration capabilities.

14.15 Just-In-Time (JIT) Access

The proposed solution shall support Just-In-Time access provisioning.

Capabilities shall include:

- Time-Limited Access.
- Approval-Based Access.
- Temporary Permissions.
- Automatic Access Revocation.
- Administrative Auditing.

The bidder shall describe available JIT controls.

14.16 Administrative Access Security

Administrative access shall be protected through enhanced controls.

Mandatory Requirements

- MFA.
- SSO.
- JIT Access.
- Audit Logging.
- Session Monitoring.
- Role Separation.

The bidder shall explain how privileged administrative accounts are protected against compromise.

14.17 Session Management Requirements

The solution shall support monitoring and governance of user sessions.

Session Controls

Mandatory capabilities:

- Session Logging.
- Session Monitoring.
- Session Timeout.
- Session Revocation.

- Session Termination.
- Session Risk Assessment.

High-Risk Sessions

The solution shall support:

- Forced Reauthentication.
- Session Escalation.
- Session Blocking.

14.18 Contractor and Third-Party Access Control

The solution shall provide dedicated controls for contractor access.

Mandatory Controls

- Identity Verification.
- Role-Based Access.
- Application-Level Access.
- Time-Limited Access.
- Approval-Based Access.
- Session Monitoring.
- Session Recording.

The solution shall ensure third-party users cannot access unauthorised resources.

14.19 Identity Governance and Administration

The solution shall support identity governance processes.

Capabilities shall include:

- User Lifecycle Management.
- Access Reviews.
- Entitlement Reviews.
- Access Certification.
- Access Recertification.

The bidder shall describe available governance capabilities.

14.20 Identity Analytics

The solution shall provide identity-focused analytics.

The solution shall support:

- User Risk Scoring.
- User Behaviour Analysis.
- Anomalous Authentication Detection.
- Credential Compromise Detection.
- Identity Threat Detection.

The bidder shall explain how identity analytics integrates with:

- Wazuh.
- Microsoft Defender.
- Entra ID.
- Security Operations processes.

14.21 Audit and Compliance Requirements

The solution shall maintain complete audit records for:

- Authentication Events.
- Access Requests.
- Access Approvals.
- Access Denials.
- Administrative Changes.
- Role Changes.
- Device Compliance Decisions.

Audit logs shall:

- Be tamper resistant.
- Be exportable.
- Be searchable.
- Support retention requirements.

Retention Requirements

Requirement	Duration
Online Audit Records	30 Days
Archived Audit Records	5 Years

14.22 Reporting Requirements

The solution shall provide identity and access management reporting.

Required Reports

- User Access Reports.
- Administrative Activity Reports.
- MFA Utilisation Reports.
- Device Compliance Reports.
- Contractor Access Reports.
- Privileged Access Reports.
- Access Violation Reports.

Reports shall support export to:

- PDF.
- CSV.
- Microsoft Excel.

14.23 Proof of Concept Requirements

Shortlisted bidders may be required to demonstrate:

Capability	Demonstration Required
Entra ID Integration	Yes
MFA Enforcement	Yes
SSO Configuration	Yes
Device Compliance Validation	Yes
Conditional Access Integration	Yes

BitLocker Verification	Yes
Defender Validation	Yes
Intune Compliance Validation	Yes
Contractor Access Control	Yes
Session Recording	Yes

14.24 Bidder Response Requirements

The bidder shall complete the Identity, Access Control and Device Posture Compliance Schedule contained within Annexure A.

Responses shall indicate:

- Fully Compliant.
- Partially Compliant.
- Non-Compliant.

Supporting evidence, architectural explanations and product documentation shall be provided for all mandatory requirements.

Failure to comply with mandatory Identity, Access Control and Device Posture requirements may result in the proposal being deemed non-responsive and excluded from further evaluation.

15. SECURITY OPERATIONS CENTRE (SOC) INTEGRATION REQUIREMENTS

15.1 Objectives

MIBCO operates an internal Security Operations Centre (SOC) responsible for cyber threat detection, incident response, threat hunting, security monitoring, compliance reporting and cyber risk management.

The proposed solution shall integrate seamlessly with MIBCO's existing SOC ecosystem and support centralised monitoring, analysis, automation and reporting.

The objective is to ensure that the proposed solution enhances MIBCO's existing SOC capabilities and does not create isolated security management silos.

The bidder shall describe how the proposed solution supports:

- Threat Detection.
- Incident Response.
- Threat Hunting.
- Security Monitoring.
- Compliance Monitoring.

- Security Analytics.
- Security Automation.
- Operational Reporting.

15.2 Existing SOC Environment

The proposed solution shall integrate with the following existing SOC platforms:

Platform	Required
Wazuh	Yes
Grafana	Yes
Ollama	Yes
N8N	Yes

The bidder shall identify:

- Native integrations.
- Available connectors.
- Supported APIs.
- Configuration requirements.
- Licensing dependencies.

15.3 Centralised Security Monitoring

The proposed solution shall support centralised monitoring of:

Security Events

- Firewall Events.
- Threat Prevention Events.
- SD-WAN Events.
- ZTNA Events.
- CASB Events.
- SWG Events.
- DLP Events.
- UEBA Events.

Infrastructure Events

- Device Health.
- Resource Utilisation.
- Connectivity Status.
- Service Availability.

Identity Events

- Authentication Activity.
- MFA Activity.
- Access Control Decisions.
- User Risk Activity.
- Device Compliance Events.

15.4 Logging Integration Requirements

The solution shall support comprehensive logging and event forwarding capabilities.

Mandatory Log Sources

The solution shall export:

Event Category	Required
Firewall Events	Yes
Authentication Events	Yes
Threat Events	Yes
Malware Events	Yes
IPS Events	Yes
DNS Events	Yes
URL Filtering Events	Yes
Administrative Events	Yes
Configuration Changes	Yes
SD-WAN Events	Yes
ZTNA Events	Yes

DLP Events	Yes
CASB Events	Yes
RBI Events	Yes
UEBA Events	Yes

15.5 Log Export Requirements

The proposed solution shall support the following export mechanisms:

Method	Mandatory
Syslog	Yes
REST API	Yes
JSON Export	Yes
Webhooks	Yes
STIX/TAXII	Yes
CSV Export	Yes

The solution shall not require proprietary tools for basic log export functionality.

The bidder shall identify any limitations.

15.6 Security Event Correlation

The proposed solution shall support the correlation of events from multiple sources.

The solution shall provide:

- Threat Correlation.
- User Activity Correlation.
- Device Activity Correlation.
- Identity Correlation.
- Azure Security Correlation.
- Threat Intelligence Correlation.

The bidder shall describe:

- Correlation methodologies.

- Correlation rules.
- Risk scoring methodology.
- Event prioritisation capabilities.

15.7 Incident Response Integration

The solution shall support MIBCO incident response processes.

Mandatory Capabilities

- Alert Generation.
- Alert Escalation.
- Automated Ticket Creation.
- Incident Workflow Integration.
- Root Cause Analysis Support.
- Incident Investigation Support.

The solution shall provide sufficient information to support forensic investigations.

15.8 Threat Hunting Requirements

The proposed solution shall support proactive threat hunting activities.

The solution shall enable analysts to:

- Search historical events.
- Investigate Indicators of Compromise (IoCs).
- Investigate suspicious users.
- Investigate suspicious devices.
- Investigate anomalous activity.

The bidder shall describe available threat hunting capabilities.

15.9 Security Analytics Integration

The proposed solution shall provide integration with security analytics functions.

Security data shall be available for:

- Wazuh Correlation Rules.
- Grafana Visualisation.
- N8N Automation Workflows.
- AI-Assisted Analysis using Ollama.

The bidder shall describe how security data can be consumed by external analytics platforms.

15.10 Threat Intelligence Integration

The proposed solution shall support:

- Threat Feed Consumption.
- Indicator of Compromise (IOC) Integration.
- Indicator of Attack (IOA) Detection.
- Reputation Services.
- Threat Intelligence Sharing.

The bidder shall identify:

- Threat intelligence sources.
- Update frequency.
- Threat enrichment capabilities.

15.11 Security Automation and Orchestration

The proposed solution should support Security Orchestration, Automation and Response (SOAR) concepts.

The bidder shall provide details regarding:

Supported Automation Functions

- Automated Alerting.
- Automated Ticket Creation.
- Automated Event Enrichment.
- Automated Policy Enforcement.
- Automated Access Revocation.
- Automated Device Isolation.
- Automated Threat Containment.

15.12 N8N Integration Requirements

The proposed solution shall integrate with N8N automation workflows.

The bidder shall demonstrate support for:

- REST APIs.
- Webhooks.
- JSON Data Exchange.

- Event Triggering.
- Workflow Execution.

The bidder shall describe examples of workflows that can be automated.

15.13 Wazuh Integration Requirements

The proposed solution shall integrate with the MIBCO Wazuh platform.

The bidder shall identify:

- Supported log sources.
- Parsing capabilities.
- Correlation capabilities.
- Custom decoder support.
- Alert generation support.

The bidder shall provide examples of successful integrations.

15.14 Grafana Integration Requirements

The proposed solution shall provide data access suitable for Grafana visualisation.

The bidder shall identify:

- Supported connectors.
- API endpoints.
- Data export formats.
- Dashboard integration methods.

The solution shall support:

- Security Dashboards.
- Operational Dashboards.
- Compliance Dashboards.
- Executive Dashboards.

15.15 Ollama Integration Requirements

The proposed solution should support integration with AI-assisted security analysis capabilities.

The bidder shall describe:

- API capabilities.
- Data extraction methods.

- Security controls.
- Supported use cases.

Examples may include:

- Alert summarisation.
- Threat analysis.
- Security recommendations.
- Incident investigation support.

15.16 Security Dashboard Requirements

The proposed solution shall provide dashboards suitable for different stakeholder groups.

Executive Dashboard

The dashboard shall include:

- Security Posture.
- Security Risk Trends.
- Compliance Status.
- Top Security Risks.
- SLA Performance.

SOC Dashboard

The dashboard shall include:

- Active Threats.
- Security Alerts.
- User Risks.
- Device Risks.
- Threat Intelligence Indicators.

Operational Dashboard

The dashboard shall include:

- Device Health.
- Service Availability.
- Performance Metrics.
- Connectivity Status.

15.17 Alerting Requirements

The solution shall generate alerts for:

Critical Security Events

- Malware Detection.
- Ransomware Detection.
- Intrusion Detection.
- Privilege Escalation.
- Credential Theft Indicators.
- Policy Violations.
- Data Exfiltration.

Operational Events

- Device Failure.
- Connectivity Failure.
- Service Failure.
- Capacity Threshold Breaches.

The bidder shall describe alert prioritisation capabilities.

15.18 Security Reporting Requirements

The solution shall support scheduled and ad-hoc reporting.

Operational Reports

- Daily Security Summary.
- Weekly Security Summary.
- Monthly Security Report.

Compliance Reports

- POPIA Reports.
- PCI-DSS Reports.
- NIST Reports.
- ISO Reports.

Executive Reports

- Risk Exposure Reports.

- Security Posture Reports.
- Threat Landscape Reports.

15.19 Log Retention Requirements

The proposed solution shall support:

Requirement	Mandatory
Online Log Retention	30 Days
Archived Log Retention	5 Years
Full Event Searchability	Yes
Log Integrity Validation	Yes
Audit Trail Protection	Yes

The bidder shall describe:

- Retention architecture.
- Archival processes.
- Recovery processes.

15.20 Security Operations Performance Requirements

The solution shall support the following minimum capabilities:

Requirement	Minimum
Security Event Processing	10,000 EPS
Log Export Delay	Less than 1 Minute
Dashboard Refresh Rate	Less than 60 Seconds
Search Response Time	Less than 30 Seconds
API Availability	99.9%

The bidder shall explain how performance is maintained during periods of elevated security activity.

15.21 SOC Operational Support Requirements

The successful bidder shall provide support for:

- Security Incident Investigations.

- Platform Health Monitoring.
- Threat Intelligence Updates.
- Security Tuning.
- Rule Optimisation.
- Integration Maintenance.

The bidder shall describe ongoing SOC support services included within the managed service offering.

15.22 Bidder Response Requirements

The bidder shall complete the SOC Integration Compliance Schedule contained within Annexure A.

Responses shall indicate:

- Fully Compliant.
- Partially Compliant.
- Non-Compliant.

The bidder shall provide supporting documentation, architecture diagrams and evidence for each response.

Failure to comply with mandatory SOC Integration requirements may result in the proposal being deemed non-responsive and excluded from further evaluation.

15.23 Preferred Future-State Security Operations Capability

MIBCO's preferred future-state architecture is one where the proposed solution becomes an integrated component of a unified cyber defence ecosystem comprising:

- Microsoft Entra ID.
- Microsoft Defender for Endpoint.
- Microsoft Intune.
- Wazuh.
- Grafana.
- N8N.
- Ollama.
- Azure Security Services.

The bidder shall describe how the proposed solution supports this target operating model and enables future security automation, advanced analytics, AI-assisted investigations and continuous improvement of MIBCO's cybersecurity maturity.

16. RISK MANAGEMENT REQUIREMENTS

16.1 Objectives

MIBCO recognises cybersecurity, operational disruption, technology failure, data loss and service availability as critical organisational risks.

The successful bidder shall provide a comprehensive risk management approach covering the design, implementation, operation, maintenance and continuous improvement of the proposed solution.

The bidder shall demonstrate how risks will be identified, assessed, monitored, mitigated, escalated and reported throughout the contract lifecycle.

The proposed risk management framework shall align with:

- NIST Cybersecurity Framework.
- ISO 27001.
- ISO 27005.
- ISO 31000.
- POPIA.
- PCI-DSS.
- FSCA governance requirements.
- MIBCO internal governance requirements.

16.2 Risk Management Framework

The bidder shall provide a formal and documented risk management framework.

The framework shall include:

Governance

- Risk ownership.
- Risk accountability.
- Decision-making authority.
- Escalation procedures.
- Management reporting.

Risk Lifecycle

- Risk identification.
- Risk assessment.
- Risk treatment.

- Risk monitoring.
- Risk reporting.
- Risk review.

The bidder shall provide copies of its risk management methodology and governance framework.

16.3 Risk Assessment Requirements

The successful bidder shall perform risk assessments during:

Solution Design

- Architecture Review.
- Security Architecture Review.
- Network Design Review.
- Azure Integration Review.

Implementation

- Implementation Readiness Assessment.
- Migration Risk Assessment.
- Security Control Validation.

Operations

- Operational Risk Assessments.
- Security Risk Reviews.
- Capacity Risk Reviews.
- Technology Lifecycle Risk Reviews.

Risk assessments shall be conducted at least annually.

16.4 Risk Registers

The successful bidder shall establish and maintain the following risk registers:

Risk Register	Mandatory
Project Risk Register	Yes
Migration Risk Register	Yes
Operational Risk Register	Yes
Cybersecurity Risk Register	Yes

Service Continuity Risk Register	Yes
Disaster Recovery Risk Register	Yes
Third-Party Risk Register	Yes

Updated risk registers shall be provided during service review meetings.

16.5 Project Risk Management

The bidder shall identify and manage risks associated with:

- Project delays.
- Resource shortages.
- Scope changes.
- Third-party dependencies.
- Migration failures.
- Data loss.
- Service interruptions.
- Technical incompatibilities.

The bidder shall provide a detailed project risk management plan as part of the implementation proposal.

16.6 Migration Risk Management

Migration from the current Cisco Meraki environment shall be treated as a high-risk activity.

The bidder shall provide:

Migration Risk Controls

- Migration Runbook.
- Pre-Migration Validation.
- Configuration Backup Procedures.
- Rollback Procedures.
- Testing Procedures.
- Acceptance Procedures.

The bidder shall identify risks relating to:

- Firewall migration.
- SD-WAN migration.

- User migration.
- Azure integration.
- Security policy migration.
- Internet connectivity migration.

16.7 Cybersecurity Risk Management

The proposed solution shall reduce exposure to cyber threats.

The bidder shall identify controls addressing:

External Threats

- Ransomware.
- Malware.
- Phishing.
- Denial of Service attacks.
- Supply Chain Attacks.
- Advanced Persistent Threats (APT).

Internal Threats

- Insider threats.
- Privilege abuse.
- Unauthorised access.
- Data leakage.
- Policy violations.

Identity Threats

- Account compromise.
- Credential theft.
- MFA fatigue attacks.
- Password spraying.
- Session hijacking.

The bidder shall describe how the proposed solution assists in managing these risks.

16.8 Operational Risk Management

The proposed solution shall minimise operational disruption.

The bidder shall describe controls for:

- Service outages.
- Hardware failures.
- Software failures.
- Misconfigurations.
- Capacity constraints.
- Human error.
- Configuration drift.

The bidder shall provide examples of operational controls included within the managed service offering.

16.9 Business Continuity Risk Management

The solution shall support MIBCO's business continuity objectives.

The bidder shall identify risks relating to:

- Data Centre outages.
- Cloud outages.
- Connectivity failures.
- Security incidents.
- Supplier failures.
- Utility failures.

The solution shall support rapid restoration of services following disruption.

16.10 Disaster Recovery Risk Management

Because MIBCO operates:

- Randburg Production Data Centre.
- Azure South Africa Disaster Recovery Environment.

the bidder shall provide specific controls addressing:

Disaster Recovery Risks

- Replication failure.
- DR connectivity failure.
- Security policy inconsistency.
- Backup failure.

- Recovery process failure.
- Infrastructure availability.

The bidder shall provide documented procedures describing how these risks are managed.

16.11 Third-Party Risk Management

The bidder shall identify and manage risks associated with:

- Outsourced support.
- OEM dependencies.
- Cloud service providers.
- Third-party contractors.
- Integration partners.

The bidder shall disclose any subcontractors involved in delivering the service.

The bidder shall describe:

- Governance controls.
- Security controls.
- Oversight mechanisms.
- Escalation procedures.

16.12 Technology Lifecycle Risk Management

The successful bidder shall proactively manage technology lifecycle risks.

The bidder shall provide:

Lifecycle Management Controls

- End-of-Life Monitoring.
- End-of-Support Monitoring.
- Firmware Currency Reviews.
- Security Vulnerability Assessments.
- Technology Refresh Planning.

The bidder shall notify MIBCO of any technology approaching:

- End-of-Life (EOL).
- End-of-Sale (EOS).
- End-of-Support (EOSS).

A minimum notification period of twelve (12) months shall be provided.

16.13 Vulnerability Management

The proposed solution shall support proactive vulnerability management.

The bidder shall provide:

- Vulnerability Monitoring.
- Vulnerability Reporting.
- Patch Management.
- Remediation Planning.
- Security Advisory Notifications.

The bidder shall define target remediation timelines.

Recommended Timeframes

Severity	Target Remediation
Critical	7 Days
High	14 Days
Medium	30 Days
Low	90 Days

16.14 Risk Monitoring and Reporting

The bidder shall provide ongoing risk reporting.

Monthly Reports

- Security Risks.
- Operational Risks.
- Capacity Risks.
- Compliance Risks.

Quarterly Reports

- Risk Trend Analysis.
- Strategic Risk Review.
- Emerging Threat Review.

- Technology Risk Assessment.

Annual Reports

- Security Posture Assessment.
- Cyber Risk Assessment.
- Technology Roadmap Review.

16.15 Risk Escalation Requirements

The bidder shall maintain formal escalation processes.

The escalation process shall include:

Severity Levels

Severity	Example
Critical	Major outage or cybersecurity incident
High	Significant degradation or elevated risk
Medium	Service impairment
Low	Minor issue or observation

Escalation Requirements

- Technical escalation.
- Management escalation.
- Executive escalation.
- OEM escalation.

Escalation paths shall be documented and included in operational procedures.

16.16 Risk Workshops

The successful bidder shall facilitate risk workshops.

Mandatory Workshops

Workshop	Minimum Frequency
Project Risk Review	Monthly during implementation
Operational Risk Review	Quarterly
Cybersecurity Risk Review	Quarterly

Business Continuity Review	Annually
Disaster Recovery Review	Annually

MIBCO reserves the right to request additional workshops following significant incidents.

16.17 Insurance Requirements

The bidder shall maintain adequate insurance coverage throughout the contract period.

Minimum requirements include:

- Professional Indemnity Insurance.
- Public Liability Insurance.
- Cyber Liability Insurance.

Proof of insurance shall be submitted with the proposal.

The bidder shall immediately notify MIBCO of any changes to insurance coverage during the contract period.

16.18 Incident Risk Management

The bidder shall provide documented procedures for managing:

- Cybersecurity Incidents.
- Data Breaches.
- Service Outages.
- Security Control Failures.
- Identity Compromise.
- Ransomware Events.

The procedures shall include:

- Detection.
- Analysis.
- Containment.
- Eradication.
- Recovery.
- Post-Incident Review.

16.19 Risk-Based Service Improvement

The bidder shall provide a continual improvement programme.

The programme shall identify:

- Emerging Risks.
- Technology Improvements.
- Security Improvements.
- Operational Improvements.
- Compliance Enhancements.

Recommendations shall be presented during quarterly service review meetings.

16.20 Bidder Response Requirements

The bidder shall complete **Annexure G – Risk Register and Risk Management Response Schedule**.

The bidder shall provide:

- Sample Risk Register.
- Risk Management Methodology.
- Risk Escalation Matrix.
- Business Continuity Approach.
- Disaster Recovery Risk Management Approach.

Responses shall indicate:

- Fully Compliant.
- Partially Compliant.
- Non-Compliant.

Failure to comply with mandatory Risk Management requirements may result in the proposal being deemed non-responsive and excluded from further evaluation.

16.21 Mandatory Deliverables

The successful bidder shall provide the following deliverables:

Deliverable	Required
Risk Management Plan	Yes
Project Risk Register	Yes
Cybersecurity Risk Register	Yes
Operational Risk Register	Yes

Disaster Recovery Risk Register	Yes
Business Continuity Risk Register	Yes
Risk Escalation Matrix	Yes
Quarterly Risk Reports	Yes
Annual Security Risk Assessment	Yes

These deliverables shall remain current throughout the contract period and shall form part of MIBCO's governance and oversight framework for the managed service.

17. COMPLIANCE REQUIREMENTS

17.1 Objectives

MIBCO operates within a regulated environment and is required to comply with various legislative, regulatory, governance, cybersecurity and information security obligations.

The proposed solution shall provide capabilities that support MIBCO's compliance obligations and shall enable the organisation to demonstrate compliance through appropriate controls, reporting, monitoring, auditing and evidence collection.

The bidder shall demonstrate how the proposed solution supports compliance requirements through technical controls, administrative controls, monitoring capabilities, reporting mechanisms and audit evidence.

Compliance shall be considered a core functional requirement of the proposed solution and not an optional feature.

17.2 Regulatory and Legislative Compliance

The proposed solution shall support compliance with the following legislation, regulations and governance frameworks.

Mandatory Requirements

Regulatory Requirement	Mandatory
Protection of Personal Information Act (POPIA)	Yes
King IV	Yes
King V	Yes
Pension Funds Act (PFA)	Yes
Financial Sector Conduct Authority (FSCA) Requirements	Yes

Conduct of Financial Institutions (COFI) Requirements	Yes
Payment Card Industry Data Security Standard (PCI-DSS)	Yes

The bidder shall identify the controls within the proposed solution that support each requirement.

17.3 Cybersecurity Framework Compliance

The proposed solution shall support cybersecurity best practices and industry-recognised frameworks.

Mandatory Framework Alignment

Framework	Mandatory
NIST Cybersecurity Framework (CSF)	Yes
ISO 27001	Yes
ISO 27002	Yes
ISO 27005	Yes
ISO 27032	Yes
ISO 42001	Yes

The bidder shall explain how the proposed solution aligns with and supports each framework.

17.4 POPIA Compliance Requirements

The proposed solution shall support MIBCO's obligations under the Protection of Personal Information Act (POPIA).

The bidder shall demonstrate capabilities supporting:

Confidentiality

- Access controls.
- Encryption controls.
- Identity verification.
- Least privilege access.

Integrity

- Audit logging.
- Change management.
- Data integrity validation.

Availability

- Disaster recovery.
- Business continuity.
- Service resilience.

Accountability

- Administrative auditing.
- Reporting.
- Compliance monitoring.

Data Protection

- Data loss prevention.
- Secure transmission.
- Monitoring of unauthorised disclosure.

The bidder shall identify how the proposed solution assists MIBCO in protecting personal information.

17.5 PCI-DSS Compliance Requirements

The proposed solution shall provide controls capable of supporting PCI-DSS compliance where applicable.

Capabilities shall include:

- Network segmentation.
- Firewall controls.
- Access control.
- Encryption.
- Monitoring.
- Logging.
- Vulnerability management.
- Security event monitoring.

The bidder shall identify which PCI-DSS control objectives are supported by the proposed solution.

17.6 Information Security Compliance Requirements

The proposed solution shall support implementation of information security controls relating to:

Access Control

- Authentication.

- Authorisation.
- Least privilege.

Network Security

- Segmentation.
- Threat prevention.
- Secure connectivity.

Data Security

- Encryption.
- Data protection.
- DLP.

Monitoring

- Event logging.
- Monitoring.
- Threat detection.

Incident Response

- Alerting.
- Investigation.
- Containment.

The bidder shall describe available capabilities.

17.7 Security Policy Compliance

The proposed solution shall support the enforcement of MIBCO information security policies.

The bidder shall describe how security policies can be:

- Defined.
- Enforced.
- Monitored.
- Reported.
- Audited.

The solution shall support consistent policy application across:

- Randburg Data Centre.

- Azure DR.
- Branch Offices.
- Remote Users.
- Contractors.

17.8 Audit and Assurance Requirements

The proposed solution shall support internal and external audit processes.

Audit Requirements

The solution shall maintain audit records for:

- Administrative Activities.
- Authentication Events.
- Configuration Changes.
- Security Events.
- Access Requests.
- Policy Changes.

The solution shall support:

- Audit evidence collection.
- Audit reporting.
- Historical reporting.
- Event reconstruction.

The bidder shall identify any limitations.

17.9 Compliance Monitoring Requirements

The proposed solution shall provide capabilities enabling continuous compliance monitoring.

Capabilities shall include:

- Configuration Compliance Monitoring.
- Security Policy Monitoring.
- Device Compliance Monitoring.
- User Compliance Monitoring.
- Patch Compliance Monitoring.

The bidder shall describe mechanisms for detecting and reporting non-compliance.

17.10 Compliance Reporting Requirements

The solution shall provide compliance reporting capabilities.

Regulatory Reporting

Reports shall support:

- POPIA.
- PCI-DSS.
- FSCA.
- Governance reporting.

Security Reporting

Reports shall include:

- Security posture.
- Security policy compliance.
- Access control compliance.
- Device compliance.

Executive Reporting

Reports shall include:

- Compliance status.
- Compliance trends.
- Compliance gaps.
- Risk indicators.

Reports shall be available on demand and scheduled.

17.11 Log Retention and Audit Trail Compliance

The proposed solution shall support retention requirements necessary for audit and compliance purposes.

Minimum Requirements

Requirement	Mandatory
Online Log Retention	30 Days
Archived Log Retention	5 Years
Searchable Audit Records	Yes

Tamper Resistant Audit Logs	Yes
Exportable Audit Records	Yes

The bidder shall describe:

- Archiving methodology.
- Integrity validation.
- Retrieval process.

17.12 Encryption Compliance Requirements

The proposed solution shall support approved encryption standards.

Mandatory Standards

Standard	Mandatory
TLS 1.3	Yes
AES-256	Yes
SHA-256 or Higher	Yes
IPsec IKEv2	Yes
Perfect Forward Secrecy	Yes

The bidder shall describe:

- Encryption implementation.
- Key management.
- Certificate management.

17.13 Security Certification Requirements

The proposed solution shall support recognised security certifications.

Mandatory Requirements

Certification	Requirement
FIPS 140-2 or FIPS 140-3	Mandatory
Common Criteria	Preferred where available
Manufacturer Security Certifications	Mandatory

The bidder shall submit evidence supporting certification claims.

17.14 Data Residency and Data Sovereignty Requirements

The proposed solution shall support MIBCO's data governance requirements.

The bidder shall disclose:

- Location of management services.
- Location of data storage.
- Location of log storage.
- Location of security analytics services.
- Location of support services.

The bidder shall identify any data that leaves South Africa.

The bidder shall identify controls protecting such information.

17.15 Vulnerability and Patch Compliance

The successful bidder shall provide processes supporting:

- Vulnerability monitoring.
- Vulnerability reporting.
- Patch monitoring.
- Patch deployment.
- Security updates.

The bidder shall support compliance reporting relating to vulnerability management activities.

17.16 Third-Party Compliance Requirements

The bidder shall identify all third parties involved in:

- Service delivery.
- Support services.
- Cloud services.
- Professional services.
- Security operations.

The bidder shall identify:

- Compliance certifications.
- Security controls.

- Governance controls.

MIBCO reserves the right to assess third-party compliance posture.

17.17 Compliance Governance

The successful bidder shall participate in compliance governance activities.

This shall include:

Monthly Activities

- Compliance reviews.
- Security review meetings.
- Service review meetings.

Quarterly Activities

- Compliance status reviews.
- Risk reviews.
- Control effectiveness reviews.

Annual Activities

- Compliance assessments.
- Security posture assessments.
- Strategic compliance reviews.

17.18 Compliance Exceptions Management

The bidder shall provide documented procedures for managing compliance exceptions.

The procedures shall include:

- Identification of exceptions.
- Risk assessment.
- Approval process.
- Remediation planning.
- Exception reporting.

The bidder shall describe how exceptions are tracked and managed.

17.19 Compliance Deliverables

The successful bidder shall provide the following deliverables:

Deliverable	Required
Compliance Matrix	Yes
Compliance Reporting Framework	Yes
Security Control Mapping	Yes
Audit Evidence Procedures	Yes
Regulatory Reporting Templates	Yes
Annual Compliance Assessment Support	Yes

17.20 Bidder Response Requirements

The bidder shall complete the Compliance Response Schedule contained within **Annexure A – Compliance Matrix**.

For each requirement the bidder shall indicate:

- Fully Compliant.
- Partially Compliant.
- Non-Compliant.

Supporting evidence shall be provided for all compliance claims.

The bidder shall cross-reference proposed controls to the compliance requirements contained within this section.

Failure to comply with mandatory compliance requirements may result in the proposal being deemed non-responsive and excluded from further evaluation.

17.21 Compliance Roadmap and Continuous Improvement

The bidder shall provide recommendations for improving MIBCO's cybersecurity and compliance maturity over the term of the contract.

The roadmap shall identify:

Year 1

- Foundational Controls.
- Compliance Baseline.
- Security Control Optimisation.

Year 2

- Advanced Security Monitoring.
- Zero Trust Maturity Enhancements.
- Compliance Automation.

Year 3

- Continuous Compliance Monitoring.
- Advanced Analytics.
- Security and Compliance Optimisation.

The bidder shall explain how the proposed solution supports continual improvement and evolving regulatory requirements throughout the contract period.

18. SERVICE MANAGEMENT REQUIREMENTS

18.1 Objectives

The successful bidder shall provide a mature, IT service management-driven operating model that ensures the Secure Network and Cybersecurity Service remains secure, resilient, available and aligned with MIBCO's business requirements throughout the contract period.

The service management model shall be proactive rather than reactive and shall focus on:

- Service quality.
- Service availability.
- Cybersecurity resilience.
- Continuous improvement.
- Customer satisfaction.
- Risk reduction.
- Operational efficiency.
- Governance and reporting.

The bidder shall provide a detailed description of the proposed service management framework.

18.2 Service Management Framework

The successful bidder shall operate the service using recognised service management practices.

Preference will be given to service providers operating according to recognised frameworks, including:

- ITIL.
- ISO 20000.

- COBIT.
- ISO 27001 Service Management Controls.

The bidder shall describe:

- The service management framework used.
- Governance structure.
- Operational management processes.
- Escalation framework.
- Service review model.

18.3 Service Delivery Model

The bidder shall provide a fully managed service incorporating:

Service Governance

- Service ownership.
- Service accountability.
- Service reporting.
- Executive stakeholder engagement.

Technical Operations

- Platform monitoring.
- Security monitoring.
- Capacity management.
- Configuration management.

Service Operations

- Incident management.
- Problem management.
- Change management.
- Request fulfilment.

Vendor Management

- OEM engagement.
- Escalation management.
- Warranty management.

- Subscription management.

18.4 Service Desk Requirements

The successful bidder shall provide a Service Desk for the logging, management and escalation of support requests.

Service Desk Availability

Requirement	Mandatory
Business Hours Support	Yes
24x7 Critical Support	Yes
Telephone Support	Yes
Email Support	Yes
Web Portal Support	Yes

Service Desk Functions

The Service Desk shall provide:

- Incident logging.
- Service request logging.
- Escalation management.
- Communication management.
- Service tracking.
- Status updates.

18.5 Incident Management

The bidder shall provide a documented Incident Management process.

Incident Management Objectives

The process shall support:

- Rapid incident identification.
- Incident classification.
- Incident prioritisation.
- Escalation and resolution.
- Business impact reduction.

Mandatory Incident Information

Each incident shall include:

- Incident number.
- Description.
- Severity.
- Root cause (where known).
- Resolution actions.
- Resolution time.
- Closure information.

18.6 Incident Severity Classification

The bidder shall classify incidents according to business impact.

Severity	Definition
Critical	Complete business service outage or significant cybersecurity incident
High	Significant impact on service delivery
Medium	Limited impact affecting selected users or systems
Low	Minor issue with limited operational impact

18.7 Problem Management

The bidder shall maintain a Problem Management process.

The process shall support:

- Root cause analysis.
- Trend identification.
- Prevention of recurring incidents.
- Corrective action planning.
- Known error management.

Problem Management Deliverables

The bidder shall provide:

- Problem reports.
- Root cause analysis reports.

- Corrective action recommendations.
- Trend analysis reports.

18.8 Change Management

The bidder shall manage all changes affecting the service.

Change Categories

Change Type	Description
Standard Change	Pre-approved low-risk change
Normal Change	Planned change requiring approval
Emergency Change	Urgent change required to restore service

Change Requirements

The process shall include:

- Change requests.
- Risk assessments.
- Impact analysis.
- Testing requirements.
- Approval processes.
- Post-implementation reviews.

MIBCO must approve all material changes affecting production services.

18.9 Configuration Management

The bidder shall maintain accurate configuration information for all service components.

Configuration Management Requirements

The configuration repository shall include:

- Hardware inventory.
- Software inventory.
- Licensing inventory.
- Network diagrams.
- Configuration baselines.
- Security policies.

Configuration records shall be maintained throughout the contract period.

18.10 Asset Management

The bidder shall maintain accurate inventories of all assets utilised in delivering the service.

The inventory shall include:

- Firewalls.
- SD-WAN appliances.
- Management platforms.
- Licences.
- Cloud services.
- Security services.

MIBCO shall have access to asset reporting upon request.

18.11 Capacity Management

The bidder shall continuously monitor service capacity.

Capacity management shall include:

- Bandwidth utilisation.
- Device utilisation.
- Session utilisation.
- Security event volumes.
- Cloud resource utilisation.

The bidder shall provide proactive recommendations when capacity thresholds are approached.

Capacity Thresholds

The bidder shall notify MIBCO when utilisation exceeds:

Metric	Threshold
Device Utilisation	70%
Throughput Utilisation	70%
Session Capacity	70%
Storage Capacity	80%

18.12 Availability Management

The bidder shall actively manage service availability.

Minimum Service Availability

Service	Min Availability
Managed Service Platform	99.9%
Security Services	99.9%
SD-WAN Services	99.9%
Management Platform	99.9%

The bidder shall provide:

- Availability monitoring.
- Availability reporting.
- Availability improvement plans.

18.13 Service Continuity Management

The bidder shall provide Service Continuity Management procedures.

The procedures shall support:

- Disaster recovery.
- Business continuity.
- Service restoration.
- Recovery planning.
- Recovery testing.

The bidder shall participate in annual service continuity reviews.

18.14 Security Service Management

The bidder shall provide operational management for all security services.

Security Management Activities

- Security policy administration.
- Threat intelligence updates.
- Security tuning.
- Signature updates.

- Threat monitoring.
- Security reporting.

The bidder shall provide evidence of regular security maintenance activities.

18.15 Supplier and OEM Management

The bidder shall manage all OEM and supplier relationships necessary to deliver the service.

Responsibilities shall include:

- Escalation management.
- Vendor support cases.
- Warranty administration.
- Subscription renewals.
- Product lifecycle management.

MIBCO shall not be required to interact directly with OEMs for operational matters.

18.16 Service Reporting Requirements

The bidder shall provide detailed operational reporting.

Monthly Reports

The following minimum information shall be included:

- SLA performance.
- Availability statistics.
- Incident summary.
- Security incident summary.
- Capacity statistics.
- Risk summary.
- Change summary.

Quarterly Reports

- Strategic service review.
- Security posture review.
- Capacity planning review.
- Technology roadmap review.
- Service improvement recommendations.

18.17 Service Review Meetings

The successful bidder shall conduct structured service review meetings.

Monthly Operational Review

Agenda shall include:

- Incident review.
- SLA performance.
- Security events.
- Capacity review.
- Outstanding actions.

Quarterly Service Review

Agenda shall include:

- Strategic review.
- Risk review.
- Technology review.
- Compliance review.
- Continuous improvement initiatives.

18.18 Continual Service Improvement (CSI)

The bidder shall maintain a Continual Service Improvement programme.

The programme shall identify:

- Security improvements.
- Performance improvements.
- Service improvements.
- Cost optimisation opportunities.
- Process improvements.

Recommendations shall be formally presented during Quarterly Service Reviews.

18.19 Escalation Management

The bidder shall maintain a documented escalation framework.

The framework shall include:

Technical Escalation

- Level 1 Support.
- Level 2 Support.
- Level 3 Support.
- OEM Support.

Management Escalation

- Service Delivery Manager.
- Operations Manager.
- Executive Sponsor.

Escalation contact details shall be maintained throughout the contract period.

18.20 Service Management Tooling

The bidder shall provide access to service management tooling.

The tooling shall support:

- Incident logging.
- Request tracking.
- Change management.
- Status monitoring.
- SLA tracking.
- Reporting.

The bidder shall identify whether integration with GLPI is supported.

18.21 Service Transition Requirements

The implementation phase shall conclude with a formal service transition process.

The transition shall include:

- Knowledge transfer.
- Documentation handover.
- Operational acceptance testing.
- Support readiness review.
- Service acceptance.

The service shall not be considered operational until MIBCO formally accepts the service.

18.22 Service Management Team Requirements

The bidder shall identify all personnel responsible for delivery of the service.

The submission shall include:

Role	Mandatory
Service Delivery Manager	Yes
Technical Architect	Yes
Security Specialist	Yes
Network Specialist	Yes
Escalation Manager	Yes
Project Manager	Yes

Resumes and certifications shall be included where applicable.

18.23 Key Performance Indicators (KPIs)

The bidder shall report against agreed KPIs including:

- SLA compliance.
- Service availability.
- Incident response times.
- Incident resolution times.
- Change success rate.
- Customer satisfaction.
- Security service effectiveness.

Additional KPIs may be agreed during contract negotiations.

18.24 Bidder Response Requirements

The bidder shall provide:

- Service Management Methodology.
- Service Delivery Model.
- Service Governance Model.
- Escalation Matrix.

- Service Review Process.
- Service Reporting Examples.
- Sample Monthly Report.
- Sample Quarterly Service Review Pack.

The bidder shall complete the Service Management Response Schedule included in the relevant Annexure.

Failure to comply with mandatory Service Management requirements may result in the proposal being deemed non-responsive and excluded from further evaluation.

19. IMPLEMENTATION REQUIREMENTS

19.1 Objectives

The successful bidder shall provide a comprehensive implementation approach that ensures the successful transition from the existing Cisco Meraki environment to the proposed Secure Network and Cybersecurity Service (SNaaS) with minimal disruption to MIBCO business operations.

The implementation approach shall be designed to:

- Minimise operational risk.
- Minimise service interruption.
- Maintain cybersecurity controls throughout the implementation.
- Ensure continuity of business operations.
- Ensure knowledge transfer to MIBCO personnel.
- Ensure a successful transition into operational support.

The bidder shall provide a detailed implementation methodology covering all phases of the project lifecycle.

19.2 Project Governance

The bidder shall establish a formal project governance structure.

The governance model shall include:

Project Steering Committee

Participants shall include:

- MIBCO Executive Sponsor.
- MIBCO ICT Management.
- MIBCO Project Manager
- Service Provider Project Manager.
- Service Provider Technical Architect.

Project Management

The successful bidder shall appoint:

Role	Mandatory
Project Manager	Yes
Technical Architect	Yes
Lead Security Consultant	Yes
Lead Network Engineer	Yes
Service Transition Manager	Yes

The bidder shall provide details of all proposed resources.

19.3 Project Methodology

The bidder shall provide a structured implementation methodology.

The methodology shall include, at a minimum:

Phase 1 – Initiation

- Project Kick-Off.
- Project Charter.
- Stakeholder Identification.
- Project Governance Establishment.
- Communication Plan Development.

Phase 2 – Discovery

- Current State Assessment.
- Infrastructure Assessment.
- Security Assessment.
- Azure Environment Assessment.
- Branch Connectivity Assessment.
- Risk Assessment.

Phase 3 – Design

- High-Level Design (HLD).
- Low-Level Design (LLD).

- Security Architecture Design.
- Azure DR Architecture Design.
- Network Segmentation Design.

Phase 4 – Build

- Solution Provisioning.
- Configuration.
- Integration.
- Security Policy Configuration.
- Management Platform Configuration.

Phase 5 – Validation

- System Testing.
- Security Testing.
- Performance Testing.
- Integration Testing.
- User Acceptance Testing.

Phase 6 – Migration

- Production Cutover.
- Validation.
- Monitoring.
- Issue Resolution.

Phase 7 – Hypercare

- Enhanced Support.
- Performance Monitoring.
- Issue Resolution.
- Optimisation.

Phase 8 – Operational Handover

- Knowledge Transfer.
- Documentation Handover.
- Service Acceptance.

- Transition to Operations.

19.4 Discovery and Assessment Requirements

The bidder shall conduct a detailed assessment of the current environment.

The assessment shall include:

Infrastructure Assessment

- Cisco Meraki MX67.
- Cisco Meraki MX100.
- Cisco Meraki MX105.
- Existing SD-WAN Configuration.
- Existing VPN Configuration.
- Existing Internet Connectivity.

Security Assessment

- Firewall Policies.
- Access Control Policies.
- Security Zones.
- Segmentation Requirements.
- Threat Protection Controls.

Cloud Assessment

- Azure Connectivity.
- Azure VPN Configuration.
- Azure DR Environment.
- Azure Security Controls.

Deliverable:

- Current State Assessment Report.

19.5 Design Requirements

The bidder shall develop a comprehensive future-state design.

Mandatory Deliverables

Deliverable	Required
High-Level Design (HLD)	Yes
Low-Level Design (LLD)	Yes
Security Architecture	Yes
SD-WAN Architecture	Yes
Azure DR Architecture	Yes
Network Segmentation Design	Yes
ZTNA Design	Yes
Operational Design	Yes

All design documentation shall be reviewed and approved by MIBCO prior to implementation.

19.6 Architecture Review Workshops

The bidder shall conduct formal architecture workshops with MIBCO.

Workshops shall include:

Security Architecture Workshop

Review:

- Security Controls.
- Zero Trust Design.
- Segmentation Model.
- Threat Prevention Capabilities.

Network Architecture Workshop

Review:

- SD-WAN Architecture.
- Routing Design.
- Branch Connectivity.

- Azure Integration.

Operational Architecture Workshop

Review:

- Monitoring Architecture.
- Reporting Architecture.
- SOC Integration.
- Service Management.

Approval of architecture documentation shall be a mandatory project milestone.

19.7 Build and Configuration Requirements

The bidder shall configure all solution components.

Configuration activities shall include:

Security Services

- Firewall Policies.
- IPS Policies.
- Malware Policies.
- DNS Security Policies.
- URL Filtering Policies.

Zero Trust Services

- Identity Integration.
- MFA Integration.
- Device Posture Policies.
- ZTNA Policies.

SOC Integration

- Wazuh Integration.
- Grafana Integration.
- N8N Integration.
- API Configuration.

Azure Integration

- Azure VPN Configuration.

- Azure Routing.
- Azure Policy Integration.

19.8 Migration Requirements

The bidder shall provide a comprehensive migration strategy.

The migration plan shall include:

- Detailed Migration Activities.
- Migration Sequence.
- Migration Dependencies.
- Rollback Procedures.
- Validation Procedures.
- User Communication Plan.

The bidder shall identify all migration risks and associated mitigation measures.

19.9 Cutover Requirements

A formal cutover plan shall be developed.

The cutover plan shall include:

- Detailed Task Schedule.
- Resource Allocation.
- Escalation Procedures.
- Technical Validation Steps.
- Acceptance Criteria.

The plan shall be reviewed and approved by MIBCO before execution.

19.10 Rollback Requirements

The bidder shall provide a tested rollback strategy.

Rollback procedures shall include:

- Configuration Backups.
- Recovery Procedures.
- Reversion Activities.
- Validation Procedures.

The rollback strategy shall ensure the restoration of services within the agreed service restoration objectives.

19.11 Testing Requirements

The bidder shall provide a formal testing programme.

Functional Testing

The testing programme shall validate:

- Firewall Policies.
- SD-WAN Operation.
- ZTNA Functionality.
- CASB Functionality.
- DLP Functionality.
- SWG Functionality.

Integration Testing

The testing programme shall validate:

- Entra ID Integration.
- Intune Integration.
- Defender Integration.
- Wazuh Integration.
- Azure Integration.

Security Testing

The testing programme shall validate:

- Authentication Controls.
- Device Posture Checks.
- Threat Prevention.
- IPS Functionality.
- Logging and Reporting.

19.12 User Acceptance Testing (UAT)

The bidder shall facilitate User Acceptance Testing.

The UAT Plan shall include:

- Test Scripts.
- Success Criteria.

- Test Data.
- Test Participants.
- Defect Management Procedures.

The environment shall not proceed to production until UAT has been successfully completed and approved by MIBCO.

19.13 Performance Validation

The proposed solution shall undergo performance validation before production deployment.

The bidder shall validate:

Requirement	Validation Required
NGFW Throughput	Yes
Threat Prevention Throughput	Yes
SSL Inspection Throughput	Yes
SD-WAN Performance	Yes
ZTNA Performance	Yes
Azure Connectivity Performance	Yes

The bidder shall provide documented evidence of successful testing.

19.14 Security Validation

The bidder shall perform security validation activities including:

- Security Policy Validation.
- Threat Prevention Validation.
- Access Control Validation.
- Segmentation Validation.
- Logging Validation.

The bidder shall provide a Security Validation Report.

19.15 Disaster Recovery Validation

The bidder shall validate:

- Azure DR Connectivity.
- Security Policy Synchronisation.

- DR Access Controls.
- Logging Continuity.
- Failover Connectivity.

The bidder shall provide a Disaster Recovery Validation Report.

19.16 Documentation Requirements

The bidder shall provide complete project documentation.

Mandatory Documentation

Document	Required
Project Plan	Yes
High-Level Design	Yes
Low-Level Design	Yes
As-Built Documentation	Yes
Security Design	Yes
Migration Plan	Yes
Rollback Plan	Yes
Operational Procedures	Yes
Support Procedures	Yes
Training Material	Yes

Documentation shall be supplied in editable Microsoft Office format.

19.17 Knowledge Transfer Requirements

The bidder shall provide formal knowledge transfer sessions to MIBCO personnel.

Training shall be delivered to:

- Network Administrators.
- Security Administrators.
- Service Delivery Personnel.
- SOC Personnel.

Knowledge transfer shall include practical demonstrations and operational procedures.

19.18 Hypercare Requirements

Following production cutover, the bidder shall provide a Hypercare support period.

Minimum Hypercare Requirements

Requirement	Minimum
Hypercare Period	30 Days
Daily Monitoring	Yes
Daily Status Reporting	Yes
Escalated Support	Yes

The bidder shall identify all Hypercare resources.

19.19 Service Transition Requirements

Prior to project closure, the bidder shall complete a formal service transition process.

Activities shall include:

- Operational Readiness Review.
- Documentation Handover.
- Support Handover.
- Knowledge Transfer Completion.
- Service Acceptance Review.

The service shall only transition into operational support after written acceptance by MIBCO.

19.20 Project Plan Requirements

The bidder shall submit a detailed project plan including:

- Activities.
- Milestones.
- Deliverables.
- Dependencies.
- Resource Assignments.
- Critical Path.

The project plan shall clearly identify:

- Discovery Phase.

- Design Phase.
- Build Phase.
- Testing Phase.
- Migration Phase.
- Hypercare Phase.
- Operational Handover Phase.

19.21 Project Reporting Requirements

The bidder shall provide:

Weekly Reports

- Progress Status.
- Risks.
- Issues.
- Actions.
- Milestones.

Monthly Reports

- Schedule Performance.
- Deliverable Status.
- Budget Status.
- Risk Status.

The format shall be approved by MIBCO during project initiation.

19.22 Mandatory Project Deliverables

The successful bidder shall deliver the following:

Governance Deliverables

- Project Charter.
- Project Plan.
- Stakeholder Register.
- Communications Plan.

Design Deliverables

- HLD.

- LLD.
- Security Architecture.
- Azure Architecture.

Implementation Deliverables

- Migration Plan.
- Test Plan.
- Rollback Plan.
- Validation Reports.

Operations Deliverables

- As-Built Documentation.
- SOPs.
- Knowledge Transfer Material.
- Support Documentation.

Closure Deliverables

- Operational Acceptance Certificate.
- Project Closure Report.
- Lessons Learnt Report.

19.23 Bidder Response Requirements

The bidder shall complete the Implementation Response Schedule included in the relevant Annexure.

The bidder shall provide:

- Proposed Project Methodology.
- Detailed Project Plan.
- Resource Plan.
- Governance Structure.
- Risk Management Approach.
- Migration Approach.
- Testing Approach.
- Hypercare Approach.

Failure to comply with mandatory implementation requirements may result in the proposal being deemed non-responsive and excluded from further evaluation.

20. TRAINING AND KNOWLEDGE TRANSFER REQUIREMENTS

20.1 Objectives

MIBCO requires that the successful bidder provide comprehensive training and knowledge transfer services to ensure that MIBCO personnel can effectively govern, manage, monitor, support and oversee the proposed Secure Network and Cybersecurity Service throughout the contract period.

The primary objective of the training and knowledge transfer programme is to:

- Reduce operational dependency on the service provider.
- Enhance MIBCO internal skills and knowledge.
- Improve cybersecurity awareness.
- Improve operational effectiveness.
- Support effective governance and oversight.
- Improve incident response capabilities.
- Support business continuity and succession planning.

The training programme shall cater for both technical and non-technical stakeholders.

20.2 Training Principles

The training programme shall be:

- Role-based.
- Practical.
- Technology-specific.
- Outcome-focused.
- Delivered by suitably qualified resources.
- Supported by formal training materials.

Training shall include both theoretical and hands-on practical sessions.

The bidder shall provide a detailed Training and Knowledge Transfer Plan as part of the proposal submission.

20.3 Training Audience

The bidder shall provide training appropriate to the following stakeholder groups:

Functions	Required
MIBCO Network Administrators	Yes
MIBCO Security Administrators	Yes
SOC Analysts	Yes
ICT Management	Yes
Service Delivery Personnel	Yes
Business Continuity Personnel	Yes
Audit and Governance Representatives	Yes

The bidder shall identify the recommended training programme for each function.

20.4 Technical Administration Training

The successful bidder shall provide technical administration training covering all components of the proposed solution.

The training shall include:

Platform Administration

- Solution Architecture.
- Component Overview.
- Management Interfaces.
- Administrative Functions.
- Platform Maintenance.

Security Administration

- Security Policy Administration.
- Access Control Administration.
- Zero Trust Administration.
- Threat Prevention Administration.
- Incident Investigation.

Network Administration

- SD-WAN Administration.
- Routing Configuration.
- Site Management.
- Connectivity Monitoring.
- Troubleshooting.

Training shall include practical exercises.

20.5 Security Operations Centre Training

The bidder shall provide dedicated training for MIBCO SOC personnel.

The training shall include:

Security Monitoring

- Threat Monitoring.
- Event Correlation.
- Alert Investigation.
- Log Analysis.
- Threat Intelligence.

Security Analytics

- Dashboard Usage.
- Reporting.
- Threat Hunting.
- Behaviour Analytics.
- MITRE ATT&CK Mapping.

Incident Management

- Incident Investigation.
- Incident Escalation.
- Incident Documentation.
- Containment Procedures.

The bidder shall include examples based on the proposed solution.

20.6 Zero Trust Training

The bidder shall provide specialised training covering the Zero Trust architecture implemented for MIBCO.

Training shall include:

- Zero Trust Principles.
- Identity-Based Security.
- Device Trust Validation.
- Conditional Access Integration.
- Risk-Based Access Control.
- Continuous Verification.

The training shall explain how Zero Trust is implemented within the MIBCO environment.

20.7 Identity and Access Management Training

Training shall be provided covering:

Identity Management

- Microsoft Entra ID Integration.
- Authentication Flows.
- Identity Governance.
- Access Reviews.

Access Control

- Role-Based Access Control.
- Conditional Access Policies.
- Device Compliance Controls.
- Contractor Access Controls.

Administration

- User Access Administration.
- Privileged Access Controls.
- Role Management.

20.8 Hybrid Data Centre and Azure Training

The bidder shall provide training relating to the hybrid architecture implemented for MIBCO.

Training shall cover:

Randburg Data Centre

- Architecture Overview.

- Firewall Architecture.
- Security Controls.
- Segmentation Design.

Azure Disaster Recovery Environment

- Azure Connectivity.
- Azure Security Controls.
- DR Architecture.
- Failover Procedures.

Operational Management

- Monitoring.
- Troubleshooting.
- Reporting.
- Recovery Validation.

20.9 Reporting and Analytics Training

The bidder shall provide training on:

Reporting

- Executive Reporting.
- Operational Reporting.
- Compliance Reporting.
- Security Reporting.

Analytics

- Security Dashboards.
- Risk Reporting.
- Threat Monitoring.
- Capacity Reporting.

Users shall be trained on report customisation and report generation capabilities.

20.10 Operational Support Training

Training shall be provided covering operational support procedures.

Topics shall include:

Incident Management

- Incident Logging.
- Incident Escalation.
- Incident Resolution.

Change Management

- Change Requests.
- Risk Assessments.
- Change Approvals.

Service Management

- Service Reviews.
- SLA Monitoring.
- Vendor Escalation Procedures.

20.11 Disaster Recovery Training

The bidder shall provide training relating to disaster recovery and business continuity operations.

Topics shall include:

- Disaster Recovery Architecture.
- Failover Procedures.
- Failback Procedures.
- Security During Failover.
- DR Testing Procedures.
- Recovery Validation.

The training shall include practical demonstrations using the implemented architecture.

20.12 Knowledge Transfer Requirements

The successful bidder shall conduct formal knowledge transfer activities throughout the implementation project.

Knowledge transfer shall not be limited to formal classroom training.

Knowledge transfer shall occur during:

- Discovery Workshops.
- Design Workshops.

- Build Activities.
- Testing Activities.
- Migration Activities.
- Hypercare Activities.

The bidder shall identify how knowledge transfer will be achieved during each project phase.

20.13 Documentation Requirements

The bidder shall provide comprehensive documentation to support knowledge transfer.

Architecture Documentation

- High-Level Design (HLD).
- Low-Level Design (LLD).
- Security Architecture.
- Azure DR Architecture.
- Segmentation Design.

Operational Documentation

- Administration Guide.
- Operations Guide.
- Support Procedures.
- Escalation Procedures.
- Incident Response Procedures.

User Documentation

- Quick Reference Guides.
- User Administration Guides.
- Reporting Guides.

All documentation shall be supplied in editable Microsoft Office format and PDF format.

20.14 Train-the-Trainer Requirements

The bidder shall provide a train-the-trainer programme to selected MIBCO personnel.

The objective of this programme is to enable MIBCO personnel to:

- Deliver future training internally.
- Support operational onboarding.

- Support knowledge retention.
- Reduce future training costs.

The bidder shall identify the recommended number of participants.

20.15 Knowledge Transfer Workshops

The bidder shall conduct structured knowledge transfer workshops covering:

Workshop	Required
Solution Architecture Workshop	Yes
Security Architecture Workshop	Yes
Azure DR Workshop	Yes
Zero Trust Workshop	Yes
Operations Workshop	Yes
SOC Workshop	Yes
Reporting Workshop	Yes
Disaster Recovery Workshop	Yes

Attendance registers and workshop materials shall be provided.

20.16 Training Deliverables

The bidder shall provide the following minimum deliverables:

Deliverable	Required
Training Plan	Yes
Training Schedule	Yes
Training Material	Yes
Training Manuals	Yes
Practical Lab Material	Yes
Attendance Registers	Yes
Training Assessment Results	Yes

Knowledge Transfer Plan	Yes

20.17 Training Assessments

The bidder shall assess participant understanding and competency.

Assessments may include:

- Practical Exercises.
- Knowledge Assessments.
- Hands-On Demonstrations.
- Operational Scenario Exercises.

The bidder shall provide assessment results to MIBCO.

20.18 Hypercare Knowledge Transfer

During the Hypercare period, the bidder shall provide additional coaching and mentoring.

Activities shall include:

- Daily Operational Reviews.
- Issue Resolution Walkthroughs.
- Administrative Coaching.
- SOC Coaching.

The objective is to ensure MIBCO personnel become fully familiar with the implemented solution.

20.19 Ongoing Skills Development

The bidder shall identify any ongoing training opportunities available during the contract period.

This may include:

- Product Updates.
- New Feature Training.
- Security Awareness Sessions.
- Technology Roadmap Briefings.

Preference may be given to bidders that include ongoing training as part of the managed service offering.

20.20 Training Facilities and Delivery Methods

The bidder shall identify available delivery methods including:

- Classroom Training.
- Virtual Training.

- On-Site Training.
- Hands-On Workshops.
- Self-Paced Learning.

The bidder shall indicate the recommended delivery method for each training module.

20.21 Certification Training

The bidder shall indicate whether formal OEM certification training is available for:

- Firewall Administration.
- SD-WAN Administration.
- Security Administration.
- Zero Trust Administration.

The bidder shall separately identify:

- Included Training.
- Optional Training.
- Certification Examination Costs.

20.22 Knowledge Retention Requirements

The bidder shall implement measures to ensure knowledge is retained after project completion.

The proposal shall include:

- Documentation Repository.
- Training Record Repository.
- Standard Operating Procedures.
- Recorded Training Sessions (where available).

MIBCO shall have unrestricted access to all training and knowledge transfer materials.

20.23 Success Criteria

The training and knowledge transfer programme shall be considered successful when:

- Training has been completed.
- Documentation has been delivered.
- Knowledge transfer activities have been completed.
- MIBCO personnel have demonstrated operational readiness.
- MIBCO has accepted the training deliverables.

20.24 Bidder Response Requirements

The bidder shall provide:

- Training Strategy.
- Training Methodology.
- Knowledge Transfer Methodology.
- Training Schedule.
- List of Training Courses.
- Sample Training Material.
- Resource Profiles for Trainers.
- Training Deliverables.

The bidder shall complete the Training and Knowledge Transfer Response Schedule included in the relevant Annexure.

Failure to comply with mandatory Training and Knowledge Transfer requirements may result in the proposal being deemed non-responsive and excluded from further evaluation.

21. SERVICE LEVEL REQUIREMENTS

21.1 Objectives

The purpose of this section is to define the minimum service levels that the successful bidder shall provide to ensure that MIBCO receives a secure, reliable, high-performing and professionally managed Secure Network and Cybersecurity Service throughout the contract period.

The bidder shall provide a proposed Service Level Agreement (SLA) that meets or exceeds the requirements contained in this section.

MIBCO reserves the right to negotiate improved service levels during contract finalisation.

21.2 General Service Level Principles

The successful bidder shall provide:

- Proactive service management.
- Proactive monitoring.
- Proactive maintenance.
- Incident prevention.
- Continuous service improvement.
- Security operations support.
- Capacity management.

- Service reporting.

The bidder shall provide clear service level commitments and measurement methodologies.

21.3 Service Availability Requirements

The proposed solution shall achieve the following minimum availability levels.

Core Services

Service	Minimum Availability
Managed Security Service	99.90%
NGFW Services	99.90%
SD-WAN Services	99.90%
ZTNA Services	99.90%
Management Portal	99.90%
Reporting Services	99.90%

Availability shall be measured monthly.

Scheduled maintenance approved by MIBCO may be excluded from availability calculations.

21.4 Service Hours

The bidder shall provide support services as follows.

Service	Requirement
Monitoring	24x7x365
Critical Incident Support	24x7x365
Security Incident Response	24x7x365
Service Desk	Business Hours Minimum
Escalation Management	24x7x365
OEM Escalation	24x7x365

21.5 Incident Response Times

The bidder shall respond to incidents according to the following minimum requirements.

Incident Response SLA

Severity	Description	Response Time
Critical	Complete service outage or significant cybersecurity incident	30 Minutes
High	Major degradation affecting multiple users or sites	1 Hour
Medium	Service issue affecting a limited number of users	4 Hours
Low	Minor issue or service request	1 Business Day

Response time refers to acknowledgement and commencement of investigation.

21.6 Incident Restoration Targets

The bidder shall provide the following restoration objectives.

Incident Restoration SLA

Severity	Target Restoration Time
Critical	4 Hours
High	8 Hours
Medium	24 Hours
Low	Best Effort

Where restoration cannot be achieved within agreed targets, the bidder shall provide:

- Cause of delay.
- Escalation status.
- Estimated restoration plan.
- Risk mitigation plan.

21.7 Cybersecurity Incident SLA

The bidder shall provide dedicated response capabilities for cybersecurity incidents.

Security Incident Categories

Category	Response Time
Active Ransomware Event	15 Minutes
Confirmed Security Breach	15 Minutes
Compromised Administrator Account	15 Minutes

Malware Outbreak	30 Minutes
Data Exfiltration Event	30 Minutes
Critical Threat Detection	30 Minutes

Security incidents shall be escalated immediately to designated MIBCO personnel.

21.8 Service Request SLA

The bidder shall provide service request fulfilment targets.

Request Type	Target Completion Time
New User Access	1 Business Day
Firewall Rule Change	2 Business Days
Security Policy Change	2 Business Days
Standard Configuration Change	3 Business Days
Reporting Request	2 Business Days
Documentation Request	2 Business Days

Urgent requests may be escalated according to the agreed change management process.

21.9 Change Management SLA

Changes shall be processed according to the following targets.

Standard Changes

- Implemented within agreed maintenance windows.

Normal Changes

- Assessed within 2 business days.
- Scheduled following approval.

Emergency Changes

- Implemented immediately following authorisation.
- Retrospective review required.

All changes shall be logged, tracked and auditable.

21.10 Problem Management SLA

The bidder shall perform root cause analysis for recurring or major incidents.

Root Cause Analysis Requirements

Severity	RCA Delivery
Critical	5 Business Days
High	10 Business Days
Medium	15 Business Days

Root Cause Analysis reports shall include:

- Issue summary.
- Root cause.
- Impact assessment.
- Corrective actions.
- Preventative measures.

21.11 Monitoring Requirements

The bidder shall continuously monitor:

Infrastructure

- Firewalls.
- SD-WAN.
- Connectivity.
- Azure Integration.

Security Services

- IPS.
- Threat Prevention.
- ZTNA.
- CASB.
- DLP.
- SWG.
- UEBA.

Operational Health

- Capacity.

- Resource utilisation.
- Service availability.
- System performance.

Monitoring shall be proactive rather than event driven.

21.12 Alerting Requirements

The bidder shall generate proactive alerts for:

Security Events

- Malware detections.
- Threat detections.
- Ransomware activity.
- Policy violations.
- Excessive failed logons.
- Privileged access violations.

Operational Events

- Connectivity failures.
- Device failures.
- Capacity threshold breaches.
- Azure integration failures.
- DR connectivity failures.

Alerts shall be generated in near real-time.

21.13 Capacity Management SLA

The bidder shall proactively manage growth and utilisation.

Capacity Thresholds

Resource	Threshold
CPU Utilisation	70%
Memory Utilisation	70%
Throughput Utilisation	70%
Session Utilisation	70%

Storage Utilisation	80%

Exceeding thresholds shall trigger:

- Capacity review.
- Recommendations.
- Expansion planning.

21.14 Security Update SLA

The bidder shall maintain currency of all security controls.

Security Updates

Update Type	Deployment Target
Critical Security Fixes	Within 7 Days
High Severity Security Fixes	Within 14 Days
Medium Severity Security Fixes	Within 30 Days
Routine Updates	As Scheduled

Exceptions require written approval from MIBCO.

21.15 Vulnerability Management SLA

The bidder shall assess and remediate vulnerabilities according to severity.

Vulnerability Severity	Remediation Target
Critical	7 Days
High	14 Days
Medium	30 Days
Low	90 Days

Monthly vulnerability reporting shall be provided.

21.16 Backup and Recovery SLA

The bidder shall maintain all configuration backups required to support service recovery.

Requirements

- Daily configuration backups.
- Pre-change backups.

- Secure backup storage.
- Recovery validation.

The bidder shall document retention periods and recovery procedures.

21.17 Disaster Recovery SLA

The bidder shall support MIBCO's hybrid architecture.

Minimum DR Requirements

Requirement	Target
DR Support Availability	24x7
DR Incident Response	30 Minutes
Security Policy Availability During Failover	Maintained
Logging Continuity	Maintained

The bidder shall provide recommended RTO and RPO values.

21.18 Escalation Requirements

The bidder shall provide a formal escalation model.

Escalation Levels

Level	Description
Level 1	Service Desk
Level 2	Technical Specialist
Level 3	Senior Engineer
Level 4	Vendor/OEM
Level 5	Executive Escalation

Escalation contacts shall be maintained throughout the contract period.

21.19 Reporting Requirements

Monthly Service Reports

The bidder shall provide:

- Availability statistics.
- Incident statistics.

- Security statistics.
- Capacity statistics.
- Change statistics.
- SLA compliance.

Quarterly Service Reports

The bidder shall provide:

- Service review summary.
- Security posture review.
- Risk review.
- Capacity review.
- Improvement recommendations.

21.20 SLA Credits

The bidder shall propose service credits applicable when agreed service levels are not achieved.

The proposal shall include:

- Availability credits.
- Incident response credits.
- Restoration credits.
- Reporting failures.

MIBCO reserves the right to negotiate SLA penalties and credits during contract negotiations.

21.21 Service Review Meetings

The bidder shall attend:

Monthly Operational Meetings

Review:

- Incidents.
- Changes.
- Risks.
- Capacity.
- Open actions.

Quarterly Service Review Meetings

Review:

- Security posture.
- SLA performance.
- Service improvements.
- Roadmap updates.

21.22 Customer Satisfaction

The bidder shall measure customer satisfaction at least annually.

The proposal shall describe:

- Measurement methodology.
- Reporting methodology.
- Improvement processes.

21.23 Service Level Measurement

The bidder shall provide details regarding:

- SLA calculation methodology.
- Reporting methodology.
- Monitoring methodology.
- Data collection processes.

All SLA calculations shall be transparent and auditable.

21.24 Bidder Response Requirements

The bidder shall provide:

- Proposed SLA.
- Service Credit Model.
- Escalation Matrix.
- Sample Monthly Service Report.
- Sample Quarterly Service Review Report.
- Monitoring Methodology.
- Availability Calculation Methodology.

The bidder shall complete the Service Level Response Schedule contained in the relevant Annexure.

Failure to meet the mandatory minimum service levels contained in this section may result in the proposal being deemed non-compliant and excluded from further evaluation.

21.25 Key Performance Indicators (KPIs)

The successful bidder shall report monthly against the following minimum KPIs:

KPI	Target
Service Availability	≥ 99.9%
Critical Incident Response	≤ 30 Minutes
High Incident Response	≤ 1 Hour
Change Success Rate	≥ 95%
Security Update Compliance	≥ 95%
Monthly Reporting Delivery	100%
Customer Satisfaction	≥ 90%

Failure to achieve agreed KPI targets may form part of MIBCO's performance management and contract review processes.

22. SUBMISSION OF PROPOSAL

22.1 Proposal Submission Requirements

Interested bidders are invited to submit a comprehensive proposal for the provision of a Fully Managed Secure Network and Cybersecurity Service (SNaaS) in accordance with the requirements contained within this RFP.

The bidder shall ensure that the proposal is complete, accurate and submitted on or before the closing date specified in this RFP.

Late submissions may not be considered.

The responsibility for ensuring successful delivery of the proposal to MIBCO rests solely with the bidder.

22.2 Submission Format

The proposal shall be submitted electronically in PDF format.

Where applicable, editable Microsoft Office versions of supporting schedules and annexures shall also be submitted.

The submission shall consist of the following separate sections:

Section 1 – Executive and Administrative Submission

This section shall contain:

- Cover Letter.
- Executive Summary.
- Company Profile.
- Company Registration Documents.
- Mandatory Documentation.
- B-BBEE Documentation.
- Tax Compliance Documentation.

Section 2 – Technical Proposal

This section shall contain:

- Solution Overview.
- Proposed Architecture.
- Hybrid Data Centre and Azure DR Architecture.
- Security Architecture.
- SD-WAN Architecture.
- Zero Trust Architecture.
- Service Management Model.
- Implementation Methodology.
- Risk Management Approach.
- Training and Knowledge Transfer Approach.
- Compliance Response.
- Completed Technical Response Schedules.

Section 3 – Commercial Proposal

This section shall contain:

- Completed Costing Annexures.
- Licensing Costs.
- Professional Service Costs.
- Managed Service Costs.
- Expansion Costs.
- Optional Feature Costs.

- Assumptions.
- Commercial Terms.

Section 4 – Supporting Documentation

This section shall contain:

- OEM Certifications.
- Product Datasheets.
- Technical Specifications.
- Independent Performance Validation.
- Reference Letters.
- Case Studies.
- Sample Reports.
- Sample SLA.

22.3 Proposal Structure

To facilitate fair and efficient evaluation, bidders shall structure their proposals according to the sequence of sections contained within this RFP.

The proposal shall include responses to every requirement contained within this document.

Failure to respond to a requirement may result in the associated requirement being scored as non-compliant.

22.4 Mandatory Response Matrices

The bidder shall complete all annexures and response schedules included with this RFP.

At a minimum, the following annexures shall be completed:

Annexure	Description
Annexure A	Compliance Matrix
Annexure B	Technical Response Schedule
Annexure C	Modular Costing Schedule
Annexure D	Professional Services Costing
Annexure E	Managed Services Costing
Annexure F	Future Expansion Pricing

Annexure G	Risk Register and Risk Management Response
Annexure H	Project and Implementation Plan
Annexure I	Customer References
Annexure J	Hybrid Architecture Response

Failure to complete the mandatory annexures may result in disqualification.

22.5 Proposal Validity

The proposal shall remain valid and binding for a minimum period of four (4) months from the proposal closing date.

The bidder shall clearly indicate any deviations from this requirement.

22.6 Proposal Language

All proposal documentation shall be submitted in English.

Technical documentation supplied by OEMs may be submitted in their original language provided an English version is also available upon request.

22.7 Bidder Assumptions

The bidder shall clearly identify:

- Commercial assumptions.
- Technical assumptions.
- Architectural assumptions.
- Licensing assumptions.
- Service assumptions.
- Support assumptions.

Any assumptions not explicitly documented shall be deemed to be included within the proposal price.

22.8 Bidder Deviations

The bidder shall clearly identify any deviations from the requirements contained within this RFP.

The bidder shall complete a deviation register detailing:

Requirement Reference	Deviation Description	Reason for Deviation	Proposed Alternative

Failure to disclose deviations may result in the proposal being deemed non-compliant.

22.9 Proposal Clarifications

MIBCO reserves the right to:

- Request clarification of any proposal.
- Request additional information.
- Request demonstrations.
- Request technical workshops.
- Request architecture reviews.
- Request proof-of-concept activities.

Such requests shall not be construed as acceptance of a proposal.

22.10 Bidder Presentations

MIBCO reserves the right to invite shortlisted bidders to present their proposals.

The presentation may include:

- Corporate overview.
- Proposed solution architecture.
- Security capabilities.
- Hybrid architecture approach.
- Azure integration approach.
- Risk management approach.
- Implementation methodology.
- Service management model.
- Commercial model.

The bidder shall ensure that appropriately qualified technical and commercial personnel attend.

23. MANDATORY DOCUMENTATION

23.1 Purpose

The purpose of this section is to ensure that all bidders submit sufficient information to enable MIBCO to conduct a fair, transparent, objective and auditable evaluation process.

All bidders shall provide the mandatory documentation listed in this section.

The documentation will be used to assess:

- Legal compliance.

- Financial sustainability.
- Technical capability.
- Service delivery capability.
- OEM accreditation.
- Cybersecurity competence.
- Project delivery capability.
- Commercial compliance.

23.2 Important Notice

Mandatory Submission Requirement

Failure to submit any mandatory document listed in this section shall result in the proposal being regarded as non-responsive and may result in immediate disqualification.

MIBCO reserves the right to reject proposals that:

- Are incomplete.
- Do not contain all mandatory documents.
- Contain expired documentation.
- Contain inaccurate information.
- Contain misleading information.
- Do not comply with the submission requirements of this RFP.

MIBCO is under no obligation to request missing information after the closing date.

The responsibility for submitting a complete proposal rest entirely with the bidder.

23.3 Company and Legal Documentation

The bidder shall submit the following legal and corporate documentation.

Document	Mandatory
Company Registration Certificate	Yes
Proof of Business Address	Yes
Company Profile	Yes
Organisational Structure / Organogram	Yes

23.4 Tax and Regulatory Documentation

The bidder shall provide evidence of tax compliance.

Document	Mandatory
SARS Tax Compliance Status PIN	Yes
Tax Clearance Certificate (if available)	Yes
Letter of Good Standing	Yes

The bidder shall remain tax compliant throughout the procurement process and contract period.

23.5 B-BBEE Documentation

Only enterprises with a B-BBEE level from Level 1 to Level 4 will be considered.

The bidder shall provide:

Document	Mandatory
Valid B-BBEE Certificate	Yes
SANAS Accredited Verification Certificate (where applicable)	Yes
EME Affidavit (if applicable)	Yes
QSE Affidavit (if applicable)	Yes

The documentation submitted must be valid on the proposal closing date.

23.6 Financial Documentation

The bidder shall demonstrate financial sustainability and ability to support a 36-month managed services contract.

Document	Mandatory
Audited Financial Statements (Previous 2 Financial Years)	Yes
Latest Management Accounts (if available)	Preferred
Letter from Auditor Confirming Going Concern Status (if available)	Preferred

MIBCO reserves the right to conduct financial due diligence.

23.7 Insurance Documentation

The bidder shall provide evidence of insurance cover suitable for the scope of services contemplated.

Insurance Type	Mandatory
Professional Indemnity Insurance	Yes
Public Liability Insurance	Yes
Cyber Liability Insurance	Yes

The bidder shall provide:

- Policy Schedule.
- Coverage Limits.
- Expiry Dates.

The bidder shall maintain these policies for the duration of the contract.

23.8 OEM Accreditation and Certification

The bidder shall prove that it is authorised to provide, implement and support the proposed solution.

Mandatory OEM Documentation

Document	Mandatory
OEM Partner Certificate	Yes
OEM Reseller Authorisation	Yes
OEM Support Authorisation	Yes
OEM Service Delivery Accreditation	Yes

Technical Resource Certifications

The bidder shall provide certifications for resources assigned to the project.

Certification Type	Mandatory
Security Specialist Certification	Yes
Firewall Specialist Certification	Yes
SD-WAN Specialist Certification	Yes
Solution Architect Certification	Yes

Certifications shall be current and valid.

23.9 Technical Proposal Documentation

The bidder shall submit a comprehensive technical proposal.

Required Documents

Document	Mandatory
Executive Summary	Yes
Solution Overview	Yes
Proposed Architecture	Yes
Security Architecture	Yes
Hybrid Data Centre and Azure Architecture	Yes
Logical Architecture Diagram	Yes
Physical Architecture Diagram	Yes
Network Segmentation Design	Yes
Zero Trust Architecture	Yes
SOC Integration Design	Yes

23.10 Architecture Documentation

The bidder shall provide architecture diagrams and supporting documentation.

Required Architecture Documents

Deliverable	Mandatory
Current State Understanding Diagram	Yes
Future State Architecture Diagram	Yes
Hybrid Environment Diagram	Yes
Randburg Data Centre Security Diagram	Yes
Azure DR Architecture Diagram	Yes
Security Architecture Diagram	Yes
SD-WAN Architecture Diagram	Yes

ZTNA Architecture Diagram	Yes

All diagrams shall be clearly labelled and professionally presented.

23.11 Implementation Documentation

The bidder shall provide detailed implementation plans.

Document	Mandatory
Project Plan	Yes
Resource Plan	Yes
Governance Model	Yes
Risk Management Plan	Yes
Migration Plan	Yes
Rollback Plan	Yes
Cutover Plan	Yes
Hypercare Plan	Yes

23.12 Service Management Documentation

The bidder shall submit documentation describing the managed service offering.

Document	Mandatory
Service Management Framework	Yes
Service Delivery Model	Yes
Service Desk Model	Yes
Escalation Matrix	Yes
Monitoring Framework	Yes
Monthly Reporting Template	Yes
Quarterly Service Review Template	Yes

23.13 Security Documentation

The bidder shall submit documentation describing the cybersecurity capabilities of the proposed solution.

Document	Mandatory
Security Capability Statement	Yes
Threat Intelligence Description	Yes
Security Operations Integration Description	Yes
Security Analytics Description	Yes
Compliance Mapping	Yes
Encryption Standards Statement	Yes

23.14 Compliance Documentation

The bidder shall submit evidence supporting compliance claims.

Document	Mandatory
Compliance Matrix	Yes
POPIA Compliance Statement	Yes
PCI-DSS Support Statement	Yes
NIST Alignment Statement	Yes
ISO Alignment Statement	Yes
FIPS Certification Evidence	Yes
Common Criteria Evidence (where applicable)	Preferred

23.15 Risk Management Documentation

The bidder shall provide:

Document	Mandatory
Risk Management Methodology	Yes

Sample Risk Register	Yes
Security Risk Management Approach	Yes
Business Continuity Approach	Yes
Disaster Recovery Approach	Yes
Vulnerability Management Approach	Yes

23.16 Training and Knowledge Transfer Documentation

The bidder shall provide:

Document	Mandatory
Training Plan	Yes
Knowledge Transfer Plan	Yes
Training Schedule	Yes
Sample Training Material	Yes
Skills Transfer Methodology	Yes

23.17 Performance Validation Documentation

The bidder shall provide evidence to support all performance claims.

Document	Mandatory
OEM Product Datasheets	Yes
Published Performance Figures	Yes
NGFW Throughput Evidence	Yes
Threat Prevention Throughput Evidence	Yes
SSL Inspection Throughput Evidence	Yes
SD-WAN Throughput Evidence	Yes
Independent Benchmark Results (where available)	Preferred

Customer Reference Validation	Yes

Failure to provide supporting evidence may result in performance claims being disregarded during evaluation.

23.18 Customer Reference Documentation

The bidder shall provide at least three (3) reference engagements.

Required Information

Requirement	Mandatory
Customer Name	Yes
Industry	Yes
Contact Person	Yes
Email Address	Yes
Telephone Number	Yes
Scope of Solution	Yes
Number of Sites	Yes
Number of Users	Yes

Preference may be given to:

- Hybrid Data Centre and Azure environments.
- Managed security services.
- Financial services environments.
- Regulated environments.

23.19 Commercial Documentation

The bidder shall complete all commercial schedules and annexures.

Mandatory Commercial Documents

Document	Mandatory
Annexure C – Modular Costing Schedule	Yes
Annexure D – Professional Services Costing	Yes
Annexure E – Managed Services Costing	Yes

Annexure F – Future Expansion Pricing	Yes
Pricing Assumptions	Yes
Commercial Terms and Conditions	Yes

All pricing shall be submitted exclusive of VAT unless otherwise specified.

23.20 Mandatory Annexures

The bidder shall complete and submit all response schedules contained within this RFP.

Annexure	Mandatory
Annexure A – Compliance Matrix	Yes
Annexure B – Technical Response Schedule	Yes
Annexure C – Modular Costing Schedule	Yes
Annexure D – Professional Services Schedule	Yes
Annexure E – Managed Services Schedule	Yes
Annexure F – Future Expansion Pricing Schedule	Yes
Annexure G – Risk Register	Yes
Annexure H – Project Plan	Yes
Annexure I – Customer References	Yes
Annexure J – Hybrid Architecture Response	Yes
Annexure K – Proof of Concept Response	Yes

23.21 Proposal Completeness Declaration

The bidder shall submit a signed declaration confirming:

1. The proposal is complete.
2. All mandatory documentation has been provided.
3. All information supplied is accurate.
4. The bidder agrees to the terms of the RFP.
5. The bidder acknowledges the modular procurement approach.

6. The bidder acknowledges that MIBCO may procure all or selected modules.

23.22 Mandatory Compliance Checklist

Before submission, bidders shall verify that all mandatory documentation has been included.

Final Mandatory Submission Checklist

Section	Included
Company Documentation	☐
Tax Documentation	☐
B-BBEE Documentation	☐
Insurance Documentation	☐
OEM Certifications	☐
Technical Proposal	☐
Architecture Diagrams	☐
Implementation Plan	☐
Risk Management Documentation	☐
Service Management Documentation	☐
Compliance Documentation	☐
Training Documentation	☐
Costing Annexures	☐
Reference Documentation	☐
Completed Annexures A–K	☐

IMPORTANT

Failure to submit any mandatory documentation listed in this section may result in immediate disqualification without further evaluation.

MIBCO reserves the right to reject any proposal that is incomplete, materially deficient, misleading, inaccurate or non-compliant with the mandatory requirements of this RFP.

24. EVALUATION PROCESS

24.1 Evaluation Principles

MIBCO shall evaluate all proposals in a fair, transparent, objective and auditable manner.

The evaluation process is intended to identify the proposal that offers the best overall value to MIBCO, taking into consideration:

- Cybersecurity capability.
- Technical compliance.
- Service delivery capability.
- Vendor experience and capacity.
- Commercial competitiveness.
- B-BBEE status.
- Risk profile.
- Future scalability.
- Alignment to MIBCO's strategic objectives.

Submission of a proposal does not guarantee selection, shortlisting or contract award.

MIBCO reserves the right to:

- Accept or reject any proposal.
- Request clarification.
- Request additional information.
- Conduct due diligence.
- Conduct site visits.
- Conduct reference checks.
- Conduct architecture reviews.
- Conduct Proof of Concept (PoC) evaluations.
- Award all or part of the scope of work.
- Cancel the RFP without obligation.

24.2 Evaluation Stages

The evaluation process shall consist of the following stages:

Stage	Description

Stage 1	Administrative Compliance Evaluation
Stage 2	Mandatory Requirements Evaluation
Stage 3	Functional Evaluation
Stage 4	Technical Clarifications (if required)
Stage 5	Reference Checks and Due Diligence
Stage 6	Architecture Review and Demonstrations
Stage 7	Commercial Evaluation
Stage 8	B-BBEE Evaluation
Stage 9	Final Recommendation and Contract Award

MIBCO reserves the right to omit or expand any evaluation stage as deemed necessary.

24.3 Stage 1 – Administrative Compliance Evaluation

The purpose of this stage is to verify that the proposal has been submitted in the correct format and includes all mandatory documentation.

The following will be reviewed:

- Submission completeness.
- Signed proposal documents.
- Mandatory documentation.
- Completion of annexures.
- Compliance schedules.
- Commercial schedules.

Failure to pass this stage may result in disqualification.

24.4 Stage 2 – Mandatory Requirements Evaluation

The purpose of this stage is to verify compliance with non-negotiable requirements.

Mandatory requirements include, but are not limited to:

Contracting Model

- Fully Managed Service.

- Security Network as a Service (SNaaS).

Technical Requirements

- NGFW.
- Secure SD-WAN.
- ZTNA.
- Azure Integration.
- Hybrid Architecture Support.

Security Requirements

- CASB.
- SWG.
- DLP.
- RBI.
- UEBA.
- DNS Security.
- Threat Prevention.

Operational Requirements

- 24x7 Support.
- Managed Services.
- Service Reporting.

Bidders that do not meet mandatory requirements may be excluded from further evaluation.

24.5 Stage 3 – Functional Evaluation

The functionality evaluation will assess how effectively the proposed solution satisfies the technical, operational, security and service requirements contained in this RFP.

Only bidders that pass Stages 1 and 2 shall proceed to functionality evaluation.

Minimum Functionality Threshold

A bidder must achieve a minimum functionality score of:

80 out of 100 points

Bidders scoring less than 80 points shall be disqualified and shall not proceed to commercial evaluation.

24.6 Functional Evaluation Criteria

The functionality score shall be allocated as follows:

Evaluation Criterion	Weight
Cybersecurity Capability	35
Technical Compliance	25
Managed Service Capability	15
Implementation Methodology	10
Vendor Experience and References	10
Support Model	5
Total	100

24.7 Evaluation Criterion Descriptions

Cybersecurity Capability (35 Points)

This category evaluates:

- NGFW capabilities.
- IPS and IDS capabilities.
- Threat prevention.
- ZTNA maturity.
- CASB capabilities.
- SWG capabilities.
- DLP capabilities.
- RBI capabilities.
- UEBA capabilities.
- Identity-based security.
- Security analytics.
- Threat intelligence capabilities.
- Hybrid security architecture.
- Compliance support.

Scoring Guidance

Rating	Score Allocation
Poor	0 – 10
Acceptable	11 – 20
Good	21 – 27
Very Good	28 – 32
Excellent	33 – 35

Technical Compliance (25 Points)

This category evaluates:

- Compliance with RFP requirements.
- Hybrid Data Centre support.
- Azure integration.
- Scalability.
- Performance.
- Architecture quality.
- Extensibility.
- Manageability.

Scoring Guidance

Rating	Score Allocation
Poor	0 – 7
Acceptable	8 – 14
Good	15 – 19
Very Good	20 – 23
Excellent	24 – 25

Managed Service Capability (15 Points)

This category evaluates:

- Service delivery model.
- Monitoring capabilities.
- Vendor management.
- Service governance.
- Reporting framework.
- Lifecycle management.

Scoring Guidance

Rating	Score Allocation
Poor	0 – 4
Acceptable	5 – 8
Good	9 – 11
Very Good	12 – 14
Excellent	15

Implementation Methodology (10 Points)

This category evaluates:

- Project governance.
- Project management approach.
- Migration methodology.
- Risk management.
- Testing methodology.
- Cutover planning.
- Rollback planning.

Scoring Guidance

Rating	Score Allocation

Poor	0 – 2
Acceptable	3 – 5
Good	6 – 7
Very Good	8 – 9
Excellent	10

Vendor Experience and References (10 Points)

This category evaluates:

- Relevant project experience.
- Hybrid architecture experience.
- Azure experience.
- Managed security services experience.
- Customer references.
- Organisational capability.

Scoring Guidance

Rating	Score Allocation
Poor	0 – 2
Acceptable	3 – 5
Good	6 – 7
Very Good	8 – 9
Excellent	10

Support Model (5 Points)

This category evaluates:

- Local presence.
- Escalation capability.
- Availability of resources.

- OEM relationships.
- Support responsiveness.

Scoring Guidance

Rating	Score Allocation
Poor	0 – 1
Acceptable	2
Good	3
Very Good	4
Excellent	5

24.8 Stage 4 – Clarification Phase

MIBCO may request clarification regarding:

- Technical responses.
- Commercial responses.
- Architecture assumptions.
- Capacity assumptions.
- Licensing assumptions.
- Compliance statements.

Clarifications shall not be used to materially change a proposal after submission.

24.9 Stage 5 – Reference Checks and Due Diligence

MIBCO reserves the right to contact customer references supplied by the bidder.

Reference checks may consider:

- Service quality.
- Technical capability.
- Support quality.
- Project delivery success.
- Contract management.
- Customer satisfaction.

MIBCO reserves the right to conduct independent reference checks.

24.10 Stage 6 – Architecture Review and Demonstration

Shortlisted bidders may be invited to present their proposed solution.

Presentations may include:

- Architecture review.
- Security controls.
- Zero Trust architecture.
- Azure integration.
- Hybrid architecture.
- Service management model.
- Reporting capabilities.

The presentation may contribute to the overall technical evaluation.

24.11 Stage 7 – Commercial Evaluation

Commercial evaluation will only be conducted for bidders that meet the minimum functionality threshold.

Commercial evaluation will consider:

- Once-off costs.
- Monthly managed service costs.
- Licensing costs.
- Implementation costs.
- Future expansion costs.
- Total Cost of Ownership (TCO).

The modular pricing model will be evaluated to determine:

- Affordability.
- Scalability.
- Flexibility.
- Future budget planning benefits.

24.12 Stage 8 – B-BBEE Evaluation

B-BBEE points shall be allocated according to applicable legislation and MIBCO procurement policies.

Only valid B-BBEE submissions shall be considered.

The bidder shall provide all required supporting documentation.

24.13 Stage 9 – Final Evaluation and Recommendation

The evaluation committee shall consider:

- Functionality results.
- Risk profile.
- Commercial evaluation.
- B-BBEE evaluation.
- Reference checks.
- Proof of Concept results.
- Due diligence outcomes.

The committee shall recommend the preferred bidder to the appropriate approval authority.

24.14 Evaluation Committee Rights

The evaluation committee reserves the right to:

- Verify any information supplied.
- Request supporting evidence.
- Request product demonstrations.
- Request architecture workshops.
- Conduct site visits.
- Engage OEMs.
- Conduct financial due diligence.
- Verify certifications.

Any false, misleading or materially inaccurate information may result in disqualification.

24.15 Modular Award Approach

Because MIBCO has adopted a modular procurement approach, the evaluation committee may recommend:

- Award of the full solution.
- Award of selected modules only.
- Phased implementation.
- Deferred implementation of selected modules.
- Future procurement of optional modules.

The bidder acknowledges that MIBCO is not obligated to procure all modules simultaneously and may expand the solution during future budget cycles.

24.16 Evaluation Outcomes

At the conclusion of the evaluation process, MIBCO may:

- Award the contract.
- Award a portion of the contract.
- Negotiate aspects of the proposal.
- Enter into clarification discussions.
- Retender the requirement.
- Cancel the RFP.

The decision of MIBCO shall be final.

25. FUNCTIONAL EVALUATION CRITERIA

25.1 Purpose

The purpose of the Functional Evaluation is to assess the bidder's ability to deliver a secure, reliable, scalable and fully managed Secure Network and Cybersecurity Service that meets MIBCO's strategic, operational, security and compliance requirements.

The functionality evaluation will determine whether a bidder possesses the technical capability, service delivery capability, experience, maturity and operational capacity required to successfully deliver the proposed solution.

Only bidders that achieve the minimum functionality threshold will proceed to commercial and B-BBEE evaluation.

25.2 Minimum Functionality Threshold

The minimum functionality score required to proceed to commercial evaluation shall be:

80 Points out of 100

Any bidder scoring below 80 points will be disqualified from further evaluation and will not proceed to:

- Price Evaluation
- B-BBEE Evaluation
- Final Adjudication

25.3 Functional Evaluation Weighting

The following evaluation criteria and weightings shall apply:

Evaluation Category	Weight
Cybersecurity Capability	35
Technical Compliance	25
Managed Service Capability	15
Implementation Methodology	10
Vendor Experience and References	10
Support Model	5
Total	**100**

25.4 Cybersecurity Capability (35 Points)

Objective

Evaluate the maturity, completeness and effectiveness of the cybersecurity controls proposed by the bidder.

This category carries the highest weighting due to the importance of cybersecurity to MIBCO's business operations, regulatory obligations and risk management objectives.

Areas of Evaluation

The following areas will be evaluated:

Core Security Capabilities

- Next Generation Firewall (NGFW)
- IDS / IPS
- Advanced Threat Prevention
- Threat Intelligence
- Malware Protection
- DNS Security
- URL Filtering
- TLS 1.3 Inspection
- SSL/TLS Decryption

Zero Trust Capabilities

- ZTNA
- Identity-Aware Security
- Device Trust Validation
- Continuous Verification
- Conditional Access Integration
- Least Privilege Controls

Security Service Edge Capabilities

- CASB
- SWG
- DLP
- RBI
- UEBA

Threat Detection and Analytics

- Threat Hunting
- Security Analytics
- MITRE ATT&CK Mapping
- AI-Assisted Threat Detection
- SOC Integration

Security Governance

- Audit Trails
- Compliance Controls
- Security Reporting
- Policy Enforcement

Scoring Guidance

Rating	Description	Score
Poor	Significant deficiencies	0 – 10
Acceptable	Meets minimum requirements	11 – 20

Good	Exceeds several requirements	21 – 27
Very Good	Exceeds most requirements	28 – 32
Excellent	Comprehensive and industry-leading capability	33 – 35

25.5 Technical Compliance (25 Points)

Objective

Assess the extent to which the proposed solution complies with the technical requirements defined within the RFP.

Areas of Evaluation

Hybrid Architecture Support

- Randburg Data Centre Security
- Azure DR Security
- Unified Management
- Policy Synchronisation

Performance

- Throughput
- Scalability
- Capacity
- Performance Headroom

Integration

- Microsoft Entra ID
- Intune
- Defender for Endpoint
- Azure Virtual WAN
- Azure VPN Gateway

Architecture

- Design Quality
- Simplicity
- Scalability

- Resilience

Future Readiness

- Expandability
- Modular Deployment
- Future Growth Support

Scoring Guidance

Rating	Description	Score
Poor	Major technical gaps	0 – 7
Acceptable	Meets minimum requirements	8 – 14
Good	Exceeds requirements	15 – 19
Very Good	Strong alignment	20 – 23
Excellent	Outstanding technical solution	24 – 25

25.6 Managed Service Capability (15 Points)

Objective

Evaluate the maturity of the bidder's managed service offering.

Areas of Evaluation

Service Management

- ITIL Alignment
- Service Governance
- Service Reporting
- Escalation Management

Operational Services

- Monitoring
- Incident Management
- Change Management
- Problem Management

Security Operations Support

- Security Monitoring
- Threat Intelligence Management
- Security Tuning
- Security Reporting

Lifecycle Management

- Patch Management
- Firmware Management
- Vendor Management
- Technology Refresh

Scoring Guidance

Rating	Description	Score
Poor	Immature service model	0 – 4
Acceptable	Meets minimum requirements	5 – 8
Good	Mature service capability	9 – 11
Very Good	Strong managed service offering	12 – 14
Excellent	Industry-leading managed service capability	15

25.7 Implementation Methodology (10 Points)

Objective

Assess the bidder's ability to successfully implement and transition the solution into operational service.

Areas of Evaluation

Project Governance

- Governance Structure
- Resource Allocation
- Stakeholder Management

Migration Approach

- Meraki Migration Strategy
- Testing Strategy

- Rollback Strategy
- Hypercare Approach

Risk Management

- Risk Identification
- Risk Mitigation
- Risk Monitoring

Delivery Capability

- Realism of Project Plan
- Resource Availability
- Quality Assurance

Scoring Guidance

Rating	Description	Score
Poor	Significant concerns	0 – 2
Acceptable	Meets minimum standards	3 – 5
Good	Strong methodology	6 – 7
Very Good	Highly structured approach	8 – 9
Excellent	Low-risk implementation approach	10

25.8 Vendor Experience and References (10 Points)

Objective

Assess the bidder's proven ability to deliver similar solutions.

Areas of Evaluation

Organisational Experience

- Years in Business
- Security Services Experience
- Managed Service Experience

Relevant Project Experience

- NGFW Implementations

- SD-WAN Implementations
- ZTNA Deployments
- Hybrid Cloud Security Deployments

Customer References

Preference will be given to references involving:

- Financial Services
- Regulatory Environments
- Hybrid Data Centre and Azure Environments
- Managed Security Services

Resource Capability

- Security Architects
- Network Specialists
- Certified Engineers

Scoring Guidance

Rating	Description	Score
Poor	Limited experience	0 – 2
Acceptable	Adequate experience	3 – 5
Good	Relevant experience	6 – 7
Very Good	Strong track record	8 – 9
Excellent	Extensive proven capability	10

25.9 Support Model (5 Points)

Objective

Assess the bidder's support capabilities and operational responsiveness.

Areas of Evaluation

Support Availability

- 24x7 Support
- Escalation Capability

- OEM Support Coverage

Local Capability

- South African Presence
- Local Technical Resources
- Escalation Resources

Service Levels

- Response Times
- Resolution Targets
- Support Processes

Customer Engagement

- Service Reviews
- Account Management
- Escalation Procedures

Scoring Guidance

Rating	Description	Score
Poor	Inadequate support capability	0 – 1
Acceptable	Meets minimum requirements	2
Good	Strong support capability	3
Very Good	Highly responsive support model	4
Excellent	Exceptional support model	5

25.10 Evaluation Methodology

Each evaluation criterion shall be scored independently by the evaluation committee.

The final functionality score shall be the sum of all criterion scores.

The evaluation committee may consider:

- Proposal responses.
- Annexure responses.
- Technical demonstrations.

- Architecture workshops.
- Clarification responses.
- Customer references.
- Proof of Concept outcomes.

25.11 Proof of Concept Adjustment

Where a Proof of Concept is conducted, MIBCO reserves the right to adjust technical evaluation scores based on demonstrated capability.

Particular consideration may be given to:

- Performance validation.
- Azure integration.
- ZTNA functionality.
- Security effectiveness.
- SOC integration.
- Administration and usability.

A bidder that cannot demonstrate critical functionality during the Proof of Concept may be disqualified irrespective of its initial functionality score.

25.12 Functional Evaluation Deliverables

The evaluation committee shall produce:

- Functional Evaluation Scorecard.
- Evaluation Findings Report.
- Technical Risk Assessment.
- Recommendation Report.

These documents shall form part of MIBCO's procurement record and governance process.

25.13 Evaluation Committee Rights

The evaluation committee reserves the right to:

- Verify technical claims.
- Verify certifications.
- Verify reference projects.
- Request additional evidence.
- Request demonstrations.

- Conduct architecture reviews.
- Conduct Proof of Concept validation.

Failure to substantiate claims made in the proposal may result in a reduced score or disqualification.

26. FUNCTIONAL EVALUATION TABLE

26.1 Purpose

This section defines the methodology that will be used by the Evaluation Committee to assess the functionality of proposals received in response to this RFP.

The functionality evaluation is intended to assess the bidder's ability to deliver a secure, resilient, scalable and fully managed Secure Network and Cybersecurity Service aligned to MIBCO's requirements.

Only bidders that achieve the minimum functionality threshold shall proceed to the Commercial and B-BBEE evaluation stages.

26.2 Minimum Qualification Threshold

Bidders must achieve a minimum functionality score of:

80 Points out of 100

Any bidder scoring less than 90 points shall be disqualified and will not proceed to:

- Commercial Evaluation.
- B-BBEE Evaluation.
- Final Adjudication.

26.3 Functional Evaluation Summary Table

Evaluation Criteria	Weight
Cybersecurity Capability	35
Technical Compliance	25
Managed Service Capability	15
Implementation Methodology	10
Vendor Experience and References	10
Support Model	5
Total	**100**

26.4 Detailed Functional Evaluation Matrix

1. Cybersecurity Capability (35 Points)

Evaluation Areas

Evaluation Area	Maximum Points
NGFW Security Capabilities	5
Threat Prevention, IPS and IDS	5
Zero Trust Maturity and ZTNA Capabilities	5
CASB, SWG, DLP and RBI Capabilities	5
UEBA and Security Analytics	4
Threat Intelligence and MITRE ATT&CK Integration	3
Azure Security Controls	3
Identity-Centric Security and Device Posture Enforcement	3
Security Reporting and Compliance Capabilities	2
Total	**35**

Scoring Guide

Rating	Description
0%	No response or non-compliant
25%	Limited functionality
50%	Meets minimum requirements
75%	Exceeds requirements
100%	Best practice / industry-leading capability

2. Technical Compliance (25 Points)

Evaluation Areas

Evaluation Area	Maximum Points

Compliance with Technical Requirements	5
Hybrid Data Centre and Azure Architecture	5
Microsoft Integration Capabilities	4
Scalability and Future Growth	3
Performance Benchmarks and Headroom	4
Architecture Quality and Design	4
Total	**25**

Evaluation Considerations

The Evaluation Committee will consider:

- Architectural simplicity.
- Operational efficiency.
- Security effectiveness.
- Resilience.
- Future scalability.
- Integration capability.

3. Managed Service Capability (15 Points)

Evaluation Areas

Evaluation Area	Maximum Points
Service Delivery Model	3
Service Governance Framework	2
Monitoring and Operational Management	3
Security Operations Support	2
Reporting and Service Reviews	2
Technology Lifecycle Management	3
Total	**15**

Evaluation Considerations

Preference will be given to bidders demonstrating:

- Mature managed service offerings.
- Proven operational processes.
- Strong governance frameworks.
- Proactive service management.

4. Implementation Methodology (10 Points)

Evaluation Areas

Evaluation Area	Maximum Points
Project Governance	2
Project Methodology	2
Migration Approach	2
Risk Management Approach	2
Testing and Cutover Methodology	2
Total	**10**

Evaluation Considerations

Preference will be given to bidders demonstrating:

- Low implementation risk.
- Proven methodologies.
- Detailed planning.
- Comprehensive rollback capabilities.

5. Vendor Experience and References (10 Points)

Evaluation Areas

Evaluation Area	Maximum Points
Similar Security Implementations	2
Hybrid Data Centre and Azure Projects	2

Managed Security Service Experience	2
Relevant Customer References	2
Qualifications and Experience of Resources	2
Total	**10**

Preferred Experience

Preference will be given to experience within:

- Financial Services.
- Pension and Fund Administration.
- Regulated Industries.
- Hybrid Azure Environments.
- National Multi-Site Organisations.

6. Support Model (5 Points)

Evaluation Areas

Evaluation Area	Maximum Points
Support Availability	1
Escalation Capability	1
Local Presence and Resources	1
OEM Relationships	1
Service Level Commitments	1
Total	**5**

26.6 Functional Evaluation Score Sheet

The Evaluation Committee shall use the following scoring template.

Evaluation Criteria	Weight	Score Awarded
Cybersecurity Capability	35	
Technical Compliance	25	

Managed Service Capability	15	
Implementation Methodology	10	
Vendor Experience and References	10	
Support Model	5	
Total	**100**	

26.7 Functional Qualification Outcome

Total Score	Outcome
80 – 100	Qualified for Commercial Evaluation
Below 80	Disqualified from Further Evaluation

26.8 Evaluation Committee Guidance

The Evaluation Committee shall score proposals based on:

- Written responses.
- Annexure submissions.
- Technical documentation.
- Architecture diagrams.
- Demonstrations.
- Clarification sessions.
- Reference checks.
- Proof of Concept outcomes (where applicable).

The Evaluation Committee reserves the right to request supporting evidence for any claim made within the proposal.

Unsubstantiated claims may receive a reduced score or may be regarded as non-compliant.

26.9 Adjudication Principles

To ensure fairness and consistency:

- All bidders shall be evaluated against the same criteria.

- Evaluators shall score independently.
- Scores shall be consolidated and moderated.
- Evaluation records shall be retained for audit purposes.
- Any conflict of interest shall be declared and managed in accordance with MIBCO governance requirements.

The Functional Evaluation score shall form the basis on which bidders progress to the Commercial and B-BBEE evaluation stages.

27. PRICE AND B-BBEE EVALUATION

27.1 Purpose

The purpose of this phase of the evaluation process is to evaluate the commercial competitiveness of qualifying proposals and to allocate preference points in accordance with MIBCO procurement principles and applicable legislation.

Only bidders that successfully:

- Comply with all mandatory requirements;
- Achieve the minimum functionality threshold of 90 points; and
- Pass any required clarification, due diligence or PoC activities,

shall proceed to the Price and B-BBEE Evaluation stage.

27.2 Commercial Evaluation Principles

MIBCO is procuring a:

Fully Managed Secure Network and Cybersecurity Service (SNaaS)

using a modular procurement approach.

Accordingly, the evaluation committee will not assess cost based solely on the lowest price submitted.

The following factors will be considered:

- Total Cost of Ownership (TCO).
- Affordability.
- Scalability.
- Commercial transparency.
- Flexibility of phased procurement.
- Future expansion costs.
- Technology refresh costs.

- Managed service costs.
- Licensing costs.
- Implementation costs.
- Long-term sustainability.

The bidder shall clearly identify:

- Once-off costs.
- Recurring monthly costs.
- Recurring annual costs.
- Optional costs.
- Future expansion costs.

27.3 Modular Pricing Principle

MIBCO reserves the right to procure the solution in phases according to budget availability.

The proposed pricing structure shall therefore be modular and support independent procurement of the following phases:

Phase	Description
Phase 1	Foundation Platform
Phase 2	Zero Trust Services
Phase 3	Security Service Edge Services
Phase 4	Advanced Security Services

The bidder shall ensure that pricing submitted permits MIBCO to:

- Procure all phases simultaneously;
- Procure selected phases only;
- Defer selected phases;
- Implement additional phases in future budget cycles.

Failure to provide modular pricing may result in a reduction in commercial evaluation scoring or disqualification.

27.4 Costing Requirements

The bidder shall complete:

- Annexure C – Modular Costing Schedule.

- Annexure D – Professional Services Costing Schedule.
- Annexure E – Managed Services Costing Schedule.
- Annexure F – Future Expansion Pricing Schedule.

The bidder shall ensure that all pricing:

- Is stated in South African Rand (ZAR).
- Is exclusive of VAT.
- Remains valid for a minimum of four (4) months.
- Includes all applicable licensing.
- Includes all subscriptions.
- Includes all management costs.
- Includes all support costs.
- Includes all professional service costs.

Any exclusions shall be clearly identified.

27.5 Cost Evaluation Components

The commercial evaluation shall consider the following components:

Foundation Platform Costs

Including:

- NGFW
- SD-WAN
- Threat Prevention
- DNS Security
- Logging and Reporting

Zero Trust Costs

Including:

- ZTNA
- Device Posture Assessment
- Conditional Access Integration
- Contractor Access Controls

SSE Costs

Including:

- CASB
- SWG
- RBI

Advanced Security Costs

Including:

- DLP
- UEBA
- AI-Assisted Analytics

Professional Services Costs

Including:

- Discovery
- Design
- Implementation
- Migration
- Testing
- Training
- Hypercare

Managed Service Costs

Including:

- Monitoring
- Incident Management
- Change Management
- Reporting
- Vendor Management
- Security Operations Support

Future Expansion Costs

Including:

- Additional Sites

- Additional Users
- Additional Contractors
- Additional Throughput
- Additional Security Services

27.6 Total Cost of Ownership (TCO)

The evaluation committee shall calculate the Total Cost of Ownership across the full contract period.

The TCO may include:

Cost Category	Included
Hardware	Yes
Software	Yes
Licensing	Yes
Subscriptions	Yes
Professional Services	Yes
Managed Services	Yes
Support Services	Yes
Maintenance Services	Yes
Technology Refresh	Yes
Future Expansion Pricing	Evaluation Purpose

The bidder shall provide a three-year TCO summary.

27.7 Commercial Evaluation Matrix

The evaluation committee may consider the following commercial criteria:

Evaluation Area	Consideration
Initial Cost	Once-off expenditure
Monthly Service Cost	Operational expenditure
Three-Year TCO	Overall affordability

Cost Transparency	Clarity of pricing
Modular Pricing	Ability to phase procurement
Future Expansion Costs	Scalability costs
Commercial Risk	Licensing and renewal risk

27.8 Pricing Assumptions

The bidder shall document all pricing assumptions.

The proposal shall clearly identify:

- User licensing assumptions.
- Site licensing assumptions.
- Throughput assumptions.
- Subscription assumptions.
- Currency assumptions.
- Third-party service assumptions.

Undisclosed assumptions may not be considered during contract negotiations.

27.9 Optional Pricing

Optional functionality shall be clearly separated from mandatory functionality.

The bidder shall identify:

Cost Category	Mandatory Separation
Optional Security Services	Yes
Optional Licences	Yes
Optional Integrations	Yes
Optional Reporting Services	Yes
Optional Training Services	Yes

Optional costs shall not be included within mandatory solution pricing.

27.10 Unrealistic Pricing

MIBCO reserves the right to investigate pricing that appears:

- Unreasonably low.
- Unreasonably high.
- Incomplete.
- Misleading.
- Unsustainable.

The bidder may be required to provide additional information supporting submitted pricing.

Failure to satisfactorily justify pricing may result in disqualification.

27.11 B-BBEE Evaluation

B-BBEE shall be evaluated based on the valid documentation submitted by the bidder.

Only valid B-BBEE documentation submitted before the closing date shall be considered.

MIBCO Preference

MIBCO prefers to do business with appropriately transformed suppliers and reserves the right to apply procurement principles that support transformation objectives.

Only bidders with a valid B-BBEE status level from:

- Level 1
- Level 2
- Level 3
- Level 4

will be considered.

27.12 B-BBEE Recognition Levels

B-BBEE Status	Qualification	Recognition Level
Level 1	100 points or more	135%
Level 2	95 points or more but less than 100	125%
Level 3	90 points or more but less than 95	110%
Level 4	80 points or more but less than 90	100%
Level 5	75 points or more but less than 80	80%
Level 6	70 points or more but less than 75	60%

Level 7	55 points or more but less than 70	50%
Level 8	40 points or more but less than 55	10%
Non-Compliant	Less than 40	0%

27.13 Preference Point System

The following preference point model shall apply:

Category	Points
Price	80
B-BBEE	20
Total	100

Only bidders that successfully pass the functionality evaluation shall be considered for Price and B-BBEE scoring.

27.14 Commercial Adjudication Considerations

The Evaluation Committee may consider:

- Total Cost of Ownership.
- Risk-adjusted value.
- Cybersecurity capability.
- Service sustainability.
- Vendor viability.
- Future expansion affordability.
- Modular procurement flexibility.

MIBCO is not obligated to appoint the lowest-priced bidder.

The contract may be awarded to the bidder whose proposal is determined to provide the best overall value and lowest operational and cybersecurity risk to MIBCO.

27.15 Mandatory Commercial Deliverables

The bidder shall submit:

Deliverable	Mandatory
Annexure C – Modular Costing Schedule	Yes
Annexure D – Professional Services Costing	Yes
Annexure E – Managed Services Costing	Yes
Annexure F – Future Expansion Pricing	Yes
Three-Year TCO Summary	Yes

Pricing Assumptions Register	Yes
B-BBEE Certificate	Yes

Failure to provide any mandatory commercial submission may result in the proposal being deemed non-responsive and excluded from further evaluation.

27.16 Recommended Commercial Evaluation Worksheet

The Evaluation Committee may utilise the following worksheet for comparative assessment:

Cost Component	Bidder A	Bidder B	Bidder C
Phase 1 Cost			
Phase 2 Cost			
Phase 3 Cost			
Phase 4 Cost			
Professional Services			
Managed Services (36 Months)			
Future Expansion Benchmark			
Total 36-Month TCO			
B-BBEE Level			
Risk Assessment			
Overall Ranking			

This worksheet shall assist the adjudication committee in comparing proposals consistently and fairly.

28. SUB-CONTRACTING

28.1 Purpose

The purpose of this section is to ensure that MIBCO has full visibility of all entities that will participate in the delivery, implementation, support, management and operation of the proposed Secure Network and Cybersecurity Service.

Given the critical nature of the services being procured, MIBCO requires transparency regarding all subcontracting arrangements, responsibilities, dependencies and associated risks.

The bidder shall disclose all subcontracting arrangements as part of its proposal.

28.2 General Requirements

The bidder shall remain fully responsible and accountable for the delivery of all services described in this RFP, irrespective of whether any portion of the work is subcontracted.

The successful bidder shall:

- Retain overall accountability for service delivery.
- Retain overall accountability for security.
- Retain overall accountability for project delivery.
- Ensure subcontractor compliance with all contractual obligations.
- Ensure subcontractor compliance with security requirements.
- Ensure subcontractor compliance with regulatory requirements.

No subcontracting arrangement shall diminish the bidder's responsibility to MIBCO.

28.3 Disclosure of Subcontractors

The bidder shall disclose all proposed subcontractors and third-party delivery partners that will participate in any aspect of:

- Design.
- Implementation.
- Security Services.
- Managed Services.
- Project Management.
- Support Services.
- Monitoring Services.
- Cloud Services.
- Training.
- Knowledge Transfer.

The bidder shall complete the following schedule.

Subcontractor	Service Provided	Percentage of Contract Value	Location	OEM Authorised Partner

Failure to disclose subcontracting arrangements may result in disqualification or contract termination.

28.4 Percentage of Work Subcontracted

The bidder shall clearly indicate the percentage of the contract value that will be subcontracted.

The bidder shall provide:

- Total contract value.
- Percentage subcontracted.
- Services subcontracted.
- Associated risks.
- Subcontractor responsibilities.

The percentage shall be determined as a proportion of the total contract value over the full contract term.

28.5 B-BBEE Requirements

A bidder shall not be awarded preference points for B-BBEE status if it is indicated in the proposal that such bidder intends subcontracting more than twenty-five percent (25%) of the value of the contract to an enterprise that does not qualify for at least the same B-BBEE recognition level as the bidder, unless such subcontractor qualifies as an Exempted Micro Enterprise (EME) and has the capability and capacity to execute the subcontracted work.

The bidder shall clearly identify:

- Subcontractor B-BBEE Status.
- Percentage of work allocated.
- Nature of services provided.

28.6 Restrictions on Subcontracting

The successful bidder may not subcontract more than twenty-five percent (25%) of the contract value to an organisation that has a lower B-BBEE status level than the bidder unless such subcontractor qualifies as an EME and possesses the required capability and capacity.

The bidder shall provide evidence supporting any exception claimed.

28.7 OEM and Technology Partner Relationships

The bidder shall disclose any dependency on:

- OEM Professional Services.
- OEM Support Services.
- Managed Security Service Providers.
- Cloud Service Providers.
- International Support Desks.

- Third-Party Security Operations Centres.

The bidder shall describe:

- Responsibilities of each party.
- Escalation processes.
- Support arrangements.
- Service level dependencies.

28.8 Security Requirements for Subcontractors

All subcontractors shall comply fully with:

- POPIA.
- MIBCO Security Policies.
- Confidentiality Requirements.
- Security Controls defined in this RFP.
- Incident Reporting Requirements.
- Audit Requirements.

MIBCO reserves the right to request evidence of compliance.

28.9 Confidentiality Requirements

All subcontractors participating in the delivery of services to MIBCO shall be required to:

- Sign confidentiality agreements.
- Protect MIBCO information.
- Protect personal information.
- Comply with data protection requirements.
- Restrict access to authorised personnel only.

Evidence may be requested during evaluation or contract execution.

28.10 Right to Reject Subcontractors

MIBCO reserves the right to reject any proposed subcontractor where:

- The subcontractor presents an unacceptable security risk.
- The subcontractor cannot demonstrate sufficient capability.
- The subcontractor cannot demonstrate regulatory compliance.
- The subcontractor cannot demonstrate adequate financial stability.

- Prior performance concerns exist.

In such circumstances the bidder may be required to propose an alternative subcontractor.

28.11 Subcontractor Performance Management

The successful bidder shall be responsible for monitoring and managing subcontractor performance.

The bidder shall ensure subcontractors comply with:

- Service Levels.
- Security Requirements.
- Reporting Requirements.
- Contractual Obligations.

Subcontractor performance shall be included in monthly service reviews where relevant.

28.12 Subcontractor Replacement

No subcontractor may be replaced during the contract term without prior written approval from MIBCO.

The bidder shall:

- Notify MIBCO of the proposed change.
- Provide justification.
- Provide replacement details.
- Demonstrate equivalent or better capability.

MIBCO reserves the right to approve or reject the proposed change.

28.13 Cloud and Hosted Service Providers

The bidder shall disclose any third-party hosted platforms used in delivering the service.

Examples include:

- Cloud-hosted Management Platforms.
- Managed Security Platforms.
- Security Analytics Platforms.
- Logging Platforms.
- Monitoring Platforms.

The bidder shall identify:

Service	Provider	Hosting Location	Data Stored

28.14 Subcontractor Due Diligence

MIBCO reserves the right to perform due diligence on any disclosed subcontractor.

The bidder shall provide, upon request:

- Company registration information.
- Compliance certifications.
- Security certifications.
- Insurance confirmation.
- OEM certifications.
- Financial information.

28.15 Mandatory Bidder Declaration

The bidder shall provide a signed declaration confirming that:

1. All subcontractors have been disclosed.
2. All subcontractors are appropriately qualified.
3. All subcontractors comply with applicable legislation.
4. All subcontractors comply with MIBCO security requirements.
5. The bidder accepts full accountability for subcontracted services.
6. MIBCO will be notified of any future subcontractor changes.

28.16 Subcontracting Response Schedule

The bidder shall complete the following schedule as part of its proposal.

Question	Response
Will subcontractors be used?	
Total percentage of contract value to be subcontracted	
Names of subcontractors	
Services allocated to subcontractors	
B-BBEE status of subcontractors	
OEM authorisation status	
Local or international delivery resources	

Security certifications held by subcontractors	

Failure to disclose subcontracting arrangements, or submission of inaccurate subcontracting information, may result in disqualification, termination of negotiations, or termination of any resulting agreement.

29. VALIDITY PERIOD OF PROPOSAL

29.1 Purpose

The purpose of this section is to ensure that proposals remain valid for a sufficient period to enable MIBCO to complete the evaluation, clarification, due diligence, Proof of Concept (where applicable), approval and contract negotiation processes.

The bidder shall acknowledge and accept the proposal validity requirements contained in this section.

29.2 Proposal Validity Period

All proposals submitted in response to this RFP shall remain valid and binding for a minimum period of:

Four (4) Months

from the official RFP closing date.

The bidder shall maintain all:

- Pricing.
- Commercial terms.
- Technical commitments.
- Resource commitments.
- Service commitments.
- Licensing commitments.

for the duration of the validity period.

29.3 Price Validity

All pricing submitted shall remain fixed for the validity period.

The bidder shall not:

- Withdraw pricing.
- Revise pricing.
- Increase pricing.
- Apply additional charges.
- Modify pricing assumptions.

during the proposal validity period unless requested in writing by MIBCO.

29.4 Technical Validity

The bidder shall ensure that all proposed:

- Products.
- Hardware platforms.
- Software platforms.
- Licences.
- Cloud services.
- Managed services.

remain available throughout the proposal validity period.

The bidder shall immediately notify MIBCO if:

- A proposed product is withdrawn.
- A proposed product reaches End of Sale (EOS).
- A proposed product reaches End of Life (EOL).
- A material product change occurs.

MIBCO reserves the right to reject substitutions proposed after submission.

29.5 Resource Availability

The bidder shall indicate that key implementation and service delivery resources identified in the proposal will remain available during the validity period.

Where a proposed resource becomes unavailable, the bidder shall provide a replacement resource of equivalent or better qualifications and experience.

MIBCO reserves the right to review and approve such replacements.

29.6 Proposal Withdrawal

The bidder shall not withdraw its proposal during the validity period without written approval from MIBCO.

Where a bidder elects to withdraw its proposal during the validity period, MIBCO reserves the right to:

- Exclude the bidder from further consideration.
- Record the withdrawal for future procurement activities.
- Pursue any remedies available in terms of applicable legislation or contractual undertakings.

29.7 Validity Extensions

MIBCO reserves the right to request an extension to the proposal validity period where:

- The evaluation process has not been completed.

- Clarifications are still underway.
- Proof of Concept activities are in progress.
- Contract negotiations are ongoing.
- Internal approval processes require additional time.

Such requests shall be made in writing.

The bidder may:

- Accept the extension; or
- Decline the extension.

Where the bidder declines the extension request, MIBCO may remove the bidder from further consideration.

29.8 Contract Negotiation Period

Should a bidder be identified as the preferred bidder, the proposal shall remain valid until:

- Contract negotiations have been completed; or
- Negotiations have been formally terminated by either party.

The bidder shall continue to honour all commitments contained within the submitted proposal during this period.

29.9 Changes During Validity Period

The bidder shall promptly notify MIBCO of any material changes affecting:

Organisation

- Ownership Structure.
- Corporate Structure.
- B-BBEE Status.
- Financial Standing.

Solution

- Product Availability.
- OEM Partner Status.
- Software Licensing.
- Architecture.

Service Delivery

- Key Personnel.

- Support Arrangements.
- Subcontractors.
- Service Locations.

MIBCO reserves the right to reassess the proposal where material changes occur.

29.10 Currency and Exchange Rate Risk

The bidder shall clearly indicate whether pricing is:

- Fixed in South African Rand (ZAR); or
- Subject to exchange rate fluctuations.

Preference will be given to proposals that provide pricing certainty throughout the validity period.

The bidder shall clearly identify any exchange-rate assumptions.

29.11 OEM Pricing Commitments

Where OEM products, licences or subscriptions form part of the proposed solution, the bidder shall confirm that:

- OEM pricing is secured for the proposal validity period.
- OEM licensing remains available.
- OEM support remains available.
- OEM partner status remains valid.

Evidence may be requested by MIBCO.

29.12 Confirmation of Validity

The bidder shall provide a formal statement within its proposal confirming that:

The proposal shall remain valid for a minimum period of four (4) months from the official proposal closing date and that all pricing, technical commitments, service commitments and resource commitments shall remain unchanged for the duration of the validity period.

29.13 Bidder Declaration

The bidder shall complete the following declaration:

Requirement	Confirm (Yes/No)
Proposal valid for minimum four (4) months	
Pricing valid for minimum four (4) months	
Technical solution valid for minimum four (4) months	

Key resources available during validity period	
OEM commitments secured	
Material changes will be disclosed to MIBCO	

Failure to comply with the proposal validity requirements may result in the proposal being deemed non-responsive and excluded from further evaluation.

30. CONTRACT AWARD

30.1 Purpose

The purpose of this section is to define the basis upon which MIBCO may award a contract arising from this Request for Proposal (RFP).

The contract award process shall be conducted in a fair, transparent, objective and auditable manner and shall be consistent with MIBCO procurement governance requirements.

Submission of a proposal does not create any obligation on MIBCO to award a contract to any bidder.

30.2 Right to Award

MIBCO reserves the right to:

- Award the entire scope of work to a single bidder.
- Award selected components of the scope.
- Award selected phases of the solution.
- Award based on budget availability.
- Award based on strategic priorities.
- Negotiate aspects of the proposal.
- Not award the contract.
- Cancel the RFP entirely.

MIBCO shall not be liable for any costs incurred by bidders in preparing or submitting a proposal.

30.3 Basis of Award

The contract shall not necessarily be awarded to:

- The lowest-priced bidder; or
- The highest-scoring bidder.

The final award decision shall consider:

- Functional Evaluation Results.

- Cybersecurity Capability.
- Technical Compliance.
- Managed Service Capability.
- Commercial Value.
- B-BBEE Status.
- Risk Profile.
- Organisational Capability.
- Reference Checks.
- Due Diligence Findings.
- Proof of Concept Results (where applicable).

The successful bidder shall be the bidder whose proposal is considered to provide the best overall value and lowest operational and cybersecurity risk to MIBCO.

30.4 Modular Award Approach

MIBCO has adopted a modular procurement strategy.

Accordingly, MIBCO reserves the right to:

Award Phase 1 Only

- NGFW
- SD-WAN
- Threat Prevention
- Azure Integration

Award Phase 1 and Phase 2

- Foundation Platform
- Zero Trust Services

Award Full Solution

- Foundation Platform
- Zero Trust Services
- Security Service Edge
- Advanced Security Services

Defer Components

MIBCO may elect to defer:

- CASB
- DLP
- UEBA
- RBI
- Other optional services

for future procurement cycles.

The bidder acknowledges and accepts this procurement approach.

30.5 Future Expansion Rights

The successful bidder shall honour the future expansion pricing submitted within:

- Annexure F – Future Expansion Pricing Schedule.

MIBCO reserves the right to procure future services during the contract period including:

- Additional users.
- Additional branch offices.
- Additional contractors.
- Additional bandwidth.
- Additional security services.

The bidder shall maintain pricing consistency and commercially reasonable expansion costs throughout the contract period.

30.6 Clarification and Negotiation

Following evaluation, MIBCO may enter into clarification and negotiation discussions with one or more bidders.

Discussions may include:

Commercial Matters

- Pricing.
- Payment terms.
- Contract structure.
- Service credits.

Technical Matters

- Architecture.

- Sizing.
- Integration.
- Security controls.

Operational Matters

- Support model.
- Escalation processes.
- Reporting arrangements.

Clarification discussions shall not automatically imply contract award.

30.7 Proof of Concept Requirement

Where MIBCO elects to conduct a Proof of Concept (PoC), successful completion of the PoC may be a prerequisite for contract award.

The PoC may assess:

- NGFW Functionality.
- SD-WAN Functionality.
- Azure Integration.
- ZTNA Capabilities.
- Security Analytics.
- Device Posture Controls.
- SOC Integration.

MIBCO reserves the right to disqualify a bidder that fails critical PoC test scenarios.

30.8 Due Diligence Rights

MIBCO reserves the right to conduct due diligence on any bidder.

Due diligence may include:

Financial Due Diligence

- Financial Stability.
- Creditworthiness.
- Sustainability.

Technical Due Diligence

- Solution Validation.

- Architecture Validation.
- Performance Validation.

Operational Due Diligence

- Support Capability.
- Resource Capability.
- Service Management Capability.

Security Due Diligence

- Security Practices.
- Certifications.
- Compliance Posture.

The bidder shall cooperate fully with any due diligence activities.

30.9 Customer Reference Verification

MIBCO reserves the right to contact customer references supplied by the bidder.

Reference checks may evaluate:

- Project delivery performance.
- Security capability.
- Managed service performance.
- Support responsiveness.
- Customer satisfaction.

MIBCO may reject a proposal where reference feedback raises significant concerns.

30.10 Contract Negotiation

The successful bidder shall enter into contract negotiations with MIBCO.

The following documents may form part of the contractual agreement:

- Proposal Submission.
- RFP Document.
- Response Annexures.
- SLA.
- Managed Service Agreement.
- Implementation Plan.

- Pricing Schedule.
- Security Requirements.
- Compliance Requirements.

The bidder shall remain bound by the commitments contained within its submitted proposal unless otherwise agreed in writing.

30.11 Failure of Contract Negotiations

Should contract negotiations fail, MIBCO reserves the right to:

- Terminate negotiations.
- Enter negotiations with the next-ranked bidder.
- Reissue the RFP.
- Cancel the procurement process.

MIBCO shall not be obliged to provide compensation for unsuccessful negotiations.

30.12 Conditions Precedent to Award

Contract award may be subject to successful completion of one or more of the following:

Requirement	May Be Required
Technical Clarification	Yes
Due Diligence	Yes
Architecture Workshop	Yes
Proof of Concept	Yes
Reference Verification	Yes
OEM Verification	Yes
Financial Due Diligence	Yes
Security Assessment	Yes

MIBCO reserves the right to introduce additional conditions where considered necessary.

30.13 Contract Term

The intended contract term shall be:

Thirty-Six (36) Months

The contract may include provisions for:

- Extension.
- Expansion.
- Additional services.
- Additional sites.
- Additional users.

subject to mutual agreement and budget availability.

30.14 Technology Refresh

Because the solution is being procured as a managed service, the successful bidder shall be responsible for ensuring that the solution remains supported throughout the contract period.

The bidder shall provide:

- Hardware lifecycle management.
- Software lifecycle management.
- Firmware management.
- Security updates.
- Technology refresh recommendations.

No component of the solution shall reach:

- End of Sale (EOS),
- End of Support (EOSP), or
- End of Life (EOL)

during the contract period without an approved replacement strategy.

30.15 Transition-In Requirements

Following contract award, the successful bidder shall participate in a formal project initiation process including:

- Kick-Off Meeting.
- Governance Establishment.
- Project Mobilisation.
- Discovery Phase Planning.
- Resource Allocation.
- Detailed Scheduling.

The bidder shall commence implementation only after formal approval from MIBCO.

30.16 Transition-Out Requirements

At the conclusion of the contract, or in the event of contract termination, the successful bidder shall provide orderly transition assistance.

The transition process shall include:

- Knowledge transfer.
- Documentation handover.
- Configuration export.
- Access revocation.
- Service continuity planning.

The bidder shall cooperate fully with any replacement service provider appointed by MIBCO.

30.17 No Obligation to Award

MIBCO reserves the unrestricted right to:

- Reject any proposal.
- Reject all proposals.
- Modify procurement requirements.
- Re-advertise the requirement.
- Cancel the RFP.

without incurring any liability to any bidder.

30.18 Notification of Award

Following completion of the evaluation and approval process:

- The successful bidder shall be notified in writing.
- Unsuccessful bidders may be notified in accordance with MIBCO procurement processes.
- No public announcement shall be made by the successful bidder without prior written approval from MIBCO.

30.19 Bidder Acknowledgement

By submitting a proposal, the bidder acknowledges and accepts that:

1. MIBCO may award all or part of the scope.
2. MIBCO may procure solution modules in phases.
3. MIBCO is not obliged to award a contract.

4. MIBCO may conduct due diligence and Proof of Concept activities.
5. MIBCO may negotiate with one or more bidders.
6. MIBCO may enter negotiations with another bidder if negotiations fail.
7. MIBCO's decision regarding contract award shall be final.

The submission of a proposal shall constitute acceptance of the contract award principles contained within this RFP.

31. QUESTIONS REGARDING THE RFP

31.1 Purpose

The purpose of this section is to provide a formal process through which bidders may seek clarification regarding the requirements contained within this Request for Proposal (RFP).

MIBCO recognises that this procurement involves a complex hybrid architecture incorporating:

- Secure Network as a Service (SNaaS)
- Next Generation Firewall (NGFW)
- Secure SD-WAN
- Zero Trust Network Access (ZTNA)
- Security Service Edge (SSE)
- Hybrid Data Centre Security
- Microsoft Azure Disaster Recovery Security
- Managed Security Services

Accordingly, bidders are encouraged to seek clarification on any aspect of the RFP that may be unclear or require further explanation.

31.2 RFP Contact Person

All enquiries relating to this RFP shall be directed to:

Dan Mkwanazi

Email: Dan.Mkwanazi@mibco.org.za

Organisation: Motor Industry Bargaining Council (MIBCO)

31.3 Official Communication Channel

All communication regarding this RFP shall be conducted via email.

The subject line of all correspondence shall be:

"RFP – Fully Managed Secure Network and Cybersecurity Service (SNaaS)"

MIBCO reserves the right to disregard queries submitted through unofficial communication channels.

31.4 Clarification Period

Bidders may submit clarification questions from the date of issue of this RFP until the clarification closing date.

Questions received after the clarification closing date may not be considered.

MIBCO reserves the right to:

- Respond to questions received after the closing date;
- Decline to respond to late questions;
- Extend the clarification period where required.

31.5 Clarification Meetings

MIBCO reserves the right to facilitate:

- Individual clarification sessions;
- Virtual clarification meetings;
- Technical workshops;
- Architecture review discussions;
- Question and answer sessions.

such meetings may be conducted:

- In person;
- Via Microsoft Teams;
- Via other approved collaboration platforms.

Participation in clarification meetings does not confer any advantage during the evaluation process.

31.6 Bidder Site Visits and Information Sessions

Where considered appropriate, MIBCO may arrange:

- Site visits;
- Current environment briefings;
- High-level architecture discussions;
- Hybrid infrastructure overview sessions.

The purpose of such engagements is solely to assist bidders in understanding the environment and requirements.

No bidder shall rely on verbal statements made during such engagements unless confirmed in writing by MIBCO.

31.7 Nature of Questions

Questions may relate to:

Technical Requirements

- NGFW requirements;
- SD-WAN requirements;
- Azure integration requirements;
- ZTNA requirements;
- Security requirements;
- SOC integration requirements.

Commercial Requirements

- Pricing schedules;
- Modular procurement requirements;
- Contracting model;
- Managed service requirements.

Submission Requirements

- Mandatory documentation;
- Annexures;
- Proposal structure.

Evaluation Requirements

- Functional evaluation criteria;
- Evaluation process;
- Proof of Concept requirements.

31.8 Response to Questions

MIBCO may respond to bidder questions by:

- Email response;
- Formal clarification notice;
- Addendum to the RFP;
- Clarification workshop.

Where a question and answer may be relevant to all bidders, MIBCO reserves the right to distribute the response to all participating bidders.

MIBCO shall not be obliged to identify the originating bidder.

31.9 Formal Addenda

Where a clarification materially affects the requirements of this RFP, MIBCO may issue a formal addendum.

Addenda may include:

- Corrections;
- Clarifications;
- Amendments;
- Additional requirements;
- Revised submission dates.

Any addendum issued by MIBCO shall form part of the RFP and shall be binding on all bidders.

31.10 Bidder Responsibility

It remains the responsibility of the bidder to ensure that:

- All clarifications are obtained prior to submission;
- All addenda are reviewed;
- All proposal assumptions are valid;
- The submitted proposal fully addresses the requirements of this RFP.

Failure to obtain clarification shall not relieve the bidder of responsibility for meeting the requirements of this RFP.

31.11 Restrictions on Communication

Bidders shall not attempt to obtain information relating to this RFP from:

- Evaluation Committee members;
- Adjudication Committee members;
- MIBCO Executives;
- MIBCO employees not formally designated as RFP contacts.

Any attempt to improperly influence the procurement process may result in disqualification.

31.12 No Verbal Commitments

No statement made verbally by any MIBCO employee, representative, consultant or advisor shall be regarded as binding unless confirmed in writing by MIBCO.

Only written responses issued through the formal clarification process shall be considered authoritative.

31.13 Confidentiality of Questions

All questions submitted by bidders shall be treated confidentially.

However, where a clarification is deemed relevant to all bidders, MIBCO may distribute the clarification response without identifying the originating bidder.

31.14 Request for Additional Information

MIBCO reserves the right to request additional information from any bidder during:

- Clarification activities;
- Technical evaluation;
- Commercial evaluation;
- Due diligence activities;
- Proof of Concept activities;
- Contract negotiations.

Such requests shall not constitute acceptance of a proposal.

31.15 Clarification Register

MIBCO may maintain a Clarification Register containing:

Reference Number	Question	Response	Date Issued

Where maintained, the Clarification Register shall form part of the official procurement record.

31.16 Bidder Declaration

By submitting a proposal, the bidder acknowledges that:

1. The bidder has had a reasonable opportunity to seek clarification.
2. The bidder understands the requirements contained within the RFP.
3. The bidder has considered all responses and addenda issued by MIBCO.
4. The bidder accepts responsibility for the completeness of its proposal.
5. No verbal representations have been relied upon unless confirmed in writing by MIBCO.

The bidder further acknowledges that failure to request clarification prior to submission shall not constitute grounds for variation, dispute, additional costs or relief following contract award.

32. TERMS AND CONDITIONS

32.1 Purpose

These Terms and Conditions govern the procurement process associated with this Request for Proposal (RFP) and shall apply to all bidders participating in the procurement process.

Submission of a proposal shall constitute acceptance of these Terms and Conditions.

32.2 RFP Not an Offer

This RFP is an invitation to submit proposals and does not constitute:

- An offer to contract.
- A commitment to procure.
- A commitment to award a contract.
- A representation that a contract will be awarded.

No contractual relationship shall arise between MIBCO and any bidder until a formal written agreement has been executed by both parties.

32.3 Cost of Proposal Preparation

All costs associated with:

- Preparing a proposal.
- Attending meetings.
- Participating in workshops.
- Conducting demonstrations.
- Participating in a Proof of Concept (PoC).
- Participating in contract negotiations.

shall be borne solely by the bidder.

MIBCO shall not be liable for any costs incurred by bidders in connection with this RFP process.

32.4 Right to Amend the RFP

MIBCO reserves the right to:

- Amend any part of this RFP.
- Revise requirements.
- Clarify requirements.
- Correct errors.

- Extend closing dates.
- Issue addenda.

Any amendments shall be communicated through formal written communication and shall form part of the RFP.

Bidders shall ensure that they consider all amendments and addenda when preparing proposals.

32.5 Right to Request Further Information

MIBCO reserves the right to request additional information at any stage of the evaluation process including:

- Technical information.
- Commercial information.
- Financial information.
- Corporate information.
- Security information.
- Compliance information.

Bidders shall provide such information within the timeframe specified by MIBCO.

Failure to do so may adversely affect evaluation outcomes.

32.6 Right to Verify Information

MIBCO reserves the right to verify any information provided by a bidder.

Verification activities may include:

- Reference checks.
- Certification validation.
- Financial verification.
- OEM verification.
- Site visits.
- Background checks.
- Professional qualification verification.

Any inaccurate, misleading or false information may result in disqualification.

32.7 Proposal Ownership

All proposals and supporting documentation submitted to MIBCO shall become the property of MIBCO upon submission.

MIBCO shall not be required to return submitted proposals or supporting documentation.

This provision shall not affect the bidder's ownership of its intellectual property.

32.8 Confidentiality

All parties shall treat information obtained during the procurement process as confidential.

Bidders shall:

- Protect MIBCO information.
- Not disclose information to unauthorised parties.
- Use information solely for preparing their proposals.

The confidentiality obligation shall survive the conclusion of the procurement process.

32.9 Protection of Personal Information

Bidders shall comply with all applicable data protection legislation including:

- Protection of Personal Information Act (POPIA).
- Relevant privacy regulations.
- Information security obligations.

Any personal information received from MIBCO shall be:

- Protected.
- Secured.
- Processed lawfully.
- Used only for purposes related to this RFP.

32.10 Intellectual Property

The bidder shall retain ownership of its pre-existing intellectual property.

However:

- Architectural designs.
- Project deliverables.
- Documentation.
- Operating procedures.
- Configuration documentation.

developed specifically for MIBCO under any resulting contract shall become the property of MIBCO unless otherwise agreed in writing.

The bidder shall grant MIBCO unrestricted rights to use all deliverables produced during the contract term.

32.11 Conflict of Interest

Bidders shall disclose any actual, perceived or potential conflict of interest.

Examples include:

- Personal relationships with MIBCO employees.
- Financial relationships with MIBCO personnel.
- Existing contractual arrangements creating conflicts.
- Participation in preparing this RFP.

MIBCO reserves the right to determine whether a disclosed conflict is acceptable.

Failure to disclose a conflict of interest may result in disqualification.

32.12 Ethical Conduct

Bidders shall conduct themselves ethically and professionally throughout the procurement process.

Bidders shall not:

- Attempt to influence evaluation outcomes.
- Offer gifts or benefits.
- Provide inducements.
- Engage in collusion.
- Engage in anti-competitive conduct.
- Misrepresent information.

Any such conduct may result in disqualification.

32.13 Fraud and Corruption

MIBCO maintains a zero-tolerance approach to:

- Fraud.
- Corruption.
- Bribery.
- Collusion.
- Unethical procurement practices.

Any bidder found to have engaged in such conduct may be:

- Disqualified.
- Excluded from future procurement opportunities.

- Reported to relevant authorities.

32.14 Compliance with Laws

The bidder shall comply with all applicable:

- Laws.
- Regulations.
- Industry standards.
- Regulatory obligations.

This includes compliance with:

- Labour legislation.
- Tax legislation.
- Cybersecurity legislation.
- Data protection legislation.
- Competition legislation.

32.15 Subcontracting

Any subcontracting arrangements shall comply with Section 29 of this RFP.

The bidder shall remain fully responsible for:

- Performance.
- Security.
- Compliance.
- Service delivery.

of any subcontracted services.

No subcontracting arrangement shall relieve the bidder of accountability to MIBCO.

32.16 Reserved Rights

MIBCO reserves the right to:

- Reject any proposal.
- Reject all proposals.
- Not award the contract.
- Award part of the scope.
- Award selected modules only.

- Negotiate with one or more bidders.
- Cancel the RFP.
- Reissue the RFP.

without obligation or liability to any bidder.

32.17 Evaluation Rights

MIBCO reserves the right to:

- Conduct technical evaluations.
- Conduct commercial evaluations.
- Conduct reference checks.
- Conduct due diligence.
- Conduct site visits.
- Conduct Proof of Concept activities.
- Verify certifications.
- Verify OEM relationships.

The bidder shall cooperate with all reasonable evaluation activities.

32.18 Proof of Concept Rights

MIBCO reserves the right to require shortlisted bidders to participate in a Proof of Concept.

The Proof of Concept may include:

- Technical validation.
- Security validation.
- Performance validation.
- Integration validation.

Failure to reasonably participate in a PoC may result in disqualification.

32.19 Modular Procurement Model

The bidder acknowledges that MIBCO may:

- Procure the complete solution.
- Procure selected modules only.
- Procure modules over multiple budget periods.
- Expand or defer functionality.

The bidder shall honour the modular pricing submitted as part of the proposal.

32.20 No Exclusivity

Participation in this RFP shall not create any exclusivity rights.

MIBCO may:

- Engage multiple vendors.
- Conduct separate procurement processes.
- Seek alternative solutions.

at its sole discretion.

32.21 Contract Negotiations

Selection as a preferred bidder shall not constitute contract award.

Contract award shall be subject to:

- Successful negotiations.
- Approval by MIBCO.
- Agreement on contractual terms.
- Agreement on commercial terms.
- Agreement on service levels.

Should negotiations fail, MIBCO reserves the right to negotiate with another bidder.

32.22 Liability

MIBCO shall not be liable for:

- Proposal preparation costs.
- Demonstration costs.
- PoC costs.
- Travel costs.
- Consulting costs.
- Opportunity costs.

incurred by any bidder.

32.23 Public Statements

Bidders shall not issue:

- Press statements.

- Public announcements.
- Marketing communications.

relating to this RFP or any resulting contract without prior written approval from MIBCO.

32.24 Record Retention

The bidder shall retain records relating to:

- Proposal submissions.
- Project activities.
- Service delivery.
- Security activities.
- Compliance activities.

for the duration of the contract and any applicable legal retention period.

32.25 Audit Rights

MIBCO reserves the right to audit:

- Contract performance.
- Service delivery.
- Security controls.
- Compliance controls.
- Service management processes.

The successful bidder shall provide reasonable cooperation with audit activities.

32.26 Cybersecurity Obligations

Because the services relate directly to critical cybersecurity functions, the successful bidder shall:

- Maintain appropriate security controls.
- Protect MIBCO information.
- Notify MIBCO of cybersecurity incidents.
- Cooperate in security investigations.
- Maintain secure operational practices.

The bidder shall immediately notify MIBCO of any security incident that could affect the confidentiality, integrity or availability of MIBCO information or services.

32.27 Business Continuity

The successful bidder shall maintain appropriate business continuity and disaster recovery capabilities to ensure uninterrupted service delivery.

Evidence of these capabilities may be requested during evaluation or contract execution.

32.28 Acceptance of Terms

Submission of a proposal shall constitute acknowledgement and acceptance of all terms and conditions contained within this RFP.

Any exceptions shall be clearly identified within the proposal.

Where no exceptions are submitted, MIBCO shall assume that the bidder accepts these Terms and Conditions in full.

32.29 Governing Law

Any resulting contract shall be governed by and interpreted in accordance with the laws of the Republic of South Africa.

The bidder agrees to submit to the jurisdiction of the South African courts in relation to any disputes arising from the procurement process or resulting agreement.

32.30 Survival of Provisions

The following provisions shall survive the conclusion, cancellation or termination of the procurement process or any resulting agreement:

- Confidentiality.
- Intellectual Property.
- Audit Rights.
- Record Retention.
- Cybersecurity Obligations.
- Compliance Obligations.
- Dispute Resolution.
- Applicable Regulatory Requirements.

These provisions shall remain in force for as long as required by law or contract.

33. DISCLAIMER

33.1 General Disclaimer

This Request for Proposal (RFP) has been prepared by the Motor Industry Bargaining Council (MIBCO) for the purpose of obtaining proposals from suitably qualified service providers for the provision of a Fully Managed Secure Network and Cybersecurity Service (SNaaS).

The information contained in this RFP is provided in good faith and is believed to be accurate at the date of publication. However, MIBCO makes no representation, warranty or guarantee, express or implied, regarding the accuracy, completeness or suitability of the information contained herein.

Bidders shall satisfy themselves as to the accuracy, completeness and relevance of all information contained within this RFP and any subsequently issued addenda or clarification notices.

33.2 No Obligation to Award

Nothing contained in this RFP shall be construed as:

- A commitment by MIBCO to award a contract.
- A commitment by MIBCO to proceed with the procurement.
- An offer capable of acceptance.
- A promise to enter into a contractual relationship with any bidder.

MIBCO reserves the right, at its sole discretion, to:

- Accept or reject any proposal.
- Accept or reject part of any proposal.
- Negotiate with one or more bidders.
- Suspend the procurement process.
- Amend the procurement process.
- Re-advertise the requirement.
- Cancel this RFP at any time.

without incurring any liability to any bidder.

33.3 Costs and Expenses

All costs incurred in connection with:

- Reviewing this RFP.
- Attending clarification meetings.
- Preparing a proposal.
- Participating in demonstrations.
- Participating in architecture workshops.
- Participating in a Proof of Concept (PoC).
- Participating in negotiations.

shall be entirely for the account of the bidder.

MIBCO shall not be liable for:

- Bid preparation costs.
- Travel costs.
- Consultant costs.
- Opportunity costs.
- Demonstration costs.
- PoC costs.

regardless of the outcome of this procurement process.

33.4 Accuracy of Information

Although every effort has been made to provide accurate information, MIBCO does not warrant that:

- All information provided is complete.
- All information provided is accurate.
- All requirements have been fully described.
- Circumstances will remain unchanged during the procurement process.

Bidders are encouraged to submit clarification requests where additional information may be required.

33.5 Right to Amend

MIBCO reserves the right to amend, clarify, substitute or withdraw any part of this RFP.

Such amendments may include:

- Technical requirements.
- Commercial requirements.
- Submission requirements.
- Timelines.
- Evaluation criteria.
- Scope of work.

Any amendment issued by MIBCO shall form part of this RFP.

Bidders shall be responsible for ensuring that all amendments and addenda have been considered when preparing their proposals.

33.6 Proposal Evaluation

MIBCO reserves the right to:

- Verify information supplied by bidders.
- Conduct due diligence.
- Conduct reference checks.
- Conduct site visits.
- Conduct architecture reviews.
- Request additional information.
- Conduct a Proof of Concept.
- Verify certifications.
- Verify financial information.

MIBCO shall not be required to provide justification for evaluation decisions beyond applicable governance and legal requirements.

33.7 Confidentiality of Evaluation

All evaluation activities, assessments, scoring, recommendations and deliberations conducted by MIBCO shall remain confidential.

Bidders shall not attempt to:

- Obtain access to evaluation records.
- Influence evaluation outcomes.
- Contact evaluators directly.
- Influence decision makers through unofficial channels.

Such actions may result in disqualification.

33.8 No Reliance on Verbal Statements

Bidders shall not rely on:

- Verbal communications.
- Informal discussions.
- Assumptions.
- Unconfirmed statements.

Only information contained within:

- This RFP.
- Official clarification responses.
- Official addenda issued by MIBCO.

shall be considered authoritative.

33.9 Limitation of Liability

MIBCO, its officers, employees, advisors and representatives shall not be liable for any loss, damage, expense or claim arising from:

- Participation in this procurement process.
- Preparation of proposals.
- Reliance on information contained within this RFP.
- Cancellation of the procurement process.
- Failure to award a contract.

The bidder participates in this process entirely at its own risk.

33.10 No Exclusivity

This RFP does not create:

- Exclusivity rights.
- Preferred supplier status.
- Guaranteed future opportunities.

MIBCO reserves the right to engage with other suppliers, conduct additional procurements or source alternative solutions at its sole discretion.

33.11 Intellectual Property

All intellectual property rights relating to this RFP remain the property of MIBCO.

This RFP may not be:

- Copied.
- Reproduced.
- Distributed.
- Published.
- Disclosed to third parties.

except to the extent required for the preparation of a proposal.

Bidders shall not use the contents of this RFP for any purpose other than responding to the procurement.

33.12 Data Protection and Privacy

Any information provided by MIBCO to bidders shall be treated as confidential and shall be protected in accordance with:

- The Protection of Personal Information Act (POPIA).
- Applicable privacy legislation.
- Industry best practices.

Bidders shall implement appropriate safeguards to protect information received during the procurement process.

33.13 Reservation of Rights

MIBCO expressly reserves the right to:

- Procure all modules.
- Procure selected modules only.
- Procure services in phases.
- Delay implementation phases.
- Expand programme scope.
- Reduce programme scope.
- Change priorities due to budget considerations.

The modular procurement approach described in this RFP is a fundamental requirement of the procurement strategy.

33.14 Contractual Supremacy

In the event of a contract being awarded, the final signed agreement between MIBCO and the successful bidder shall supersede this RFP to the extent that any inconsistency exists between the two documents.

Until such time as a contract is executed by both parties, no legally binding agreement shall exist.

33.15 Bidder Declaration

By submitting a proposal, the bidder acknowledges and agrees that:

1. It has read and understood this RFP in its entirety.
2. It accepts the requirements, conditions and procedures contained herein.
3. It has had sufficient opportunity to seek clarification.
4. It has relied on its own investigations and assessments.
5. It understands that MIBCO is under no obligation to award any contract.
6. It accepts all risks associated with participation in this procurement process.
7. It agrees to be bound by the terms and conditions of this RFP.

ANNEXURE A – COMPLIANCE MATRIX

Instructions: Complete all fields. Use:

- FC = Fully Compliant
- PC = Partially Compliant
- NC = Non-Compliant

Ref	Requirement	FC	PC	NC	Evidence Reference	Comments
10	NGFW					
10	SD-WAN					
10	TLS 1.3 Inspection					
11	IPS					
11	IDS					
11	DNS Security					
11	Sandboxing					
11	Threat Intelligence					
11	DLP					
11	CASB					
11	SWG					
11	RBI					
11	UEBA					
12	Azure DR Integration					
12	Hybrid Security Architecture					
13	ZTNA					
13	Continuous Verification					
14	Entra ID Integration					

14	Intune Integration					
14	Defender Integration					
15	Wazuh Integration					
15	Grafana Integration					
15	N8N Integration					
16	Risk Management Framework					
17	POPIA Support					
17	PCI-DSS Support					

ANNEXURE B – TECHNICAL RESPONSE SCHEDULE

Solution Overview

Requirement	Vendor Response
Proposed OEM	
Product Suite	
Architecture Summary	
Deployment Model	
Management Platform	
Primary Security Platform	
Azure Security Model	
DR Security Model	

Performance Declaration

Requirement	Manufacturer Published	Independently Tested	Proposed
Firewall Throughput			

NGFW Throughput			
Threat Prevention Throughput			
SSL Inspection Throughput			
IPSEC Throughput			
Concurrent Sessions			
New Sessions Per Second			
Remote Users Supported			

ANNEXURE C – MODULAR COSTING SCHEDULE

PHASE 1 – FOUNDATION PLATFORM

Component	Qty	Once-Off	Monthly	36-Month Total
Data Centre NGFW				
Branch Firewalls				
SD-WAN				
IPS				
DNS Security				
Threat Prevention				
Azure Connectivity				
Logging Platform				
Reporting Platform				

Phase 1 Total

PHASE 2 – ZERO TRUST

Component	Qty	Once-Off	Monthly	36-Month Total
ZTNA				
Device Posture Validation				

Conditional Access Integration				
Contractor Controls				
Session Recording				

Phase 2 Total

PHASE 3 – SSE

Component	Qty	Once-Off	Monthly	36-Month Total
CASB				
SWG				
RBI				

Phase 3 Total

PHASE 4 – ADVANCED SECURITY

Component	Qty	Once-Off	Monthly	36-Month Total
DLP				
UEBA				
AI Security Analytics				
Threat Hunting				

Phase 4 Total

ANNEXURE D – PROFESSIONAL SERVICES COST SCHEDULE

Deliverable	Mandatory	Cost
Discovery Workshops	Yes	
Current State Assessment	Yes	
High Level Design	Yes	
Low Level Design	Yes	
Project Management	Yes	

Installation	Yes	
Configuration	Yes	
Migration	Yes	
Testing	Yes	
UAT Support	Yes	
Hypercare	Yes	
Documentation	Yes	
Knowledge Transfer	Yes	
Training	Yes	

Total Professional Services Cost

ANNEXURE E – MANAGED SERVICES COST SCHEDULE

Service	Monthly Cost
24x7 Monitoring	
Incident Management	
Problem Management	
Change Management	
Security Monitoring	
Reporting	
Service Reviews	
Vendor Management	
Patch Management	
Firmware Management	
Threat Intelligence Management	

ZTNA Administration	
DLP Administration	
CASB Administration	

Total Monthly Managed Service Cost

ANNEXURE F – FUTURE EXPANSION PRICING

Item	Unit Cost
Additional Branch Site	
Additional User	
Additional ZTNA User	
Additional Contractor User	
Additional 100Mbps Throughput	
Additional 500Mbps Throughput	
Additional Firewall Appliance	
Additional CASB User	
Additional DLP User	
Additional UEBA User	
Additional Reporting Storage Year	

ANNEXURE G – RISK REGISTER

Risk ID	Risk Description	Impact	Probability	Mitigation	Owner
R1	Migration Failure				
R2	Security Misconfiguration				
R3	Azure DR Failure				

R4	Data Loss				
R5	Service Outage				
R6	Credential Compromise				
R7	Third-Party Risk				
R8	Capacity Exhaustion				

ANNEXURE H – IMPLEMENTATION PLAN

Phase	Activity	Start Date	End Date	Deliverable
Initiation	Kick-Off			
Discovery	Current State Assessment			
Design	HLD			
Design	LLD			
Build	Infrastructure Build			
Testing	UAT			
Migration	Production Cutover			
Hypercare	Stabilisation			
Handover	Operational Acceptance			

ANNEXURE I – CUSTOMER REFERENCES

Minimum 3 References Required

Customer	Industry	Sites	Users	Scope Delivered	Contact	Telephone

ANNEXURE J – HYBRID ARCHITECTURE RESPONSE

Requirement	Vendor Response
Data Centre Security Architecture	
Azure DR Architecture	
Policy Synchronisation Method	
Security Management Approach	
DR Security Controls	
Azure Connectivity Design	
Replication Security Controls	
RTO Supported	
RPO Supported	
Logging Continuity Approach	

ANNEXURE K – PROOF OF CONCEPT RESPONSE (NOT COMPULSORY)

Capability	Demonstrated	Comments
NGFW		
SD-WAN		
ZTNA		
CASB		
DLP		
UEBA		
Azure Integration		
Wazuh Integration		
Grafana Integration		

N8N Integration		

ANNEXURE L – MANDATORY DOCUMENTATION CHECKLIST

Document	Included
Company Registration	☐
Tax Compliance PIN	☐
B-BBEE Certificate	☐
Audited Financial Statements	☐
Professional Indemnity Insurance	☐
Cyber Insurance	☐
OEM Certifications	☐
Technical Proposal	☐
Architecture Diagrams	☐
Project Plan	☐
Migration Plan	☐
Rollback Plan	☐
Risk Register	☐
SLA Proposal	☐
Completed Annexures A–P	☐

ANNEXURE M – DETAILED FUNCTIONAL EVALUATION SCORECARD

Cybersecurity Capability (35)

Criterion	Max
NGFW	5
Threat Prevention	5
Zero Trust	5
CASB/SWG/DLP/RBI	5
UEBA	4
Threat Intelligence	3
Azure Security	3
Identity Security	3
Security Reporting	2

Technical Compliance (25)

Criterion	Max
Technical Compliance	5
Hybrid Architecture	5
Microsoft Integration	4
Scalability	3
Performance	4
Architecture Quality	4

Managed Service Capability (15)

Criterion	Max
Service Delivery	3
Governance	2

Monitoring	3
SOC Support	2
Reporting	2
Lifecycle Management	3

Implementation Methodology (10)

Criterion	Max
Governance	2
Methodology	2
Migration	2
Risk Management	2
Testing & Cutover	2

Vendor Experience (10)

Criterion	Max
Similar Deployments	2
Azure Projects	2
Managed Security Experience	2
References	2
Resource Capability	2

Support Model (5)

Criterion	Max
Support Availability	1
Escalations	1
Local Presence	1
OEM Support	1

Service Levels	1

ANNEXURE N – PROPOSAL COMPLETENESS DECLARATION

I, _____, hereby declare that:

- The proposal is complete.
- All mandatory documents have been submitted.
- All information supplied is true and accurate.
- All Annexures have been completed.
- Modular pricing has been supplied.
- The bidder accepts the requirements of the RFP.

Signature: _____

Date: _____

ANNEXURE O – BIDDER DECLARATION AND ACCEPTANCE

Company Name: _____

Authorised Representative: _____

Position: _____

I confirm that:

- I am authorised to submit this proposal.
- I accept the RFP Terms and Conditions.
- I accept the modular procurement approach.
- I understand MIBCO is not obligated to award a contract.
- I accept the evaluation process.

Signature: _____

Date: _____

ANNEXURE P – GLOSSARY OF TERMS, ACRONYMS AND ABBREVIATIONS

Acronym	Meaning
NGFW	Next Generation Firewall
SD-WAN	Software Defined Wide Area Network
ZTNA	Zero Trust Network Access
SSE	Security Service Edge
CASB	Cloud Access Security Broker
SWG	Secure Web Gateway
DLP	Data Loss Prevention
RBI	Remote Browser Isolation
UEBA	User and Entity Behaviour Analytics
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
MFA	Multi-Factor Authentication
PAM	Privileged Access Management
JIT	Just-In-Time Access
SOC	Security Operations Centre
SIEM	Security Information and Event Management
API	Application Programming Interface
Azure DR	Azure Disaster Recovery
POPIA	Protection of Personal Information Act
PCI-DSS	Payment Card Industry Data Security Standard
FSCA	Financial Sector Conduct Authority
COFI	Conduct of Financial Institutions

PFA	Pension Funds Act
NIST	National Institute of Standards and Technology
FIPS	Federal Information Processing Standard
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Indicator Information
OEM	Original Equipment Manufacturer
SLA	Service Level Agreement
RTO	Recovery Time Objective
RPO	Recovery Point Objective
HLD	High Level Design
LLD	Low Level Design
UAT	User Acceptance Testing
TCO	Total Cost of Ownership