|  |  |  |  |
| --- | --- | --- | --- |
| **5.1** | | **Description** | **Page ref** |
| **WAN Connectivity (IAAS)** |  | Primary **Fibre**: **60 MB** Fibre connection to the provider’s closest POP; |  |
|  | Secondary **Wireless:** **60MB** wireless backup link compliant with ICASA regulations; |  |
|  | Implement BGP and HSRP protocols (or equivalent) to facilitate failover between primary and secondary links, in case of router or line failure, inbound and outbound; |  |
|  | Quality of Service on both links to ensure application priority according to WCPP’s business requirements; |  |
|  | At least 95% Uptime; and |  |
|  | Fully outsourced customer edge equipment and router management; Management of router-infrastructure to ensure reliability, security, reachability and availability. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.2 | | **Description** | **Page ref** |
| Internet breakout (IAAS)  ( |  | Uncapped internet breakout; |  |
|  | 60MB bandwidth; |  |
|  | synchronous; |  |
|  | Low contention, preferred 1:1; and |  |
|  | At least 95% uptime. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.3 | | **Description** | **Page ref** |
| Managed Firewall, IDS / IPS (IAAS) |  | Implement rules as per WCPP security policy and compliance with industry best practices and mitigation against known cyber threats; |  |
|  | Performance and availability management; |  |
|  | Real-time threat monitoring and response; |  |
|  | On-demand security and compliance reporting; |  |
|  | Expert support - management of firewall-infrastructure to ensure reliability, security,reachability and availability; |  |
|  | At least 95% uptime; |  |
|  | Change management; and |  |
|  | Backup and recovery. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5.4** | | **Description** | **Page ref** |
| **SITA site-site VPN Tunnel (IAAS)** |  | Create Service Provider -to - SITA IPsec VPN Tunnel; |  |
|  | Firewall Configuration of IPsec tunnel on A-side (Provider side); |  |
|  | Collaboration with SITA to complete the firewall configuration on B-side (SITA side); |  |
|  | Monitoring to ensure tunnel remains up; |  |
|  | Proactive escalation with SITA and notification to WCPP if tunnel goes down; |  |
|  | **NB**: Decommissioning of tunnel when contract with SITA ends in Nov 2018; and |  |
|  | At least 95% uptime. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5.5** | | **Description** | **Page ref** |
| **DR and Failover infrastructure (IAAS)** |  | Colocation required. Provision a full-rack to host WCPP servers, network devices and other ICT equipment; |  |
|  | Real time data replication from primary to DR through quality of service policy; |  |
|  | Sufficient bandwidth to DR / colocation environment, from WCPP LAN users and client VPN users, when a disaster is declared. |  |
|  | Intelligent climate control, access control, redundant power and environment monitoring; |  |
|  | A geographic location that exceeds a distance of **5km’s** from 7 Wale Street Cape Town, within the Western Cape area as per the Auditor General requirement; |  |
|  | Encrypted logical access to all users using the public internet backbone, using client VPN services; |  |
|  | Logical access to all users on the corporate LAN; |  |
|  | Physical access to the facility for approved WCPP stakeholders; and |  |
|  | At least 95% uptime. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5.6** | | **Description** | **Page ref** |
| **Client VPN Service (IAAS)** |  | Client VPN access to Primary and DR site; |  |
|  | 100 VPN accounts; |  |
|  | Integration with Microsoft Active Directory (AD); |  |
|  | Two-factor authentication using mobile phone; |  |
|  | Scalable to any future user seat requirement; and |  |
|  | At least 95% uptime. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.7 | | **Description** | **Page ref** |
| Web Server (Secure, reliable and scalable SAAS service) |  | Elastic web services for peaks and future high demand; |  |
|  | Linux Drupal content management and website hosting; |  |
|  | Root / administration access - self managed; |  |
|  | Similar to “Hetzner TruServ Plus” offering; |  |
|  | Protection and mitigation against DDoS attacks; |  |
|  | Web application security and patching to avoid security breaches; |  |
|  | Highly available web services; |  |
|  | TLS encryption and certificate management; |  |
|  | At least 95% uptime; |  |
|  | Web based, secure control panel for configuration; and |  |
|  | Backup and recovery. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.8 | | **Description** | **Page ref** |
| Public DNS Service (SAAS) |  | Primary DNS server; |  |
|  | Secondary DNS server hosted outside the core Cape Town environment, to ensure continuity of name resolution in case of local disaster or provincial internet outage; |  |
|  | At least 95% uptime; and |  |
|  | Web based, secure control panel for configuration. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5.9** | | **Description** | **Page ref** |
| **Email risk management and archive service (SAAS)** |  | Email relay with 256 bit TLS encryption support; |  |
|  | Email and calendar archiving; |  |
|  | Microsoft Active directory and Exchange integration; |  |
|  | Inbox and Sent items, with mapping of outlook subfolders; |  |
|  | Email threat protection (Anti-spam, Antivirus, Anti-Spoof, Anti-Ransomware) |  |
|  | Support for secure encrypted large file sharing (up to 1GB); |  |
|  | Email continuity and failover using different access methods; |  |
|  | Compliance with GDPR (general data protection regulation); |  |
|  | Email policies; |  |
|  | Email discovery; |  |
|  | At least 95% uptime; and |  |
|  | Web based configuration and monitoring. |  |