



**Annexure 1: Bid Specification: RFB 3115-2025 -****REQUEST FOR BID FOR PROCUREMENT OF NEXT GENERATION FIREWALLS, LICENSES, SUPPORT, MAINTENANCE AND TRAINING FOR THE SOUTH AFRICAN POLICE SERVICE (SAPS) FOR A PERIOD OF SIXTY (60) MONTHS**

**TECHNICAL, PRICING AND PREFERENCE POINTS REQUIREMENTS**

Contents

[Contents 2](#_Toc202540564)

[1. Introduction 4](#_Toc202540565)

[1.1 Purpose 4](#_Toc202540566)

[1.2 Background 4](#_Toc202540567)

[2. Scope of Bid 4](#_Toc202540568)

[2.1 Scope of Work 4](#_Toc202540569)

[2.2 Delivery address 5](#_Toc202540570)

[2.3 Customer Infrastructure and Environment Requirements 5](#_Toc202540571)

[2.3.1 Customer methods, standards and policy environment 5](#_Toc202540572)

[2.4 Technology Requirements 5](#_Toc202540573)

[2.4.1 Appliance Base Firewalls 5](#_Toc202540574)

[2.4.2 Manager and Reporter 8](#_Toc202540575)

[2.4.3 Sandboxing Capability (standalone appliance only) 10](#_Toc202540576)

[2.4.4 Cloud-Based or On Premise (Four (4)) Web Application Firewall . 11](#_Toc202540577)

[2.4.5 Threat Control and Network Threat Protection 13](#_Toc202540578)

[2.4.6 Intrusion Prevention System Capability 14](#_Toc202540579)

[2.4.7 Anti-DDoS capability (standalone appliance only) 15](#_Toc202540580)

[2.5 Functional requirements 16](#_Toc202540581)

[2.5.1 Lifecycle Management 16](#_Toc202540582)

[2.5.2 Skills Transfer and Training 16](#_Toc202540583)

[3 Bid Evaluation Stages 16](#_Toc202540584)

[3.1 Mandatory Administrative Responsiveness (Stage 1) 17](#_Toc202540585)

[3.1.1 Attendance of briefing session 17](#_Toc202540586)

[3.1.2 Registered Supplier 17](#_Toc202540587)

[3.1.3 Bid Submission Instructions 17](#_Toc202540588)

[3.2 Technical returnable documents 18](#_Toc202540589)

[3.2.1 Instruction and evaluation criteria 18](#_Toc202540590)

[3.2.2 Technical mandatory requirements (Stage 2) 18](#_Toc202540591)

[3.3 Special Conditions of Contract Verification (Stage 3) 20](#_Toc202540592)

[3.3.1 Special Conditions of Contract 21](#_Toc202540593)

[3.3.2 Declaration of compliance and acceptance SCC 28](#_Toc202540594)

[3.4 Costing and Preference Points Evaluation (Stage 4) 28](#_Toc202540595)

[3.4.1 Costing and Preference Evaluation 28](#_Toc202540596)

[3.4.2 Costing and Pricing Conditions 28](#_Toc202540597)

[3.4.3 Bid Pricing Schedule 29](#_Toc202540598)

[3.4.4 Rate of Exchange Pricing Information 29](#_Toc202540599)

[3.4.5 Bid Exchange Rate Conditions 29](#_Toc202540600)

[3.5 Declaration of Acceptance 30](#_Toc202540601)

[3.6 Preference Requirements 30](#_Toc202540602)

[Annex A: Bidder Substantiating Evidence 34](#_Toc202540603)

[4 Technical Mandatory Requirement Evidence 34](#_Toc202540604)

[4.1 Bidder Certification / Affiliation Requirements 34](#_Toc202540605)

[4.2 Bidder Experience and Capability Requirements 34](#_Toc202540606)

[4.3 Special Conditions of Contract Acceptance 35](#_Toc202540607)

[4.4 Third Party Risk Management Assessment 35](#_Toc202540608)

[4.5 Product Functional Requirement 35](#_Toc202540609)

[4.6 Preferential Goal Requirements 35](#_Toc202540610)

[Annex B: THIRD-PARTY RISK MANAGEMENT (TPRM) ASSESSMENT 37](#_Toc202540611)

[Annex C: Product/Service Functional Requirements ADDENDUM 1 43](#_Toc202540612)

[Appliance Base Firewalls 43](#_Toc202540613)

[Sandboxing Capability (standalone appliance only) 47](#_Toc202540614)

[On Premise or Cloud-Based Web Application Firewall Services 48](#_Toc202540615)

[Threat Control and Network Threat Protection 50](#_Toc202540616)

[Intrusion Prevention System Capability 51](#_Toc202540617)

[Anti-DDoS capability (standalone appliance only) 51](#_Toc202540618)

[Lifecycle Management 52](#_Toc202540619)

[Skills Transfer and Training 53](#_Toc202540620)

## Introduction

## 1.1 Purpose

The purpose of this **RFB** is to invite Suppliers (hereinafter referred to as “bidders”) to submit bids for the Procurement of Next-Generation Firewalls (NGFWs) technology, including necessary licenses, support, maintenance, and training for the South African Police Service (SAPS). This initiative will also cover staffing requirements, specifically one full-time junior security engineer and the services of a senior security architect on a bi-monthly basis, for a period of sixty (60) months.

## 1.2 Background

SITA entered into a Business Agreement (BA) and Service Level Agreement (SLA) with SAPS to provide Network Security services. This is a critical service to protect SAPS from the risk of exposure and being vulnerable to cyber-attacks.

The SAPS information infrastructure and databases are protected by a perimeter and application firewall. A firewall is the first line of defence in protecting the technology network environment. A firewall technology consists of hardware and software used to monitor the flow of information entering and leaving the network in order to authorise and/or reject access to network resources based on a prescribed security policy.

SAPS has been leveraging existing Check Point firewall security technologies to protect its critical infrastructure. However, with the rapid evolution of cyber threats, it is essential to evaluate SAPS’ security measures continuously. The current security infrastructure, while effective, requires modernisation to keep pace with advanced threats. An open tender process will enable SAPS to identify the best value-for-money technologies available in the market, ensuring that SAPS’ security infrastructure remains robust and future-proof.

Considering the technology growth worldwide and the move towards cloud computing, the information stored, processed and transmitted over the network daily, SAPS needs to uphold effective and controlled levels of protection.

# Scope of Bid

## 2.1 Scope of Work

The scope of work for the bidders is as follows:

1. Procurement of the following NGFW, including hardwareinstallation, and configuration to enable high availability/clustered firewall deployment:
2. Four (4) Enterprise Firewall Services.
3. Twenty (20) Regional Firewall Services.
4. Two (2) Sandbox Capability (Standalone appliance only).
5. Two (2) Anti-DDoS Capability (Standalone appliance only).
6. Cloud-Based or On Premise (Four (4) Web Application Firewall Services for 60 000 users.
7. Manager and Reporter for central management, logging and reporting.
8. Licenses for sixty (60) months.
9. Professional services and premium support and maintenance on the technology deployed, including upgrades for sixty (60) months.
10. Partner support and maintenance, including the following resources for the support and maintenance of the NGFW infrastructure for sixty (60) months:

(1). One (1) full-time certified security engineer

(2). One (1) certified security architect - required bi-monthly - i.e. not dedicated to the SAPS environment but available twice a month as required in the specification.

1. Training and Certification of the SITA / SAPS resources working in this environment, as required in the specification document for sixty (60) months.

(1). Six (6) Introduction level certification and examination.

(2). Two (2) Expert level certification and examination.

1. The NGFW technology will be managed by SITA according to the SLA with the SAPS. All data will be stored and managed within the SAPS environment.
2. The vendor in conjunction with SITA will be responsible for the deployment, upgrades and maintenance of the technology

## 2.2 Delivery address

The goods or services must be supplied or provided at the following physical addresses:

Table 1: Delivery address

|  |  |
| --- | --- |
| **No** | **Physical Address** |
| 1 | Pretoria and Regions |

## Customer Infrastructure and Environment Requirements

### 2.3.1 Customer methods, standards and policy environment

1. The controls to be identified shall be in line with:
   1. MISS - Minimum Information Security Specification
   2. ISF – Information Security Forum’s IRAM Methodology
   3. ISF – Information Security Forum’s Standard of Good Practice
   4. ISO 27001/2 Information Security Standard
   5. Cobit – Information Technology Framework
   6. NIST - National Institute of Standards and Technology
   7. CIS - Center for Internet Security

## Technology Requirements

The supply and deployment of the SAPS NGFWs, along with all associated security features/technologies, must meet the specified minimum requirements. ***Furthermore, the technology must be designed to support the full five-year contract period, including growth***. The current internet bandwidth is 1 Gbps.

### Appliance Base Firewalls

1. **Enterprise Firewall Service**

|  |  |
| --- | --- |
| **Product** | **Quantity** |
| Next-Generation Firewall Technology Appliance (Pretoria only) | 4 |

|  |  |
| --- | --- |
| **Performance** | **Minimum Requirement** |
| Threat Prevention/Protection  AV Enabled  IPS Enabled  APP Control Enabled  URL Filtering Enabled | 20 (Gbps) |
| NGFW Throughput  App Control Enabled  IPS Enabled | 75 (Gbps) |
| VPN Throughput | 80 (Gbps) |
| Connections per second | 1M |
| Concurrent sessions | 50M |
| **Network** |  |
| 10 /100/ 1000 Base-T (Ports) | 8 |
| 10GBase-F SFP+ (Ports) | 12 |
| **Additional Features** |  |
| Enclosure | 1RU |
| Storage | 500GB minimum – sufficient storage to be provisioned for the contracted period |
| Dual, Hot-Swappable Power Supplies | Yes |

1. **Regional Firewall Service**

|  |  |
| --- | --- |
| **Product** | **Quantity** |
| Next-Generation Firewall Technology Appliance (Regions) | 20 |

|  |  |
| --- | --- |
| **Performance** | **Minimum Requirement** |

|  |  |
| --- | --- |
| Threat Prevention/Protection | 10 (Gbps) |
| NGFW Throughput | 20 (Gbps) |
| IPS Throughput | 20 (Gbps) |
| Firewall | 40 (Gbps) |
| Firewall Throughput | 60 (Gbps) |
| Connections per second | 330K |
| Concurrent sessions | 20M |
| **Network** |  |
| 10 /100/ 1000 Base-T (Ports) | 12 |
| 10GBase-F SFP+ (Ports) | 6 |
| **Additional Features** |  |
| Enclosure | 1RU |
| Storage | 500GB minimum – sufficient storage to be provisioned for the contracted period |
| Dual, Hot-Swappable Power Supplies | Yes |

* + 1. **Integrate with traditional firewall functionality such as packet filtering, address translation (NAT),** stateful inspection and Virtual Private Networking (VPN) with next-generation functionality.
    2. **Mobile SSL Access Termination**

The NGFW technology must provide a Mobile SSL Access solution to provide safe and easy connectivity to corporate applications over the internet with Smartphones, tablets, or PCs. The technology must also provide enterprise-grade remote access via both Layer-3 VPN and SSL VPN, allowing simple, safe, and secure connectivity to your email, calendar, contacts, and corporate applications.

* + 1. **Clustering**

The NGFW technology must be able to provide high-end enterprise and data centre environments where performance and availability are critical. Gateways will be clustered for business continuity and/or resource sharing.

* + 1. **Additional Requirements**
    2. Outbound IPSEC and SSL encryption facilities.
    3. Port trunking functionality.
    4. Port Aggregation functionality.
    5. Detect non-standard port hopping therefore not assuming standard port assigned utilisation.
    6. Agent-based monitoring with support for customised alert generation
    7. Identify all users, systems and applications regardless of the port or protocol used.
    8. Protect against unauthorised access to systems, applications and network infrastructure
    9. Provide real-time protection against threats occurring on all layers including the application layer.
    10. Protect against data leakage.
    11. Protect against website hack attacks and defacements.
    12. Integrate with traditional firewall functionality such as packet filtering, address translation (NAT), stateful inspection and Virtual Private Networking (VPN) with next-generation functionality.
    13. Provide high performance such as gigabit in-line throughput without service degradation.
    14. **Remote VPN access:**

1. The NGFW technology must offer effective Virtual Private Network (VPN) access functionality, fully integrable with multifactor authentication to Active Directory:

1) Allow a secure VPN setup to provide remote access capability for users.

2) Allowing users to connect with any device, tablet smartphone and laptop from any remote location.

3) Allow unlimited IPSec and SSL functionality

* + 1. **Network integration:**
* The NGFW technology must provide effective:

1) VLAN support.

2) IPv6 Support.

3) Dynamic Host Configuration Protocol (DHCP) relay.

4) Routing protocols (Routing Information Protocol [RIP], OSPFv3).

5) Exterior Gateway Routing Protocols (BGP).

6) Support for Layer 2 (transparent) mode.

7) Multilink/multi-ISP connectivity.

* + 1. **Encryption:**

1. The NGFW technology must be able to:

1) Provide client-to-site SSL, TLS or DTLS VPN.

2) Provide client-to-site IPsec VPN.

3) Provide certificate-based VPN user identity recognition.

4) Support username- and password-based VPN user identity recognition.

5) Provide Site-to-site IPsec VPN.

6) Enforce and Support Strong encryption.

7) Provide VPN client load balancing and clustering.

* + 1. **Visibility into encrypted packets:**

1. The NGFW technology must be able to decrypt the traffic to inspect the content; else such traffic should be diverted to a secure area with applicable notifications raised to the OSIS team.
   * 1. **Stability and reliability:**
2. The NGFW technology must provide stability and reliability.

1) It is critical that the firewalls deployed can manage the traffic with regard to speed and bandwidth. From a growth perspective, it is important to bring scalability into the calculation and to ensure that the device(s) will be able to manage the traffic for the next five years.

* + 1. **Load balancing:**

1. The technology should be able to provide load-sharing high availability (active/active, active/standby) to ensure optimum service uptime and service delivery.
   * 1. **High availability:**
2. The technology should be able to provide high availability (active/active, active/standby) to ensure optimum service uptime and service delivery:

1) High availability and load-balanced proxy functionality for both forward and reverse proxy configurations with support for SSL termination and SSL streaming interrogation by the IPS.

2) High availability (active/active, active/standby).

3) Redundancy in physical appliances.

4) Out-of-band management.

5) Hot swap of components in physical appliances.

### Manager and Reporter

* + 1. Automatically adapt to the threat landscape without any user intervention and should be able to follow up manually on thousands of security advisories and recommendations.
    2. Integrate seamlessly into the SAPS environment and the technology will require providing a defensive posture that collaboratively leverages both internal and external intelligent sources.
    3. Needs to make filter decisions based on specific business rules, assets, users, roles and applications as well as define security policies for the set of authorised interactions between the same asset, users and applications (e.g. access control would determine whether a user is allowed to access sensitive government data or services and could qualify authorization base on the user’s location, host status, time of the day.)
    4. Correlates findings from multiple engines, signatures, reputation, behaviour, malware emulation and human validation to gain a higher level of confidence. In addition, the technology should leverage extensive and reliable internal and external threat sources to generate meaningful and actionable security intelligence (i.e. threat indicators that can be used to detect and prevent threats).
    5. **Identity Awareness**

The NGFW technology must provide granular visibility of users, groups and machines, providing application and access control through the creation of accurate, identity-based policies. Identity Awareness seamlessly integrates with Active Directory (AD) with multiple deployment options and third-party two-factor authentication solutions.

* + 1. **Audit Logging**

1. Administrator audits.
2. Reporting engine.
3. Standard reports.
4. Alerts.
5. SIEM integration.
6. Export of log information.
7. NetFlow statistics.
8. Action if the firewall cannot log events.
9. Reliable logging; and
10. Use of threat intelligence in reports.
    * 1. **Centralised Management:**
11. The NGFW technology must be able to be deployed to various peering points and report to one centralised console.
12. The NGFW technology must complement the ability to collate all different plug-ins thereby providing a unified threat management (UTM) concept. Features must, therefore, provide combined IPS/IDS, firewall and filtering methods at one location.
13. The NGFW technology must be provided.

1) Object-based configuration.

2) Change then commits.

3) Rule verification mechanism.

4) Reason/tracking of rule changes.

5) AD/LDAP integration.

6) Rule change rollback.

7) Unified three-tier management of VPNs.

8) Rule usage statistics.

9) Hierarchical management roles.

10) Lateral management roles.

11) Threat intelligence feeds.

12) Workflow and automation.

13) Simultaneous changes.

14) Rule reduction/simplification mechanism.

15) Traffic profile verification.

* + 1. **Firewall ruleset:**

1. The NGFW technology must provide the capability to implement the following ruleset:

1) Stateful inspection functionality inspection for traffic on layers 3 and 4 to allow or block traffic.

2) Anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside).

3) User permit rules (e.g. allow HTTP/S to public webserver).

4) Management permit rules (e.g. SNMP traps to network management server).

5) Noise drops (e.g. discard OSPF and HSRP chatter).

6) Deny and Alert (alert systems administrator about traffic that is suspicious).

7) Deny and log (log remaining traffic for analysis).

4) SSL Inspection.

* + 1. **User identification:**

1. The NGFW technology must:

1) Identify all users on the network with integration with Active Directory (AD) and LDAP services.

2) Link the user with an IP address and login activity locally on the LAN, VPN or any other form of network access.

3) Be able to provide security policy enforcement against all users (legal users and illegal users, permanent, contractors, visitors, and consultants) on the SAPS network and connected remote VPNs.

4) Identify and track user activity enabling the building of user profiles and tracking anomalies associated with the profiles.

5) Identify privileged users and sensitive data, and access monitoring.

6) Show a user's threat trend or risk profile of the user.

7) Provide login activity and provide monitoring.

* + 1. **Firewall policy management:**

1. The NGFW technology must have the capability to create policy-based controls utilising application identification, user identification and content identification.
   * 1. **Reporting:**
2. The bidder and the NGFW technology must provide practical extraction and reporting language functionality.
   * 1. **Provide a granular level of reporting for:**
   1. Administrators.
   2. Management.
   3. Executives.
      1. **Bandwidth control:**

The NGFW technology must allow granular level bandwidth control, and control the bandwidth for specific users, environment and function.

* + 1. **Reporter to manage and provide all reporting functionality.**

### Sandboxing Capability (standalone appliance only)

|  |  |
| --- | --- |
| **Product** | **Quantity** |
| Sandbox device | 2 |

|  |  |
| --- | --- |
| **Specification** | **Minimum Requirement** |

|  |  |
| --- | --- |
| Hardware | Standard rack-mounted 2U appliance |
| Interfaces | 4 x GE electrical ports, 2 x 10GE optical ports |
| Hybrid traffic performance indicator in traffic restoration | 2 Gbit/s (bidirectional traffic of a 1 Gbit/s link) |
| HTTP performance indicator | 1.2 Gbit/s |
| FTP performance indicator | 300 Mbit/s |
| Email protocol performance indicator | 500 Mbit/s |
| PDF file inspection performance | 100000 files/day |
| (file size: 1 MB) |
| Office file inspection performance | 200000 files/day |
| (file size: 1 MB) |
| Script file inspection performance | 120000 files/day |
| (file size: 10KB) |
| Maximum number of interworking devices supported by a cluster manager | 256 |
| SWF file detection | Support obfuscated code and malformed data detection |
| Script file detection | Support trojan, backdoor, worm, virus detection |
| PE file inspection | Support trojan, backdoor, worm, virus detection |
| PDF file inspection | Support shellcode, file format vulnerability detection |
| Web file inspection | Support static flash, shellcode, script trojan detection |
| Office file inspection | Support file format vulnerability, shellcode detection |
| Support file blacklist & whitelist | Yes |

* + 1. Support segmentation as part of the threat containment, to ensure that a successful attack on one part of the environment doesn’t compromise the entire environment.
    2. Ability to constrain the system to normal behaviour thus able to block malware even if it’s successfully subverted system component (e.g. an unidentified host that is performing an abnormal network scan can be restricted using containment control).
    3. Support sandboxing technique, which allows documents and applications to be executed in a contained environment that emulates the target system to analyse detect and prevent any unexpected behaviour.
    4. The NGFW technology must provide a capability to quarantine suspected malicious content to be investigated and cleaned before the file and access are released to the network.
    5. The sandboxing technology must inspect the unknown devices and access them.

### Cloud-Based or On Premise (Four (4)) Web Application Firewall .

|  |  |
| --- | --- |
| **Product** | **Quantity** |
| Web Application Firewall | 4 appliances / 60 000 users |

|  |  |
| --- | --- |
| **Hardware Specification** | **Minimum Requirement** |
| 10 /100/ 1000 Base-T (Ports) | 6 |
| 10GBase-F SFP+ (Ports) | 6 |
| Management | 10 /100/ 1000 Base-T |
| Serial Port | 1 RJ |
| Rack | 2U |
| Dual Power Supply | Yes |
| Hard Disc (SSD storage) | 500GB minimum – sufficient storage to be provisioned for the contracted period |
| Throughput | 8 GB |
| Delay in processing | Less than 60µs |
| Application Layer Throughput | 6 GB |
| HTTP transaction / s | 100,000 TPS |
| HTTP connection / s | 38, 000 CPS |

1. **URL Filtering**

The technology must provide secure reverse proxy services to deployed public websites and SAPS systems. The technology must provide optimised web security through full integration in the gateway to prevent bypass through external proxies. Integration of policy enforcement with Application control.

1. **Application Control**

The technology must provide strong application security and identity control to organisations of all sizes. It must allow IT teams to easily create granular policies - based on users or groups - to identify, block or limit usage of Web 2.0 applications and widgets.

1. **Traffic inspection:**

* The technology must provide:

1) Passive network traffic capturing functionality.

2) Analyses and inspect traffic including all encrypted traffic such as SSH or TLS/SSL with no assumptions that such traffic is legitimate.

3) Conduct deep packet inspection.

1. **Application identification:**
2. The technology must provide dynamic application control and protection:

1) Identify and protect known and unknown applications from known and unknown sources.

2) Inspect application content.

3) Protect all Web-based Applications from cyber application attacks.

4) Inspect encrypted application traffic following through VPN IPsec tunnels using HTTPS protocols.

5) Having the capability of examining various codes such as EBCDIC, Binary, ASCII and Unicode must be considered for the device evaluation.

6) Identify all users on the network with integration with Active Directory (AD) and LDAP services.

7) Identify applications within the HTTP/S protocol (browser-based applications).

8) Enforce policy on individual users and users’ groups.

9) Enforce Bandwidth usage.

10) Provide application control support for encapsulated traffic.

11) Provide application control support of 4 over 6 and 6 over 4 tunnels.

12) Provide support for the application information feed.

13) Provide user-developed application signatures.

14) Provide application whitelist/blacklist.

15) Filter URLs.

16) IPv6 support for application control.

17) Identify applications within the SSL protocol.

18) Block the upload of data even when allowing access to the site.

1. **Application and content filtering:**
2. The technology must examine embedded content ensuring alignment with respect to application and packet content must be possible with the level of device intensity.
3. **Internet security:**
   1. URL filtering to classify content and block unwanted sites.
   2. Whitelisting and blacklisting of websites.
   3. Conduct object inspection.
   4. Content filtering with blacklist customisation and the ability to download and update blacklists via synchronisation for a centralised source.
4. **Predict the likelihood of unknown threats from IP, URL, application, and mobile. The technology must be able to protect all services against web/internet-based attacks including:**
   1. Blind SQL Injection.
   2. Cross Site Scripting.
   3. Script Source Code Disclosure.
   4. Expression Language Injection.
   5. HTTP Parameter Pollution.
   6. Application error message.
   7. Directory Listing.
   8. Error message on page.
   9. Login page password-guessing attack.
   10. Possible sensitive directories.
   11. Possible sensitive files.
   12. Session Cookie without Secure flag set.

### Threat Control and Network Threat Protection

* + 1. Enable comprehensive visibility that allows SITA to “fight through” attacks while maintaining acceptable levels of service by detecting, containing and repelling cyber-attacks, as well as supporting follow-up investigation and recovery and collaboration.
    2. The NGFW technology must reduce security breaches by guarding the SAPS information systems:

1. Minimising the likelihood of any potential information security breaches being exploited by malicious individuals, applications or systems in production.
2. Reducing time, effort and expenditure involved with pro-active identification of information security threats.
3. Providing real-time information security protection service.
4. Improving the quality of information security, and vulnerability management in SITA and the South African government.
5. Addressing all internal and external audit findings.
6. Ensuring compliance with SAPS and government information security policies, standards, processes and procedures.
7. Ensure compliance with legislative and regulatory requirements such as POPI, ECT Act, PAIA, RICA, etc.
   * 1. Anti-virus and malicious code:

The NGFW technology must provide antivirus, malicious code and spyware protection to effectively protect against malicious threats entering and exiting the SAPS environment.

* + 1. Evasion attacks:

1. The NGFW technology must provide effective protection against evasion attacks.
2. The NGFW technology must protect evasion techniques such as RPC fragmentation, FTP evasion TCP stream segmentation. IP fragmentation, HTML evasion and URL obfuscation.
   * 1. Advanced persistent attacks:

(i) The NGFW technology must protect against.

1) Advanced Persistent attacks.

2) Targeted Attacks.

* + 1. Botnets and DLP:

1. The NGFW technology must protect against.

1) Botnets.

2) Data leakage through the gateway.

3) Information Theft through the gateway.

4) Web attacks such as website defacements and website hacking.

5) Phishing attacks.

* + 1. Advanced/Intelligent threat management:

1. The bidder and the NGFW technology must be able to.

1) Provide continuous real-time advanced and intelligent threat scanning and management.

2) Predict the likelihood of an unknown threat from IP, URL, application, mobile device or user such as a malicious attack.

4) Update risk as the threat landscape evolves.

5) Protect by blocking or deleting threats against the possibility of threat that may lead to an exploit.

6) Provide in-depth defence.

### Intrusion Prevention System Capability

The NGFW technology must provide IPS protection with breakthrough performance and complete and proactive intrusion prevention—all with the deployment and management advantages of a unified and extensible next-generation firewall technology.

* 1. Provide effective Intrusion Prevention Service (IPS) protecting against vulnerability attacks including, deep packet scanning, traffic normalisation and defragmentation using mechanisms such as protocol anomalies, behaviour anomalies and heuristic detection mechanisms.
  2. Include signature-based IPS.
  3. Ability to modify existing IPS signatures.
  4. Monitor, identify and block Malicious activities and attacks.
  5. Provide multi-threaded multi-queuing IPS.
  6. DoS and DDOS protection.
  7. Stateful inspection and IPS support for encapsulated traffic.
  8. Stateful inspection and IPS support of 4 over 6 and 6 over 4 tunnels.
  9. User-developed signatures for IPS.
  10. Use AD or LDAP for context.
  11. Built-in decryption capability.
  12. Detect and prevent intrusions.

### Anti-DDoS capability (standalone appliance only)

|  |  |
| --- | --- |
| **Product** | **Quantity** |
| Anti-DDoS | 2 |

|  |  |
| --- | --- |
| **Hardware Specification** | **Minimum Requirements** |
| 10 /100/ 1000 Base-T (Ports) | 6 |
| 10GBase-F SFP+ (Ports) | 6 |
| Management | 10 /100/ 1000 Base-T |
| Serial Port | 1 RJ |
| Rack | 2U |
| Dual Power Supply | Yes |
| Hard Disc (SSD storage) | 500GB minimum – sufficient storage to be provisioned for the contracted period. |
| Throughput | 8 GB |
| Delay in processing | Less than 60µs |
| Application Layer Throughput | 6 GB |

1. Anti-DDoS attacks:
2. The technology must protect against.

1) Dynamic Denial of Service Attacks.

2) Should anticipate where and when denial of service attacks will be launched and guard against it.

3) Have the capability to know where advanced malware will be downloaded from.

4) Real-Time Traffic Monitoring: Ability to monitor and analyse traffic patterns continuously to identify and mitigate threats early.

5) Scalability: The technology must handle traffic surges of varying magnitudes, accommodating future growth in legitimate traffic and larger attack sizes.

6) Automated Response: Automation ensures rapid detection and mitigation without requiring manual intervention, minimizing downtime.

7) Layered Defense Capabilities: Protects against different attack types, including volumetric, application-layer, and protocol-based attacks.

8) Integration with Existing Infrastructure: Compatibility with the organisation’s current network architecture and security tools is essential.

9) Low Latency: The technology should not negatively impact legitimate traffic or degrade user experience.

10) Customizable Policies: Ability to tailor protection rules and thresholds to specific organisational needs.

11) Reporting and Analytics: Detailed insights into attack trends, mitigation activities, and system performance to support strategic decisions.

12) Vendor Support and SLA: Comprehensive support services and a clear service-level agreement (SLA) to ensure reliability.

## Functional requirements

## Lifecycle Management

The product lifecycle management must align with SAPS requirements, ensuring a minimum of 5 years of support and maintenance entitlement for the department. This includes the lifecycle of appliances, accessories, software, and operating system support. Throughout the contract period, the product must remain fully supported and maintained.

## Skills Transfer and Training

* 1. Comprehensive formal training, including examinations and certification, must be provided for six SAPS/SITA specialists.
  2. Training must be conducted for six SAPS/SITA personnel with each system upgrade.
  3. In addition, the Service Provider is required to offer continuous, hands-on training to ensure sustained skill development.

# Bid Evaluation Stages

* + - 1. The bid evaluation process consists of several stages, according to the nature of the bid as defined in the Table below.
      2. A bidder must qualify for each stage to be eligible to proceed to the next stage of the evaluation.

The stages are:

Table 2: Bid Evaluation Stages

|  |  |  |
| --- | --- | --- |
| **Stage** | **Description** | **Applicable for this bid YES/NO** |
| Stage 1 | Mandatory Administrative Responsiveness | YES |
| Stage 2 | Technical Mandatory Requirements | YES |
| Stage 3 | Special Conditions of Contract Verification | YES |
| Stage 4 | Price and Preference Points Evaluation | YES |

## 3.1 Mandatory Administrative Responsiveness (Stage 1)

### 3.1.1 Attendance of briefing session

1. A **Compulsory Virtual briefing session** will be held. The bidder has to sign the briefing session attendance register using the same information (bidder company name, bidder representative person name and contact details) as submitted in the bidder’s response document. Any bidder who fails to attend the compulsory briefing session will be disqualified.
2. In the case of joint ventures or consortiums the bidder must demonstrate that at least one of the parties to the bid response attended the briefing session

### 3.1.2 Registered Supplier

1. Only responses from bidders who are registered as a Supplier on National Treasury’s Central Supplier Database (CSD) in terms of National Treasury’s Instruction Note 4A of 2016/17 will be considered for award on this **RFB**.
2. Bidders need to complete all the SBD documents which needs to be submitted as stated in the Invitation to Bid Document.

### 3.1.3 Bid Submission Instructions

**Note that a Two Envelope process will be followed and therefore bidders must submit as follows:**

1. **Envelope 1: RFB Document and Technical / Functionality Response**

The following must be included and submitted in a in a separate envelope:

* 1. One (1) original file excluding pricing; **and**
  2. One (1) hard copy excluding pricing; **and**
  3. One (1) electronic copy on USB memory stick/ flash drive in Portable Document Format (PDF) of the RFP Document and Technical / Functionality Response.

1. **Envelope 2: Price Response**

The following must be included and submitted in a in a separate envelope:

* 1. One (1) original file excluding Technical / Functionality Response; and
  2. One (1) hard copy excluding Technical / Functionality Response; and
  3. One (1) electronic copy on USB memory stick/ flash drive in Portable Document Format (PDF) of pricing only.

1. **It is the Bidder’s responsibility to ensure that the information and contents on the electronic copies is the same as in the hard copies.**
2. To ensure that the electronic copies are not damaged, the bidder must submit the USB’s (memory stick/ flash drive) in a sealed padded envelope and be clearly marked.
3. Bidders shall submit Bid responses in accordance with the prescribed manner of submission as specified above. Failure to comply with the above instructions on submitting a proposal will lead to disqualification.
4. The RFB Responses (hard and electronic copies) must be clearly marked as follows: Bidder’s Name & Contact Details, RFB Number, RFB Description, and Closing Date.
5. All Bids in this regard shall only be accepted if they have been placed in the tender box before or on the closing date and stipulated time.
6. Late bids shall not be considered.
7. The Bid response must be signed by an authorised employee, agent or representative of the bidder. The Bid response Bid must bear the initials of the signatory at the bottom of every page as an indication that the bidder has familiarised itself with the terms and conditions of this RFB document.
8. Faxed or e-mailed bids will not be accepted.
9. Bidders shall submit Bid responses in accordance with the prescribed manner of submission as specified in this document. Failure to comply with the bid submission requirements will lead to disqualification.
10. Bidders are required to submit all returnable documents/information together with their Bids/proposals on or before the closing time and date of the Bids/proposals.
11. All services supplied in accordance with the bidder’s proposal must be in accordance with all applicable legal requirements in terms of South African law, policies and regulations.

## 3.2 Technical returnable documents

### 3.2.1 Instruction and evaluation criteria

1. The bidder must comply with ALL the requirements as per the Technical Mandatory Requirements below by providing substantiating evidence in the form of documentation or information, failing which it will be regarded as “NOT COMPLY”.
2. The bidder must provide a unique reference number (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response.
3. The bidder must comply with ALL the TECHNICAL MANDATORY REQUIREMENTS in order for the bid response to proceed to the next stage of the evaluation.

### 3.2.2 Technical mandatory requirements (Stage 2)

Table 3: Technical Mandatory Requirements

| **Mandatory Requirements** | **Substantiating evidence of compliance (used to evaluate bid)** | **Evidence reference (to be completed by bidder)** |
| --- | --- | --- |
| * + - 1. **Bidder Certification/ Affiliation Requirements** | | |
| The Bidder must be an Original Equipment Manufacturer (OEM), or Original Software Manufacturer (OSM), or an accredited OEM/OSM reseller, partner, or distributor to provide, deliver, install, configure, support, and maintain a NGFW technology. | Attach to **ANNEX A**, a copy of a valid documentation (certificate, letter, or license) as proof that the bidder is the OEM/OSM, or an accredited OEM/OSM reseller, partner or distributor to provide, deliver, install, configure, support, and maintain a NGFW technology.  **NOTE (1):**  The valid documentation (letter/certificate/license) clearly indicating the following information below:  (a) The Regulator Name (OSM/OEM); and  (b) The Bidder’s Name; and  (c) The date it was issued; and  (d) if applicable, the expiry date  **NOTE (2):**  SITA reserves the right to verify information provided.  **NOTE (3):**  Original Equipment Manufacturers (OEM)/Original Software Manufacturers (OSM) using Partner/ Reseller/Distributor model are not eligible to participate for this bid. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, par 4.1**> |
| * + - 1. **Bidder Experience and Capability Requirements** | | |
| The Bidder **must** have provided, delivered, installed, configured, supported and maintained NGFW technologies to at least two (02) customers during the past five (05) years from the publication of this bid. | The Bidder **must** provide reference details from at least two (02) customers to whom the NGFW technologies were provided delivered, installed, configured, supported and maintained in the past five (05) years from the publication of this bid:  **NOTE (1):**  The Bidder must provide **all of the following** information when completing **table 9**:   * 1. Company name; **and**   2. Reference Person Name, Tel **and/or** email; **and**   3. Project Scope of Work; **and**   4. Project Start and End-date.   **Note (1):**  Failure to complete **Table 9** fully as indicated above will result in disqualification.  **Note (2):**  SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, par 4.2, table 9**> |
| * + - 1. **Special Conditions of Contract Acceptance** | | |
| The Bidder must accept the following:  All the Special Conditions of Contract (SCC) as stated in **section 3.3**. | The Bidder **must accept ALL** the Special Conditions of Contract (SCC) by completing and signing the declaration of Acceptance in the Declaration of Compliance and Acceptance under the Special Conditions (**Section 3.3.2)**  **NOTE (1):**  Failure to complete and sign the SCC in **section 3.3.2** will result in disqualification. | <provide unique reference to locate substantiating evidence in the bid response – **see ANNEX A, par 4.3>** |
| * + - 1. **Third Party Risk Assessment** | | |
| The Bidder must confirm compliance with Third-Party Risk Management Assessment. | The Bidder must comply with the Third-Party Risk Management Assessment requirement by completing All the questions in **Annex B.**  **Note (1):**  SITA reserves the right to verify information provided.  **Note (2):**  Failing to complete all the questions or not Accepting the Declaration of Acceptance above will result in disqualification. | <Provide unique reference to locate substantiating evidence in the bid response – see **Annex A, par 4.4 and Annex B**> |
| * + - 1. **Product Functional Requirements** | | |
| **The Bidder must confirm compliance with the Product/Service Functional requirements.** | The Bidder must confirm that they comply with the **Product/Service Functional Requirements** by completing **Annex C: Addendum 1**.  **NOTE (1):**  Failure to comply fully to the requirements as indicated above will result in disqualification.  **NOTE (2):**  SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, paragraph 4.5 and Annex C: Addendum 1>** |

## 3.3 Special Conditions of Contract Verification (Stage 3)

1. The successful supplier will be bound by Government Procurement: General Conditions of Contract (GCC) as well as this Special Conditions of Contract (SCC), which will form part of the signed contract with the successful Supplier. However, SITA reserves the right to include or waive the condition in the signed contract.
2. SITA reserves the right to:
   1. Negotiate the conditions; or
   2. Automatically disqualify a bidder for not accepting these conditions; or
   3. Award to multiple bidders; or
   4. Not to award; or
   5. To do a partial award.
3. In the event that the bidder qualifies the proposal with own conditions and does not specifically withdraw such own conditions when called upon to do so, SITA will invoke the rights reserved in accordance with subsection 4.3. (b) above.

### 3.3.1 Special Conditions of Contract

#### 3.3.1.1 Contracting Conditions

1. **Formal Contract** - The supplier must enter into a formal written contract (agreement) with SITA.
2. **Right to Audit** - SITA reserves the right, before entering into a contract, to conduct or commission an external service provider to conduct a financial audit or probity to ascertain whether a qualifying bidder has the financial wherewithal or technical capability to provide the goods and services as required by this tender.

#### 3.3.1.2 Delivery Address

1. The supplier must deliver the required products or services at as indicated in Section 2.2, Delivery Address.

#### 3.3.1.3 Supplier performance reporting

1. Monthly meetings to be scheduled between SITA and service provider and ADHOC meetings from both sides.
2. A formal report must be submitted to the SITA representative after every service, maintenance, or repair; including the relevant job sign-off sheets signed by SITA and the service provider.

#### 3.3.1.4 Services and Performance Metrics

1. The bidder is responsible to provide the following services as specified in the Service Breakdown Structure (SBS):

Table 4: Service Element

| **SBS** | **Statement of Work** | **Service Level** |
| --- | --- | --- |
|  | Call Centre | 24h x 7days x 52weeks |
|  | Incident Response | Maximum 1 hour |
|  | Incident Restore | Maximum 4 hours |
|  | Availability | 24/7/365 - 99% Availability |
|  | Enterprise Next Generation Firewall Appliances | **Initial and Replacement (Failure)** |
|  | Regional Next Generation Firewall Appliances | **Initial and Replacement (Failure)** |
|  | Sandbox Standalone Appliances | **Initial and Replacement (Failure)** |
|  | Anti-DDoS Capability Standalone Appliances | **Initial and Replacement (Failure)** |
|  | On Premise or Cloud-Based Web Application Firewall Services | **Initial and Replacement (Failure)** |
|  | Manager and Reporter for central management logging and reporting | **5 Years (Five Years)** |
|  | All Licensing | **5 Years (Five Years)** |
|  | Professional services and premium support and maintenance on the technology deployed, including upgrades | **5 Years (Five Years)** |
|  | Hardware Provision, Installation, Configuration and support including;   * Implementation plan, * Final design documentation, * Hardware installation, * Configuration | **Once-off** |
|  | Partner Support and Maintenance   * + - 1. One (1) full-time certified junior security engineer       2. One (1) certified senior security architect - required bi-monthly - i.e. not dedicated to the SAPS environment but available twice a month as required in the specification. | **5 Years (Five Years)** |
|  | Certification Training   * + - 1. Six (6) Introduction level certification and examination.       2. Two (2) Expert-level certification and examination. | **5 Years (Five Years)** |

#### 3.3.1.5 Certification, Expertise and Qualification

The bidder certifies that:

* 1. it has the necessary expertise, skill, qualifications and ability to undertake the work required in terms of the Statement of Work or Service Definition;
  2. it is committed to provide the Products or Services;
  3. perform all obligations detailed herein without any interruption to the Customer; and
  4. it has been certified for the Products and Services required.

The bidder must provide the service in a good and workmanlike manner and in accordance with the practices and high professional standards used in well-managed operations;

1. The bidder must perform the Services in the most cost-effective manner consistent with the level of quality and performance as defined in Statement of Work or Service Definition; and
2. Original Equipment Manufacturer (OEM) or Original Software Manufacturer (OSM) work. The Supplier must ensure that work or service is performed by a person who is certified by Original Equipment Manufacturer or Original Software Manufacturer.
3. The bidder is required to provide qualified technical resources with demonstrable experience and appropriate certifications relevant to the deployment, configuration, and ongoing support of the proposed NGFW technology. The following minimum criteria must be met:
   1. Certified Expertise
      1. The bidder must allocate at least two (2) technical resources who each hold a valid and current certification specific to the OEM NGFW technology being proposed.
      2. Certifications must be issued directly by the OEM or an officially authorised certification body.
   2. Relevant Experience
      1. Each proposed technical resource must have a minimum of three (3) years of hands-on experience in the planning, implementation, configuration, and maintenance of enterprise-grade NGFW solutions.
      2. Experience must be clearly detailed in the CVs of the proposed resources, including roles and responsibilities.
   3. Project Involvement
      1. The bidder must demonstrate that the proposed technical resources have played a key technical role in at least two (2) NGFW-related projects within the last five (5) years.
      2. Each project reference must include:
         * Client name.
         * Project scope and objectives.

#### 3.3.1.6 Ongoing Training and Certification Maintenance

1. To ensure ongoing technical competence and relevance throughout the duration of the contract, the following training and certification requirements shall apply:
2. All technical resources assigned to the project must have received certified training from the OEM (or an OEM-accredited training provider) for the proposed NGFW technology within the first six (6) months of the contract period.
3. The bidder must commit to ensuring that these resources maintain up-to-date certifications and receive ongoing training for the full five (5) year contract period, especially in the event of:

* Major version upgrades
* Feature enhancements
* Security or architecture changes introduced by the OEM

1. The bidder shall be responsible for the costs and logistics associated with such training to keep resources aligned with the latest standards and product updates.
2. Proof of training completion and certification renewal must be made available to the client upon request and may be subject to periodic audit.

#### 3.3.1.7 Logistical Conditions

1. **Hours of Work**
   1. Office hours are defined as business working hours of the customer and is Mondays to Fridays between 07:30 and 16:00.
   2. After hours of the customer during week days are from 16:00 to 07:30. It also includes Saturdays, Sundays and Public Holidays.
   3. All mission critical sites will be managed on a 24 x 7 x 365 basis.
2. **Client environment**
   1. In the event that SITA grants the bidder access to SITA's and Client’s Environment including hardware, software, internet facilities, data, telecommunication facilities and/or network facilities remotely, the Supplier must adhere to SITA's relevant policies and procedures (which policy and procedures are available to the Supplier on request) or in the absence of such policy and procedures, in terms of, best industry practice.
3. **Tools of Trade**
   1. The bidder is expected to use its own resources (cell phone, laptops etc) to communicate with its own offices or outside of the SITA/Client buildings, including all tools and equipment to render the services effectively.

#### 3.3.1.8 Regulatory, Quality and Standards

* 1. The Supplier must for the duration of the contract ensure compliance with ISO/IEC General Quality Standards, ISO27001, and Protection of Personal Information Act (POPIA).
  2. The Supplier must for the duration of the contract ensure compliance with General Quality Standards, ISO 9001.

#### 3.3.1.9 Company and Personnel Security clearance requirements

(a) **Company security screening:** The supplier may be required to undergo a company security screening conducted by the State Security Agency (SSA). Should the SSA find the supplier **not** **suitable** after the conduct of the security screening, the business relationship will be terminated. The following documentation will be required for the company security screening process to be conducted:

(i) Copy of company registration documentation;

(ii) Copy(ies) of identity documentation of Director(s), Member(s) or Trustee(s);

(iii) Copy of valid tax clearance certificate.

(b) **Security suitability checks for individuals:** SITA may, at its own discretion and in line with its policies and procedures, require employees of the supplier to be subjected to a security suitability check before commencement of a project or delivering of a service. The security suitability check is conducted by SITA in order to ensure that individuals meet the minimum-security requirements and also to verify personal information. The supplier will be required to replace any employee(s) who is found to be not suitable after the conduct of the security screening. The following documentation will be required for the security suitability check:

(i) Copy of identity document;

(ii) Copy(ies) of qualification(s) if SITA requires verification thereof;

(iii) Fingerprints – will be taken electronically;

(iv) Signed consent form for the conduct of background checks.

(c) **Security clearance:** A security clearance, issued by either the SSA or Defence Intelligence (DI) is required if any employee of the supplier will have or may gain access to classified information throughout the duration of the project or in the process of delivering a service. The level of security clearance required – **Confidential**, **Secret** or **Top Secret**, will be determined at the sole discretion of SITA. The supplier will have to replace any employee who do not qualify for a security clearance or is found not suitable by the SSA or DI. The following documentation will be required for the security clearance process:

(i) Completed **Z204** or **DD1057** security clearance application form;

(ii) Fingerprints;

(iii) Personal documentation of the applicant, including but not limited to, identity document, passport, marriage certificate (if applicable), divorce order (if applicable), qualifications, salary advice and bank statements.

#### 3.3.1.10 Confidentiality and non -disclosure conditions

1. The Supplier, including its management and staff, must before commencement of the Contract, sign a non-disclosure agreement regarding Confidential Information
2. Confidential Information means any information or data, irrespective of the form or medium in which it may be stored, which is not in the public domain and which becomes available or accessible to a Party as a consequence of this Contract, including information or data which is prohibited from disclosure by virtue of:
   1. the Promotion of Access to Information Act, 2000 (Act no. 2 of 2000);
   2. being clearly marked "Confidential" and which is provided by one Party to another Party in terms of this Contract;
   3. being information or data, which one Party provides to another Party or to which a Party has access because of Services provided in terms of this Contract and in which a Party would have a reasonable expectation of confidentiality;
   4. being information provided by one Party to another Party in the course of contractual or other negotiations, which could reasonably be expected to prejudice the right of the non-disclosing Party;
   5. being information, the disclosure of which could reasonably be expected to endanger a life or physical security of a person;
   6. being technical, scientific, commercial, financial and market-related information, know-how and trade secrets of a Party;
   7. being financial, commercial, scientific or technical information, other than trade secrets, of a Party, the disclosure of which would be likely to cause harm to the commercial or financial interests of a non-disclosing Party; and
   8. being information supplied by a Party in confidence, the disclosure of which could reasonably be expected either to put the Party at a disadvantage in contractual or other negotiations or to prejudice the Party in commercial competition; or
   9. information the disclosure of which would be likely to prejudice or impair the safety and security of a building, structure or system, including, but not limited to, a computer or communication system; a means of transport; or any other property; or a person; methods, systems, plans or procedures for the protection of an individual in accordance with a witness protection scheme; the safety of the public or any part of the public; or the security of property; information the disclosure of which could reasonably be expected to cause prejudice to the defence of the Republic; security of the Republic; or international relations of the Republic; or plans, designs, drawings, functional and technical requirements and specifications of a Party, but must not include information which has been made automatically available, in terms of the Promotion of Access to Information Act, 2000; and information which a Party has a statutory or common law duty to disclose or in respect of which there is no reasonable expectation of privacy or confidentiality;
3. Notwithstanding the provisions of this Contract, no Party is entitled to disclose Confidential Information, except where required to do so in terms of a law, without the prior written consent of any other Party having an interest in the disclosure;
4. Where a Party discloses Confidential Information which materially damages or could materially damage another Party, the disclosing Party must submit all facts related to the disclosure in writing to the other Party, who must submit information related to such actual or potential material damage to be resolved as a dispute;
5. Parties may not, except to the extent that a Party is legally required to make a public statement, make any public statement or issue a press release which could affect another Party, without first submitting a written copy of the proposed public statement or press release to the other Party and obtaining the other Party's prior written approval for such public statement or press release, which consent must not unreasonably be withheld.

#### 3.3.1.11 Guarantee and warranties

1. The supplier confirms that:
   1. The warranty of goods supplied under this contract remains valid for the duration of the contract after the goods were delivered, installed and commissioned with a sign off, including the clients signature
   2. as at Commencement Date, it has the rights, title and interest in and to the Product or Services to deliver such Product or Services in terms of the Contract and that such rights are free from any encumbrances whatsoever;
   3. the Product is in good working order, free from Defects in material and workmanship, and substantially conforms to the Specifications, for the duration of the Warranty period;

#### 3.3.1.12 Intellectual Property Rights

1. SITA retains all Intellectual Property Rights in and to SITA's Intellectual Property. As of the Effective Date, the Supplier is granted a non-exclusive license, for the continued duration of this Contract, to perform any lawful act including the right to use, copy, maintain, modify, enhance and create derivative works of SITA's Intellectual Property for the sole purpose of providing the Products or Services to SITA pursuant to this Contract; provided that the Supplier must not be permitted to use SITA's Intellectual Property for the benefit of any entities other than SITA without the written consent of SITA, which consent may be withheld in SITA's sole and absolute discretion. Except as otherwise requested or approved by SITA, which approval is in SITA's sole and absolute discretion, the Supplier must cease all use of SITA's Intellectual Property, at of the earliest of:
   1. termination or expiration date of this Contract;
   2. the date of completion of the Services; and
   3. the date of rendering of the last of the Deliverables
2. If so required by SITA, the Supplier must certify in writing to SITA that it has either returned all SITA Intellectual Property to SITA or destroyed or deleted all other SITA Intellectual Property in its possession or under its control
3. SITA, at all times, owns all Intellectual Property Rights in and to all Bespoke Intellectual Property.
4. Save for the license granted in terms of this Contract, the Supplier retains all Intellectual Property Rights in and to the Supplier’s pre-existing Intellectual Property that is used or supplied in connection with the Products or Services

#### 3.3.1.13 Counter Conditions

1. Bidders’ attention is drawn to the fact that amendments to any of the Bid Conditions or setting of counter conditions by bidders may result in the invalidation of such bids.

#### 3.3.1.14 Fronting

1. The SITA supports the spirit of Broad Based Black Economic Empowerment and recognizes that real empowerment can only be achieved through individuals and businesses conducting themselves in accordance with the Constitution and in an honest, fair, equitable, transparent and legally compliant manner. Against this background the SITA will not condone any form of fronting.
2. The SITA, in ensuring that bidders conduct themselves in an honest manner will, as part of the bid evaluation processes, conduct or initiate the necessary enquiries/investigations to determine the accuracy of the representation made in bid documents. Should any of the fronting indicators as contained in the Guidelines on Complex Structures and Transactions and Fronting, issued by the Department of Trade and Industry, be established during such enquiry/investigation, the onus will be on the bidder / contractor to prove that fronting does not exist. Failure to do so within a period of 14 days from date of notification may invalidate the bid / contract and may also result in the restriction of the bidder/contractor to conduct business with the public sector for a period not exceeding ten (10) years, in addition to any other remedies SITA may have against the bidder/contractor concerned.

#### 3.3.1.15 Business Continuity and Disaster Recovery Plans

1. The bidder confirms that they have written business continuity and disaster recovery plans that define the roles, responsibilities and procedures necessary to ensure that the required services under this bid specification is in place and will be maintained continuously in the event of a disruption to the bidder’s operations, regardless of the cause of the disruption.

#### 3.3.1.16 Sub-Contracting as a condition of tender

* + - 1. SITA in terms of the SITA Preferential Policy (PPP), has an obligation to advance designated groups which includes black SMMEs (i.e. Exempted Micro Enterprises (EME) and Qualifying Small Enterprises (QSE) for the supply of certain ICT goods or services where feasible to subcontract for a contract above R50m, an organ of state must apply sub-contracting to advance designated groups.

1. The sub-contracting percentage for this bid will be negotiated at contracting stage with the bidder.
2. SITA reserves the right to accept or reject the proposed percentage subcontracting and further negotiate with the preferred bidder and if not satisfied may not award the tender.

Note (1):

In the case of sub-contracting, the sub-contractors must have valid Tax Clearance Certificates which, upon request by SITA, must be made available to SITA for due diligence purposes.

#### 3.3.1.17 Supplier Due Diligence

1. SITA reserves the right to conduct supplier due diligence prior to final award or at any time during the Contract period and this may include pre-announced / non-announced site visits. During the due diligence process the information submitted by the bidder will be verified and any misrepresentation thereof may disqualify the bid or Contract in whole or parts thereof.

#### 3.3.1.18 Preference Goal Requirements conditions

1. The Bidder’s commitment for the Preference Goal Requirements in this tender will be legally binding and the Bidder needs to perform against their commitment for the duration of the contract which will form part of the Contractual Agreement.
2. The Bidder must sustain, or improve the company’s BBBEE Level for the duration of the contact which will form part of the Contractual Agreement.
3. Performance of Preference Goal Requirements will be determined annually. Bidders must submit their Preference status report indicating progress against the Bidder’s Preferential commitments within 30 days of the yearly anniversary of the contract.
4. Bidders need to keep auditable substantive records / evidence and upon request by SITA must be made available for audit and, or due diligence purposes.
5. SITA reserves the right to require from a Bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim with regards to preferences, in any manner required by SITA.
6. SITA reserves the right to verify information / evidence provided by the Bidder.
7. SITA reserves the right to introduce a **penalty of 1%** of the overall annual year spent by SITA for the prior year if the Bidder fails to comply to **paragraphs (a), (b) and (c) above**.

### 3.3.2 Declaration of compliance and acceptance SCC

I (we), the bidder hereby declare that I (we) accept ALL the Special Conditions of Contract as specified in par 3.3.1 above and shall comply with all stated obligations:

Name of Bidder:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 3.4 Costing and Preference Points Evaluation (Stage 4)

### 3.4.1 Costing and Preference Evaluation

1. In terms of the SITA Preferential Procurement Policy (PPP), the following preference point system is applicable **for this** Bid:
   1. the 90/10 system (90 Price and 10 Specific Goals) for requirements with a Rand value above R50 000 000 (all applicable taxes included).
2. Points will be allocated for each of the **Preferential Goal Requirements** for this tender as indicated in **table 5,** dependant on paragraph (1).
3. The maximum points for this tender will be allocated as follows, subject to paragraph 4 below.
4. Points for this tender shall be awarded for:
   1. Price; and
   2. Preference points for specific goals.

**Table 5:** Points allocation

|  |  |
| --- | --- |
| **Description** | **Points** |
| Price | 90 |
| Preference points for specific goals | 10 |
| Total points for Price and preference points for specific goals | 100 |

### 3.4.2 Costing and Pricing Conditions

1. **South African Pricing** –

The total price must be VAT inclusive and be quoted in South African Rand (ZAR).

1. **Total Price**
   1. All quoted prices are the total price for the entire scope of required services and deliverables to be provided by the bidder.
   2. All additional costs as well as cost of delivery, labour, S&T, overtime, etc. must be included in this bid.
   3. All services, accessories, upgrades and options required by the technology or specified by the client must be included in the quoted price. If not included, bidders will be required to supply these accessories at no cost to the client.
   4. SITA reserves the right to negotiate pricing with the successful bidder prior to the award as well as envisaged quantities
2. **Time and Material**
   1. Time and Material Quotations will not form part of the total bid price. It will be based on an ad-hoc basis as and when required by the client.
3. These conditions will form part of the Contract between SITA and the bidder. However, SITA reserves the right to include or waive the condition in the Contract.
4. The bidder must complete the declaration of acceptance as per **par 4.3** below by marking with an “X” either “ACCEPT ALL”, or “DO NOT ACCEPT ALL”, failing which the declaration will be regarded as “DO NOT ACCEPT ALL” and the bid will be disqualified.

### 3.4.3 Bid Pricing Schedule

1. Bidders **must** complete the bid pricing schedule in the Excel spreadsheet format provided and include this as part their submission.

**Note:**

**Bidders must complete and submit bid pricing in the provided Excel spreadsheet format, and any pricing schedule submitted in a different format will not be considered.**

### 3.4.4 Rate of Exchange Pricing Information

Provide the TOTAL BID PRICE for the duration of Contract and clearly indicate the Local Price and Foreign Price, where –

1. **Local Price** means the portion of the TOTAL price that is NOT dependent on the Foreign Rate of Exchange (ROE) and;
2. **Foreign Price** means the portion of the TOTAL price that is dependent on the Foreign Rate of Exchange (ROE).
3. **Exchange Rate** means the ROE (ZA Rand vs foreign currency) as determined at time of bid.

### 3.4.5 Bid Exchange Rate Conditions

The bidders must use the exchange rate provided below to enable SITA to compare the prices provided by using the same exchange rate:

**Table 6:** Bid Exchange Rate

|  |  |
| --- | --- |
| **Foreign currency** | **South African Rand (ZAR) exchange rate** |
| 1 US Dollar | **R17.57** |
| 1 Euro | **R20.67** |
| 1 Pound | **R24.00** |

**Note (1):**

The ROE indicated above is to ensure a competitive bidding process.

**Note (2):**

The ROE stated above will apply for this tender and Bidder need to indicate the foreign content which will be subjected to ROE fluctuation.

ROE fluctuation will only be applied to the specific foreign component.

The details will be negotiated during the contracting phase.

## 3.5 Declaration of Acceptance

|  | **ACCEPT ALL** | **DO NOT ACCEPT ALL** |
| --- | --- | --- |
| 1. The bidder declares to ACCEPT ALL the Costing and Pricing conditions as specified in **par 3.4.2** above by indicating with an “X” in the “ACCEPT ALL” column, or 2. The bidder declares to NOT ACCEPT ALL the Costing and Pricing Conditions as specified in **par 3.4.2** above by -    1. Indicating with an “X” in the “DO NOT ACCEPT ALL” column, and;    2. Provide reason and proposal for each of the condition not accepted. |  |  |
| **Comments by bidder:**  Provide the condition reference, the reasons for not accepting the condition. | | |

## 3.6 Preference Requirements

1. The bidder must complete in full all the PREFERENCE requirements.
2. Allocation of points per requirements:The points allocation of bidders’ responses to the requirements will be determined by the completeness, relevance and accuracy of substantiating evidence.
3. Points will be allocated for each PREFERENCE requirement as per the criteria set in **tables 8 below**.
4. **The bidder must provide a unique reference number** (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response. During evaluation, SITA reserves the right to treat substantiation evidence that cannot be located in the bid response, as “NOT COMPLY”. The evidence needs to be attached to **Annex A**.
5. **Preference Goal Requirements**
   1. The **Bidder must complete either the 90/10 preference point system** based on the offer submitted by the Bidder and submit proof or documentation required in terms of this tender.
   2. The specific Preferential Goal Requirements for this tender is indicated in **table 7** below.
   3. The Bidder **must indicate their commitment** to claim points for each of the preference points by signing at **par 4.5** in the Invitation to Bid document.
   4. Failure on the part of a bidder to submit proof or documentation required or to comply to **paragraph (d)** above in terms of this tender to claim preference points for the **Preference Goal Requirements** for this tender, will be interpreted to mean that preference points are not claimed.
   5. The Bidder’s **commitment** for the **Preference Goal Requirements** in this tender will be **legally binding** and the Bidder needs to **perform against their commitment** for the duration of the contract which will form part of the Contractual Agreement.
   6. The Bidder **must sustain, or improve** the company’s BBBEE Level for the duration of the contact which will form part of the Contractual Agreement.
   7. **Performance of Preference Goal Requirements will be determined annually.** Bidders must submit their Preference status report to SITA indicating progress against the Bidder’s Preferential commitments **within 30 days after each quarter from the commencement date of the contract**.
   8. Bidders need to keep auditable substantive records / evidence and upon request by **SITA** must be made available for audit and, or due diligence purposes.
   9. **SITA reserves the right** **to** require from a Bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim with regards to preferences, in any manner required by SITA.
   10. **SITA reserves the right to** verify information / evidence provided by the Bidder.
   11. **SITA reserves the right to** introduce a **penalty of 1%** of the overall annual year spent by **SITA** for the prior year if the Bidder fails to comply to **paragraphs (v), (vi)and (vii) above.**

**Table 7: Preference Goal Requirements (Specific Goals)**

| **Preference Goal Requirement #** | **Preferential Goal Requirements** | **Preferential Goal Requirements** | |
| --- | --- | --- | --- |
|  | **Preferential Goal Requirements allocated for this tender** | **Substantiating evidence and evidence reference to be completed by bidder.  Evaluation per requirement: Each requirement indicated in the table below must be completed and points will be allocated based on the evidence required below** | **Evidence Reference** |
|  | **B-BBEE Requirements** |  | |
| 1) | **B-BBEE Requirements**  Promotion of Transformational Objectives. | **Evidence:** The Bidder must provide a copy of the following relevant evidence for the Preferential Goal points which the Bidder qualifies for:   1. **Columns A, B and C in tables 8**   Copy of relevant proof of B-BBEE status level of contributor as defined in the Broad-Based Black Economic Empowerment Act; **and/ or**   1. **Column D in tables 8**   Copy of South African Identification Document (ID); **and/ or**   1. **Column E in tables 8**   Copy of Medical Certificate.  **Note:**  The CIPC (Companies and Intellectual Property Commission) registration documents will also be used as evidence to confirm compliance to the Preferential procurement requirements as part of the evaluation process.  **Points allocation:** Points will be allocated for bidders that meets the requirements as indicated in table **8 in section 3.6** | <provide unique reference to locate the substantiating evidence in the bid response – **Annex A, section 4.6**> |

**Table 8: B-BBEE Points as part of the Preference Goal requirements (Preferential Goal Requirements for (90/10) system)**

**Note: Bidder to select the section for points they wish to claim (Mark as Y=Yes) in the table below.**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Ownership** | | | |  |  |  |
|  | **Reference #** | **Contributor Level as defined in the Broad-Based Black Economic Empowerment Act** | **EME/QSEs** | **Black Owned (BO) (51% or more)** | **Black Woman Owned (BWO) (More than 30%)** | **Youth Owned** | **Owned by People living with disabilities** | **Score** | **Bidder to select the section for points they wish to claim (Mark as Y= Yes)** |  |
|  |  |
|  |  |  | **(A)** | **(B)** | **(C)** | **(D)** | **(E)** | **(F)** |  |  |
|  | **1** | **Level 1** | **3** | **2** | **2** | **2** | **1** | **10** |  |  |
|  | **2** | **Level 1** | **3** | **2** | **2** | **2** | 0 | **9** |  |  |
|  | **3** | **Level 1** | **3** | **2** | **2** | 0 | 0 | **7** |  |  |
|  | **4** | **Level 1** | **3** | **2** | 0 | 0 | 0 | **5** |  |  |
|  | **5** | **Level 2 and 3** | **2** | **1** | **0,5** | **0,5** | **0,5** | **4,5** |  |  |
|  | **6** | **Level 2 and 3** | **2** | **1** | **0,5** | **0,5** | 0 | **4** |  |  |
|  | **7** | **Level 2 and 3** | **2** | **1** | **0,5** | 0 | 0 | **3,5** |  |  |
|  | **8** | **Level 2 and 3** | **2** | **1** | 0 | 0 | 0 | **3** |  |  |
|  | **9** | **Level 4 and 5** | **1** | **0,5** | **0,25** | **0,25** | **0,25** | **2,25** |  |  |
|  | **10** | **Level 4 and 5** | **1** | **0,5** | **0,25** | **0,5** | 0 | **2,25** |  |  |
|  | **11** | **Level 4 and 5** | **1** | **0,5** | **0,25** | 0 | 0 | **1,75** |  |  |
|  | **12** | **Level 4 and 5** | **1** | **0,5** | 0 | 0 | 0 | **1,5** |  |  |
|  | **13** | **Level 6** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **14** | **Level 7** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **15** | **Level 8** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **16** | **Non-Contributor** | 0 |  | 0 | 0 | 0 | **0** |  |  |
|  | **Total Maximum Score Allocation:** | | **10** |  |  |  |  |  |  |  |
|  | F= A+B+C+D+E | | | | | | | |  |  |

1. Bidder Substantiating Evidence

# Technical Mandatory Requirement Evidence

## 4.1 Bidder Certification / Affiliation Requirements

**Attach** a copy of a valid documentation (certificate, letter, or license) as proof that the bidder is the OEM/OSM, or an accredited OEM/OSM reseller, partner or distributor to provide, deliver, install, configure, support, and maintain a NGFW technology **here**.

**NOTE (1):**

The valid documentation (letter/certificate/license) clearly indicating the following information below:

(a) The Regulator Name (OSM/OEM); and

(b) The Bidder’s Name; and

(c) The date it was issued; and

(d) if applicable, the expiry date

**NOTE (2):**

SITA reserves the right to verify information provided.

## 4.2 Bidder Experience and Capability Requirements

Complete table below, noting that:

* + - 1. The Bidder **must** provide **all** of the following reference details from at least two (2) customers to whom the following were delivered, installed, configured, supported and maintained in the past five (05) years from the publication of this bid:

**NOTE (1):**

The Bidder **must provide all** of the following information when completing **table 9**:

* 1. Company name; **and**
  2. Reference Person Name, Tel **and/or** email; **and**
  3. Project Scope of Work; **and**
  4. Project Start and End-date.

**NOTE (2):**

Failure to complete **Table 9** fully as indicated above will result in disqualification.

**NOTE (3):**

SITA reserves the right to verify information provided.

Table 9: References

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Company Name** | **Contact person, telephone and/or e-mail address** | **Project Scope of Work** | **Project start and end date** |
| 1. | <Company name> | <Person Name>  <Tel>  <email> | <Provide reference details from a customer to whom the NGFW technologies was provided delivered, installed, configured, supported and maintained, in the last five (5) years from the publication date of this bid> | Start Date:  End Date: |
| 2. | <Company name> | <Person Name>  <Tel>  <email> | <Provide reference details from a customer to whom a the NGFW technologies was provided delivered, installed, configured, supported and maintained in the last five (5) years from the publication date of this bid> | Start Date:  End Date: |

## 4.3 Special Conditions of Contract Acceptance

The Bidder **must accept ALL** the Special Conditions of Contract (SCC) by completing and signing the declaration of Acceptance in Declaration of compliance and acceptance under the Special conditions (**Section 3.3.2)**

## 4.4 Third Party Risk Management Assessment

The Bidder **must comply** with the Third-Party Risk Management Assessment requirement **by completing All** the questions in **ANNEX B** and **attach it here**.

**NOTE (1):**

SITA reserves the right to verify information provided.

**NOTE (2):**

Failing to complete all the questions, or not Accepting the Declaration of Acceptance above will result in disqualification.

## 4.5 Product Functional Requirement

The Bidder must confirm that they comply with the **Product/Service Functional Requirements** **by completing and signing** **Annex C : Addendum 1** and **attach it here**.

## 4.6 Preferential Goal Requirements

The Bidder **must**:

* 1. **Preference Goal Requirements:**

Bidder to select the section for points they wish to claim (Mark as Y=Yes) in **tables 8 in section 3.6**, dependant on which preference system the Bidder selects in line with **section 3.6; and**

Provide a copy of the following relevant evidence for the Preferential Goal points which the Bidder qualifies for as set out in **table 8** in **section 3.6** and **attach it here**:

* + 1. **Columns A, B and C in tables 8**

Copy of relevant proof of B-BBEE status level of contributor as defined in the Broad-Based Black Economic Empowerment Act; **and/ or**

* + 1. **Column D in tables 8**

Copy of South African Identification Document (ID); **and/ or**

* + 1. **Column E in tables 8**

Copy of Medical Certificate.

* 1. Indicate their **commitment** to claim points for each of the preference points **by signing at par 4.5 in the Invitation to Bid document**.

**NOTE (1):**

**Failure on the part of a bidder to comply to paragraphs (1) and (2) above, will be interpreted to mean that preference points are not claimed.**

1. THIRD-PARTY RISK MANAGEMENT (TPRM) ASSESSMENT
2. **INSTRUCTIONS**
3. In terms of the approved SITA Third-Party Risk Management Framework, all Bidders responding to this bid **must** complete the following section by answering **ALL** the questions.
4. By completing the Third-Party Risk Management Assessment, the Bidder agrees to provide all reasonable supporting documentation when requested to do so, as well as during contract finalisation as this is a **pre-award condition of this bid**.
5. Any risk identified during the assessment process will have to be mitigated and/or remediated before or during the contract finalisation phase. A detailed mitigation plan, that is acceptable to SITA, may also be required.
6. Supplier due diligence, as contained in the Special Conditions of Contract, is also applicable to this Third-Party Risk Management process.
7. The following 6 (six) risk elements will be assessed:
   1. Company risk: 10 questions;
   2. Financial risk: 6 questions;
   3. Operational risk: 8 questions;
   4. Governance and compliance risk: 6 questions;
   5. Information security and privacy risk: 7 questions;
   6. Reputational risk: 6 questions.
8. **EVALUATION CRITERIA**
9. Company risk
   1. Questions 2, 3, 6, 8, 9, 10:

| **Evaluation criteria** | **Score** |
| --- | --- |
| Yes | 0 |
| Partially meet requirements | 0.5 |
| No | 1 |

* 1. Questions 4, 5:

| **Evaluation criteria** | **Score** |
| --- | --- |
| Yes | 1 |
| Partially meet requirements | 0.5 |
| No | 0 |

* 1. Question 7:

| **Evaluation criteria** | **Score** |
| --- | --- |
| Yes, actively operating for more than 5 years | 1 |
| 2-5 Years actively operating | 0.5 |
| No, actively operating for less than 2 years | 0 |

1. All questions for all other risk elements:

| **Evaluation criteria** | **Score** |
| --- | --- |
| Yes | 1 |
| Partially meet requirements | 0.5 |
| No | 0 |

1. **THIRD PARTY RISK ASSESSMENT**

The assessment of bidders’ responses to the questions will be determined by the completeness (i.e. **all** questions answered), undertaking signed (where required) and accuracy of substantiating evidence, when requested. Please note that SITA reserves the right to verify the information provided.

| **Question to assess each risk element** | **Bidders response:**  **Mark relevant box with an “X”** | | |
| --- | --- | --- | --- |
| **Company Risk** | | | |
| 1. Have you disclosed all interests and relationships as required in **SBD 4**, including whether any of your directors, members, trustees, or shareholders are employed by the state, have relationships with SITA employees, or have interests in other entities (whether they are also bidding for this contract, or not)? | **YES** | **PARTIALLY** | **NO** |
| 1. Are you currently involved in litigation against SITA – or do you foresee litigation being instituted within the next 6 months? | **YES** | **PARTIALLY** | **NO** |
| 1. Are there any law suits or ongoing litigation that could affect this transaction in any way or the bidder as an ongoing concern? | **YES** | **PARTIALLY** | **NO** |
| 1. Is customer service delivery or contract performance actively monitored by you? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have formal strategic planning processes in place? | **YES** | **PARTIALLY** | **NO** |
| 1. Are any of your directors or shareholders Prominent Influential People (PIP) or Politically Exposed Persons (PEP)? | **YES** | **PARTIALLY** | **NO** |
| 1. Has your company been actively operating as a going concern for more than 5 years? | **YES** | **2-5 YEARS** | **LESS THAN 2 YEARS** |
| 1. Is the company busy with a re-organisational/restructuring process that may impact this transaction? | **YES** | **PARTIALLY** | **NO** |
| 1. Are any of your suppliers located in a region where geopolitical risk exposure is high? | **YES** | **PARTIALLY** | **NO** |
| 1. Has any current director of the bidder ever served as a director of a company during a period where a Government contract was cancelled? | **YES** | **PARTIALLY** | **NO** |
| **Financial Risk** | | | |
| 1. Did you have positive revenue growth in the past three (3) years? | **YES** | **PARTIALLY** | **NO** |
| 1. Is the proposed bid price going to be **less than 40%** of your total annual revenue for the previous financial year? | **YES** | **PARTIALLY** | **NO** |
| 1. Is the financial health of your company in good standing? | **YES** | **PARTIALLY** | **NO** |
| 1. Were your Annual Financial Statement (AFS) unqualified in the last financial year? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have sufficient cash in the bank (2 or more months’ worth of operating cost) to operate under restricted conditions for at least 2 months? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have a clean credit record: No current or pending judgement, adverse listing, business rescue or principal sequestration listing? | **YES** | **PARTIALLY** | **NO** |
| **Operational Risk** | | | |
| 1. Do you have operational redundancy (resilience) in terms of technology and energy resources to ensure high availability of services? | **YES** | **PARTIALLY** | **NO** |
| 1. Are your dependencies for logistics either fully under your own control **or** managed through supplier performance management contracts? (Choose “Yes” if fully under your own control and “No” for supplier contracts) | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have operational procedure standards in place across the organisation, such as change control, release management, access control, incident management, back-up regimes and restore tests, etc? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have human resources management in place, including succession planning and mitigation against key reliance on single individuals? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have sound supply chain processes in place? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have sound third party risk management processes in place (fourth party for SITA)? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have a fully-fledged research and development (R&D) department to ensure continuous improvement? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you rely on locally manufactured components or have actively managed the risk relating to lead times or delivery delays? (Choose “Yes” is you rely on locally manufactured components or can actively manage lead times and prevent delivery delays where manufacturing is not local i.e. not in South Africa) | **YES** | **PARTIALLY** | **NO** |
| **Governance and Compliance Risk** | | | |
| 1. Do you comply with all legislation, including labour, health and safety regulations? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have the appropriate governance frameworks (Cobit, ITIL, King) in place with due monitoring against set standards? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have an internal audit function compliant with IIA standards (insourced, outsourced or co-sourced) in place? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you follow formally documented enterprise risk management processes? | **YES** | **PARTIALLY** | **NO** |
| 1. Are all statutory requirements of the entity up to date? Specifically, the following: CIPC Returns, Tax returns, UIF and COIDA. | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have comprehensive insurance in place, including cover for assets, business disruption and liability? | **YES** | **PARTIALLY** | **NO** |
| **Information Security and Privacy Risk** | | | |
| 1. Are your physical security perimeters appropriately safeguarded? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have video surveillance of areas that will contain SITA information/products? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you conduct security and suitability verification of all employees prior to employment? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have identification verification controls in place in all your buildings? | **YES** | **PARTIALLY** | **NO** |
| 1. Are your access control protocols verified to be effective by Internal and/or External Auditors? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have Security Information and Events Management (SIEM) processes in place? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have sufficient information security and cyber arrangements in place for employees working from home? | **YES** | **PARTIALLY** | **NO** |
| **Reputational Risk** | | | |
| 1. Do you have anti-bribery and corruption, anti-money laundering and fraud prevention practices in place? | **YES** | **PARTIALLY** | **NO** |
| 1. Please confirm that neither the company, nor any of its directors has been named in any corruption scandal (choose “Yes” to confirm **not being named** in a corruption scandal) | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have a social responsibility programme in place? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you have an environmental protection policy, including potential harmful emission or hazardous waste management? | **YES** | **PARTIALLY** | **NO** |
| 1. Do you actively manage your organisation’s energy consumption? | **YES** | **PARTIALLY** | **NO** |
| 1. Is your employment equity plan up to date and actively managed? | **YES** | **PARTIALLY** | **NO** |

1. **THIRD PARTY RISK MANAGEMENT DECLARATION**

The bidder hereby makes the following declaration and confirm the following information (mark with a “X” in the corresponding column):

| **STATEMENT OF DECLARATION** | **ACCEPT AND CONFIRM** | **DO NO ACCEPT AND CONFIRM** |
| --- | --- | --- |
| 1. All questions in this assessment were answered accurately. |  |  |
| 1. SITA can request additional supporting documentation, within reason, to confirm the accuracy and completeness of the information provided in this self-assessment. |  |  |

**DECLARATION OF ACCEPTANCE**

|  |  |  |
| --- | --- | --- |
|  | ACCEPT ALL | DO NOT ACCEPT ALL |
| 1. The bidder declares that all information provided in this assessment is accurate. 2. The bidder understands that any false information may constitute misrepresentation.    1. SITA reserves the right to verify the information provided. 3. By completing the Third-Party Risk Management Assessment the Bidder agrees to provide all reasonable supporting documentation when requested to do so, as well as during contract finalisation as this is a pre-award condition of this bid. 4. The bidders understand and agrees that this section will form part of the contract and is legally binding. |  |  |
| Any additional comments by bidder pertaining to the third-party risk assessment: | | |

**NOTE (1):**

**Failing to complete all the questions, or not Accepting the Declaration of Acceptance above will result in disqualification.**

1. Product/Service Functional Requirements ADDENDUM 1

**NB: The Bidder must confirm that they comply with the following Product / Service Functional requirements as indicated below as this will be legal contractual binding.**

Refer to Section 2 Scope of Work and Section 3 Requirements for the detailed information:

### Appliance Base Firewalls

**Enterprise Firewall Service**

|  |  |
| --- | --- |
| **Product** | **Quantity** |
| Next-Generation Firewall Technology Appliance (Pretoria only) | 4 |

|  |  |
| --- | --- |
| **Performance** | **Minimum Requirement** |
| Threat Prevention/Protection  AV Enabled  IPS Enabled  APP Control Enabled  URL Filtering Enabled | 20 (Gbps) |
| NGFW Throughput  App Control Enabled  IPS Enabled | 75 (Gbps) |
| VPN Throughput | 80 (Gbps) |
| Connections per second | 1M |
| Concurrent sessions | 50M |
| **Network** |  |
| 10 /100/ 1000 Base-T (Ports) | 8 |
| 10GBase-F SFP+ (Ports) | 12 |
| **Additional Features** |  |
| Enclosure | 1RU |
| Storage | 500GB minimum – sufficient storage to be provisioned for the contracted period |
| Dual, Hot-Swappable Power Supplies | Yes |

**Regional Firewall Service**

|  |  |
| --- | --- |
| **Product** | **Quantity** |
| Next-Generation Firewall Technology Appliance (Regions) | 20 |

|  |  |
| --- | --- |
| **Performance** | **Minimum Requirement** |

|  |  |
| --- | --- |
| Threat Prevention/Protection | 10 (Gbps) |
| NGFW Throughput | 20 (Gbps) |
| IPS Throughput | 20 (Gbps) |
| Firewall | 40 (Gbps) |
| Firewall Throughput | 60 (Gbps) |
| Connections per second | 330K |
| Concurrent sessions | 20M |
| **Network** |  |
| 10 /100/ 1000 Base-T (Ports) | 12 |
| 10GBase-F SFP+ (Ports) | 6 |
| **Additional Features** |  |
| Enclosure | 1RU |
| Storage | 500GB minimum – sufficient storage to be provisioned for the contracted period |
| Dual, Hot-Swappable Power Supplies | Yes |

**Integrate with traditional firewall functionality such as packet filtering, address translation (NAT),** stateful inspection and Virtual Private Networking (VPN) with next-generation functionality.

**Mobile SSL Access Termination**

The NGFW technology must provide a Mobile SSL Access technology to provide safe and easy connectivity to corporate applications over the internet with Smartphones, tablets, or PCs. The technology must also provide enterprise-grade remote access via both Layer-3 VPN and SSL VPN, allowing simple, safe, and secure connectivity to your email, calendar, contacts, and corporate applications.

**Clustering**

The NGFW technology must be able to provide high-end enterprise and data centre environments where performance and availability are critical. Gateways will be clustered for business continuity and/or resource sharing.

**Additional Requirements**

* + - Outbound IPSEC and SSL encryption facilities.
    - Port trunking functionality.
    - Port Aggregation functionality.
    - Detect non-standard port hopping therefore not assuming standard port assigned utilisation.
    - Agent-based monitoring with support for customised alert generation

Identify all users, systems and applications regardless of the port or protocol used.

Protect against unauthorised access to systems, applications and network infrastructure

Provide real-time protection against threats occurring on all layers including the application layer.

Protect against data leakage.

Protect against website hack attacks and defacements.

Integrate with traditional firewall functionality such as packet filtering, address translation (NAT), stateful inspection and Virtual Private Networking (VPN) with next-generation functionality.

Provide high performance such as gigabit in-line throughput without service degradation.

**Remote VPN access:**

* + - The NGFW technology must offer effective Virtual Private Network (VPN) access functionality, fully integrable with multifactor authentication to Active Directory:
      * Allow a secure VPN setup to provide remote access capability for users.
      * Allowing users to connect with any device, tablet smartphone and laptop from any remote location.
      * Allow unlimited IPSec and SSL functionality

**Network integration:**

* The NGFW technology must provide effective:
  + - * VLAN support.
      * IPv6 Support.
      * Dynamic Host Configuration Protocol (DHCP) relay.
      * Routing protocols (Routing Information Protocol [RIP], OSPFv3).
      * Exterior Gateway Routing Protocols (BGP).
      * Support for Layer 2 (transparent) mode.
      * Multilink/multi-ISP connectivity.

**Encryption:**

* The NGFW technology must be able to:
  + - * Provide client-to-site SSL, TLS or DTLS VPN.
      * Provide client-to-site IPsec VPN.
      * Provide certificate-based VPN user identity recognition.
      * Support username- and password-based VPN user identity recognition.
      * Provide Site-to-site IPsec VPN.
      * Enforce and Support Strong encryption.
      * Provide VPN client load balancing and clustering.

**Visibility into encrypted packets:**

* The NGFW technology must be able to decrypt the traffic to inspect the content; else such traffic should be diverted to a secure area with applicable notifications raised to the OSIS team.

**Stability and reliability:**

* The NGFW technology must provide stability and reliability.
  + - * It is critical that the firewalls deployed can manage the traffic with regard to speed and bandwidth. From a growth perspective, it is important to bring scalability into the calculation and to ensure that the device(s) will be able to manage the traffic for the next five years.

**Load balancing:**

* The technology should be able to provide load-sharing high availability (active/active, active/standby) to ensure optimum service uptime and service delivery.

**High availability:**

* The technology should be able to provide high availability (active/active, active/standby) to ensure optimum service uptime and service delivery:
  + - * High availability and load-balanced proxy functionality for both forward and reverse proxy configurations with support for SSL termination and SSL streaming interrogation by the IPS.
      * High availability (active/active, active/standby).
      * Redundancy in physical appliances.
      * Out-of-band management.
      * Hot swap of components in physical appliances.

**Manager and Reporter**

* Automatically adapt to the threat landscape without any user intervention and should be able to follow up manually on thousands of security advisories and recommendations.
* Integrate seamlessly into the SAPS environment and the technology will require providing a defensive posture that collaboratively leverages both internal and external intelligent sources.
* Needs to make filter decisions based on specific business rules, assets, users, roles and applications as well as define security policies for the set of authorised interactions between the same asset, users and applications (e.g. access control would determine whether a user is allowed to access sensitive government data or services and could qualify authorization base on the user’s location, host status, time of the day.)
* Correlates findings from multiple engines, signatures, reputation, behaviour, malware emulation and human validation to gain a higher level of confidence. In addition, the technology should leverage extensive and reliable internal and external threat sources to generate meaningful and actionable security intelligence (i.e. threat indicators that can be used to detect and prevent threats).

**Identity Awareness**

The NGFW technology must provide granular visibility of users, groups and machines, providing application and access control through the creation of accurate, identity-based policies. Identity Awareness seamlessly integrates with Active Directory (AD) with multiple deployment options and third-party two-factor authentication technologys.

**Audit Logging**

* Administrator audits.
* Reporting engine.
* Standard reports.
* Alerts.
* SIEM integration.
* Export of log information.
* NetFlow statistics.
* Action if the firewall cannot log events.
* Reliable logging; and
* Use of threat intelligence in reports.

**Centralised Management:**

* The NGFW technology must be able to be deployed to various peering points and report to one centralised console.
* The NGFW technology must complement the ability to collate all different plug-ins thereby providing a unified threat management (UTM) concept. Features must, therefore, provide combined IPS/IDS, firewall and filtering methods at one location.
* The NGFW technology must be provided.
  + - * Object-based configuration.
      * Change then commits.
      * Rule verification mechanism.
      * Reason/tracking of rule changes.
      * AD/LDAP integration.
      * Rule change rollback.
      * Unified three-tier management of VPNs.
      * Rule usage statistics.
      * Hierarchical management roles.
      * Lateral management roles.
      * Threat intelligence feeds.
      * Workflow and automation.
      * Simultaneous changes.
      * Rule reduction/simplification mechanism.
      * Traffic profile verification.

**Firewall ruleset:**

* The NGFW technology must provide the capability to implement the following ruleset:
  + - * Stateful inspection functionality inspection for traffic on layers 3 and 4 to allow or block traffic.
      * Anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside).
      * User permit rules (e.g. allow HTTP/S to public webserver).
      * Management permit rules (e.g. SNMP traps to network management server).
      * Noise drops (e.g. discard OSPF and HSRP chatter).
      * Deny and Alert (alert systems administrator about traffic that is suspicious).
      * Deny and log (log remaining traffic for analysis).
      * SSL Inspection.

**User identification:**

* The NGFW technology must:
  + - * Identify all users on the network with integration with Active Directory (AD) and LDAP services.
      * Link the user with an IP address and login activity locally on the LAN, VPN or any other form of network access.
      * Be able to provide security policy enforcement against all users (legal users and illegal users, permanent, contractors, visitors, and consultants) on the SAPS network and connected remote VPNs.
      * Identify and track user activity enabling the building of user profiles and tracking anomalies associated with the profiles.
      * Identify privileged users and sensitive data, and access monitoring.
      * Show a user's threat trend or risk profile of the user.
      * Provide login activity and provide monitoring.

**Firewall policy management:**

* The NGFW technology must have the capability to create policy-based controls utilising application identification, user identification and content identification.

**Reporting:**

* The bidder and the NGFW technology must provide practical extraction and reporting language functionality.

**Provide a granular level of reporting for:**

* Administrators.
* Management.
* Executives.

**Bandwidth control:**

* The NGFW technology must allow granular level bandwidth control; and control the bandwidth for specific users, environment and function.

**Reporter to manage and provide all reporting functionality.**

### Sandboxing Capability (standalone appliance only)

|  |  |
| --- | --- |
| **Product** | **Quantity** |
| Sandbox device | 2 |

| **Specification** | **Minimum Requirement** |
| --- | --- |

|  |  |
| --- | --- |
| Hardware | Standard rack-mounted 2U appliance |
| Interfaces | 4 x GE electrical ports, 2 x 10GE optical ports |
| Hybrid traffic performance indicator in traffic restoration | 2 Gbit/s (bidirectional traffic of a 1 Gbit/s link) |
| HTTP performance indicator | 1.2 Gbit/s |
| FTP performance indicator | 300 Mbit/s |
| Email protocol performance indicator | 500 Mbit/s |
| PDF file inspection performance | 100000 files/day |
| (file size: 1 MB) |
| Office file inspection performance | 200000 files/day |
| (file size: 1 MB) |
| Script file inspection performance | 120000 files/day |
| (file size: 10KB) |
| Maximum number of interworking devices supported by a cluster manager | 256 |
| SWF file detection | Support obfuscated code and malformed data detection |
| Script file detection | Support trojan, backdoor, worm, virus detection |
| PE file inspection | Support trojan, backdoor, worm, virus detection |
| PDF file inspection | Support shellcode, file format vulnerability detection |
| Web file inspection | Support static flash, shellcode, script trojan detection |
| Office file inspection | Support file format vulnerability, shellcode detection |
| Support file blacklist & whitelist | Yes |

* + - Support segmentation as part of the threat containment, to ensure that a successful attack on one part of the environment doesn’t compromise the entire environment.
    - Ability to constrain the system to normal behaviour thus able to block malware even if it’s successfully subverted system component (e.g. an unidentified host that is performing an abnormal network scan can be restricted using containment control).
    - Support sandboxing technique, which allows documents and applications to be executed in a contained environment that emulates the target system to analyse detect and prevent any unexpected behaviour.
    - The NGFW technology must provide a capability to quarantine suspected malicious content to be investigated and cleaned before the file and access are released to the network.
    - The sandboxing technology must inspect the unknown devices and access them.

### On Premise or Cloud-Based Web Application Firewall Services

|  |  |
| --- | --- |
| **Product** | **Quantity** |
| Web Application Firewall | 4 appliances / 60 000 users |

**URL Filtering**

The technology must provide secure reverse proxy services to deployed public websites and SAPS systems. The technology must provide optimised web security through full integration in the gateway to prevent bypass through external proxies. Integration of policy enforcement with Application control.

**Application Control**

The technology must provide strong application security and identity control to organisations of all sizes. It must allow IT teams to easily create granular policies - based on users or groups - to identify, block or limit usage of Web 2.0 applications and widgets.

**Traffic inspection:**

* The technology must provide:
  + - * Passive network traffic capturing functionality.
      * Analyses and inspect traffic including all encrypted traffic such as SSH or TLS/SSL with no assumptions that such traffic is legitimate.
      * Conduct deep packet inspection.

**Application identification:**

* The technology must provide dynamic application control and protection:
  + - * Identify and protect known and unknown applications from known and unknown sources.
      * Inspect application content.
      * Protect all Web-based Applications from cyber application attacks.
      * Inspect encrypted application traffic following through VPN IPsec tunnels using HTTPS protocols.
      * Having the capability of examining various codes such as EBCDIC, Binary, ASCII and Unicode must be considered for the device evaluation.
      * Identify all users on the network with integration with Active Directory (AD) and LDAP services.
      * Identify applications within the HTTP/S protocol (browser-based applications).
      * Enforce policy on individual users and users’ groups.
      * Enforce Bandwidth usage.
      * Provide application control support for encapsulated traffic.
      * Provide application control support of 4 over 6 and 6 over 4 tunnels.
      * Provide support for the application information feed.
      * Provide user-developed application signatures.
      * Provide application whitelist/blacklist.
      * Filter URLs.
      * IPv6 support for application control.
      * Identify applications within the SSL protocol.
      * Block the upload of data even when allowing access to the site.

**Application and content filtering:**

* The technology must examine embedded content ensuring alignment with respect to application and packet content must be possible with the level of device intensity.

**Internet security:**

* + URL filtering to classify content and block unwanted sites.
  + Whitelisting and blacklisting of websites.
  + Conduct object inspection.
  + Content filtering with blacklist customisation and the ability to download and update blacklists via synchronisation for a centralised source.

**Predict the likelihood of unknown threats from IP, URL, application, and mobile. The technology must be able to protect all services against web/internet-based attacks including:**

* + Blind SQL Injection.
  + Cross Site Scripting.
  + Script Source Code Disclosure.
  + Expression Language Injection.
  + HTTP Parameter Pollution.
  + Application error message.
  + Directory Listing.
  + Error message on page.
  + Login page password-guessing attack.
  + Possible sensitive directories.
  + Possible sensitive files.
  + Session Cookie without Secure flag set.

### Threat Control and Network Threat Protection

Enable comprehensive visibility that allows SITA to “fight through” attacks while maintaining acceptable levels of service by detecting, containing and repelling cyber-attacks, as well as supporting follow-up investigation and recovery and collaboration.

The NGFW technology must reduce security breaches by guarding the SAPS information systems:

* Minimising the likelihood of any potential information security breaches being exploited by malicious individuals, applications or systems in production.
* Reducing time, effort and expenditure involved with pro-active identification of information security threats.
* Providing real-time information security protection service.
* Improving the quality of information security, and vulnerability management in SITA and the South African government.
* Addressing all internal and external audit findings.
* Ensuring compliance with SAPS and government information security policies, standards, processes and procedures.
* Ensure compliance with legislative and regulatory requirements such as POPI, ECT Act, PAIA, RICA, etc.

Anti-virus and malicious code:

The NGFW technology must provide antivirus, malicious code and spyware protection to effectively protect against malicious threats entering and exiting the SAPS environment.

Evasion attacks:

* The NGFW technology must provide effective protection against evasion attacks.
* The NGFW technology must protect evasion techniques such as RPC fragmentation, FTP evasion TCP stream segmentation. IP fragmentation, HTML evasion and URL obfuscation.

Advanced persistent attacks:

* + - * + The NGFW technology must protect against.
      * Advanced Persistent attacks.
      * Targeted Attacks.

Botnets and DLP:

* + - * + The NGFW technology must protect against.
      * Botnets.
      * Data leakage through the gateway.
      * Information Theft through the gateway.
      * Web attacks such as website defacements and website hacking.
      * Phishing attacks.

Advanced/Intelligent threat management:

* + - * + The bidder and the NGFW technology must be able to.
      * Provide continuous real-time advanced and intelligent threat scanning and management.
      * Predict the likelihood of an unknown threat from IP, URL, application, mobile device or user such as a malicious attack.
      * Update risk as the threat landscape evolves.
      * Protect by blocking or deleting threats against the possibility of threat that may lead to an exploit.
      * Provide in-depth defence.

### Intrusion Prevention System Capability

The NGFW technology must provide IPS protection with breakthrough performance and complete and proactive intrusion prevention—all with the deployment and management advantages of a unified and extensible next-generation firewall technology.

* + Provide effective Intrusion Prevention Service (IPS) protecting against vulnerability attacks including, deep packet scanning, traffic normalisation and defragmentation using mechanisms such as protocol anomalies, behaviour anomalies and heuristic detection mechanisms.
  + Include signature-based IPS.
  + Ability to modify existing IPS signatures.
  + Monitor, identify and block Malicious activities and attacks.
  + Provide multi-threaded multi-queuing IPS.
  + DoS and DDOS protection.
  + Stateful inspection and IPS support for encapsulated traffic.
  + Stateful inspection and IPS support of 4 over 6 and 6 over 4 tunnels.
  + User-developed signatures for IPS.
  + Use AD or LDAP for context.
  + Built-in decryption capability.
  + Detect and prevent intrusions.

### Anti-DDoS capability (standalone appliance only)

|  |  |
| --- | --- |
| **Product** | **Quantity** |
| Anti-DDoS | 2 |

|  |  |
| --- | --- |
| **Hardware Specification** | **Minimum Requirements** |
| 10 /100/ 1000 Base-T (Ports) | 6 |
| 10GBase-F SFP+ (Ports) | 6 |
| Management | 10 /100/ 1000 Base-T |
| Serial Port | 1 RJ |
| Rack | 2U |
| Dual Power Supply | Yes |
| Hard Disc (SSD storage) | 500GB minimum – sufficient storage to be provisioned for the contracted period. |
| Throughput | 8 GB |
| Delay in processing | Less than 60µs |
| Application Layer Throughput | 6 GB |

Anti-DDoS attacks:

* The technology must protect against.
  + - * Dynamic Denial of Service Attacks.
      * Should anticipate where and when denial of service attacks will be launched and guard against it.
      * Have the capability to know where advanced malware will be downloaded from.
      * Real-Time Traffic Monitoring: Ability to monitor and analyse traffic patterns continuously to identify and mitigate threats early.
      * Scalability: The technology must handle traffic surges of varying magnitudes, accommodating future growth in legitimate traffic and larger attack sizes.
      * Automated Response: Automation ensures rapid detection and mitigation without requiring manual intervention, minimizing downtime.
      * Layered Defense Capabilities: Protects against different attack types, including volumetric, application-layer, and protocol-based attacks.
      * Integration with Existing Infrastructure: Compatibility with the organisation’s current network architecture and security tools is essential.
      * Low Latency: The technology should not negatively impact legitimate traffic or degrade user experience.
      * Customizable Policies: Ability to tailor protection rules and thresholds to specific organisational needs.
      * Reporting and Analytics: Detailed insights into attack trends, mitigation activities, and system performance to support strategic decisions.
      * Vendor Support and SLA: Comprehensive support services and a clear service-level agreement (SLA) to ensure reliability.

## Lifecycle Management

The product lifecycle management must align with SAPS requirements, ensuring a minimum of 5 years of support and maintenance entitlement for the department. This includes the lifecycle of appliances, accessories, software, and operating system support. Throughout the contract period, the product must remain fully supported and maintained.

## Skills Transfer and Training

Comprehensive formal training, including examinations and certification, must be provided for six SAPS/SITA specialists.

Training must be conducted for six SAPS/SITA personnel with each system upgrade.

In addition, the Service Provider is required to offer continuous, hands-on training to ensure sustained skill development.

**I, the bidder (Full Names)………………………………………………………….representing(company name)……………………………………………………………..Hereby confirm that I comply with the above Product/Service Functional Requirements and understand that it will form part of the contract and is legally binding.**

**Thus done and signed at …………………………………….. On this………day of……………..….20….**

**……………………………….**

**Signature**

**Designation**