**TERMS OF REFERENCE (TOR)**

# **APPOINTMENT OF A SERVICE PROVIDER FOR THE PROVISION OF CYBERSECURITY SERVICES TO THE SOUTH AFRICAN NURSING COUNCIL (SANC) FOR A PERIOD OF THREE (03) YEARS**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# **PURPOSE**

# The purpose of this document is to appoint a reputable Cybersecurity service provider to provide Cybersecurity services as per section 3 of the Terms of Reference (ToR) for a 3-year period.

# **BACKGROUND**

* 1. The South African Nursing Council (SANC) is the body entrusted to set and maintain standards of nursing education and practice in the Republic of South Africa. It is an autonomous, financially independent, statutory body, initially established by the Nursing Act, 1944 (Act No. 45 of 1944), and currently operating under the Nursing Act, 2005 (Act No. 33 of 2005).
  2. The SANC requires to procure services from a Cybersecurity service provider to ensure that the SANC remains safe and secured from Cybersecurity threats such as ransomware, data leakage, hacking, insider threats and phishing.
  3. The provision of the Cybersecurity services is required to assist the organisation to ensure that the SANC remains protected against unauthorised access to data and systems, unauthorised remote connections; that it complies with international practices for Cybersecurity, to implement adequate and effective user awareness campaigns on issues related to cyber threats for the SANC users and its stakeholders, as well as to effect knowledge transfer to the SANC staff on related matters.
  4. The SANC is in the process of migrating its Microsoft email solution (Exchange Services) to Office 365 (hybrid cloud solution) and providing online access to its core business application to the nurses, student nurses and other stakeholders. The Nurse Register application will be accessed by the nurses and student nurses through a public portal which is hosted on the SANC web site (www.sanc.co.za).

# **SCOPE OF WORK AND DELIVERABLE(S)**

* 1. The SANC has a requirement to enter into a three (03) year period agreement for Cybersecurity services to complement the SonicWALL NSA 2600.
  2. The service provider will be required to proactively identify, monitor, and remediate all known and future identified security vulnerabilities in accordance with good practises.
  3. **The scope of work should include the following:** 
     1. Access to the following service provider resources for the duration of the contract:
        1. Project / Account Manager
        2. Cyber security expert(s)
        3. Cyber security remediation expert(s)
     2. Software and Service Capability of the following (the service provider should manage the process and provide supporting reports):
        1. On-going / real-time vulnerability scanning for all devices connected to the SANC network.
        2. Patch management and deployment of remediation services.
        3. Vulnerability management and deployment of remediation services.
        4. Monitoring of the Cybersecurity status.
        5. Reporting of any adverse attempts and incidents.
        6. Reporting on remedial action taken.
        7. Perform comprehensive asset management reporting of the status of all associated devices and/or infrastructure within the SANC environment (including the firewall status).
     3. The service provider will be expected to provide a detailed report which covers the following:
        1. Risk scores (high, medium and low) for each identified vulnerability.
        2. Overall risk score based on the severity of the aggregated identified vulnerability.
        3. Suggested prioritised remedial action implementation approach and plan to rapidly mitigate all identified vulnerabilities.
     4. The service provider’s approach should be as follows:
        1. Prepare:
* Define vulnerability management process scope;
* Define vulnerability management process approach;
* Define roles and responsibilities;
* Selection and deployment of vulnerability assessment method and tools;
* Create and refine the SANC policy and Service Level Agreements (SLAs) for all devices connected to the SANC network; and
* Identify asset (endpoint devices and other relevant infrastructure) context sources.
  + - 1. Assess:
* Identify assets (endpoint devices and other relevant infrastructure); and
* Scan for vulnerabilities.
  + - 1. Prioritise:
* Prioritisation of remedial and preventative activities according to the defined risk framework;
* Identify;
* Remediate;
* Mitigate;
* Contain risk;
* Reassess; and
* Validate remedial success and rescan.
  + - 1. Improve:
* Evaluate metrics;
* Eliminate underlying issues and risks; and
* Evolve policies, processes and SLAs.
  + - 1. Penetration Testing:
* Determine whether the SANC security posture can withstand an intrusion attempt from an advanced attacker with a specific goal. The penetration testing should be executed utilising both external and internal perspectives in order to identify vulnerabilities to possible intrusion. After identifying the intrusion points, the service provider should be able to thwart attacks from external and internal sources and remediate the risks. Provide the SANC with the daily, weekly and monthly security threat reports and remediation plan(s) and activities.
  + 1. Provide the SANC with all software required licenses to be implemented for the three (03) year contracted period.
    2. Attend compulsory performance review meetings quarterly and / or ad-hoc monthly account management meetings when required, take minutes, and provide reports to the SANC Senior Manager: Information, Communication and Technology (ICT) within five (05) working days after such meeting.
    3. Plan, design and execute an ongoing Cyber security user awareness campaign for users of the SANC network and related components.
    4. Plan, prepare, schedule, execute and monitor a measurable Cyber security knowledge and skills transfer to the SANC ICT team.

# **CONTRACT PERIOD**

* 1. The SANC is looking to enter into a contract with a reputable Cybersecurity service provider for a period of three (03) years.

# **SERVICE PROVIDER ORGANISATION DUTIES AND RESPONSIBILITIES**

* 1. The service provider will be required to fully comply with all requirements/deliverables as stipulated in section 3 of this document.

# **DESIRED CONFIDENTIALITY TERMS AND CONDITIONS**

* 1. The successful bidder must strictly treat all SANC’s information with a high degree of confidentiality.
  2. The SANC’s information must not be provided by any means to a third party.
  3. The successful bidder must be compliant with the requirements of the POPI Act.
  4. SANC undertake to maintain confidentiality relating to any unpublished information you supply to us as part of this RFP and will only use any information provided for the purposes of evaluating this RFP.
  5. The South African Nursing Council reserves the right:
     1. To negotiate with one or more preferred bidder(s) identified in the evaluation process, regarding any terms and conditions, including price without offering the same opportunity to any other bidder(s) who has not been awarded the status of the preferred bidder(s),
     2. To carry out site inspections, product evaluations or explanatory meetings in order to verify the nature and quality of the services offered by the bidder(s), whether before or after adjudication of the Bid,
     3. To correct any mistake at any stage of the tender that may have been in the Bid documents or occurred at any stage of the tender process, and
     4. To cancel and/or terminate the tender process at any stage, including after the closing date and/or after presentations have been made, and/or after tenders have been evaluated and/or after the preferred bidder(s) have been notified of their status as such.

# **EVALUATION PROCESS**

* 1. The following qualifying criteria will be used:
     1. **Step 1: Administration Compliance**
        1. The service provider **must** comply with the following requirements:

|  |  |  |
| --- | --- | --- |
| Document that must be submitted | Non-compliance with items against which a “YES” is denoted shall result in disqualification | |
| Invitation to Bid | **YES** | Complete and sign the supplied pro forma document |
| Tax Status  Tax Clearance  Certificate | **YES** | 1. Proof of Registration on the Central Supplier Database 2. In the event where the Bidder submits a hard copy of the Tax Clearance Certificate, the CSD verification outcome will take precedence. |
| Declaration of Interest | **YES** | Complete and sign the supplied pro forma document |
| Preference Point Claim Form | **NO** | Non-submission will lead to a zero (0) score on B-BBEE |
| B-BBEE certificate or sworn affidavit | **NO** | Valid B-BBEE certificate or sworn affidavit  Non-submission will lead to a zero (0) score on B-BBEE |
| Declaration of Bidder’s Past Supply Chain Management Practices | **YES** | Complete and sign the supplied pro forma document |
| Certificate of Independent Bid Determination | **YES** | Complete and sign the supplied pro forma document |
| Registration on Central Supplier Database (CSD) | **YES** | Submit proof of registration. |
| Pricing Schedule | **YES** | Submit full details of the fixed pricing proposal |

* + 1. **Step 2: Functionality**
       1. Only Bidders that have met the mandatory and administrative criteria in step 1 will be evaluated in step 2 for functionality.
       2. Functionality will be evaluated as follows:
          1. Technical Evaluation – Bidders will be evaluated out of **75 points**. Bidders must score a minimum of **50 points** for invitation to presentation
          2. Presentation – Bidders will be evaluated out of **25 points**.
       3. The overall combined score must be equal or above **75 points out of 100 points** in order to proceed to step 3 for Price and B-BBEE evaluation.
       4. The following formula will be used to convert to the points scored against the weight:

****

Where:

Ps = Percentage scored for functionality by bid under

consideration

So = Total score of bid under consideration

Ms = Maximum possible score

* + - 1. The following criteria and weights shall apply when considering bids:

|  |  |  |
| --- | --- | --- |
| Criteria Requirement | Weight | Maximum Score |
| 1. Technical Team Capability:  * Curriculum Vitae’s (CV’s) of the three (03) Proposed Technical Team, detailing a minimum of 5 years’ Experience and a relevant Information Technology Security or related Cyber Security qualifications. Access to the following resources for the duration of the contract:   1. Project Manager / Account Manager CV, reflecting a minimum of five (05) years’ project management / account management experience   2. Provide copies of qualifications (Certificate/Diploma/ Degree in IT/Project Management/Finance/Business Administration) for Project Manager / Account Manager | **Minimum required points (25)**  **04**  **04**  **06**  **06**  **08**  **07** | **35** |
| * 1. Cyber Security expert CV reflecting a minimum of five (05) years’ Cyber Security experience   2. Provide copies of qualifications (Diploma/ Degree in Information Technology/Computer Science or one of the below Certificates: * Certified Information Security Manager (CISM) * Certified Information Systems Security Professional (CISSP) * SANS GIAC Security Essentials (GSEC) * Certified Ethical Hacker (CEH) * Offensive Security Certified Professional (OSCP) * Certified Cloud Security Professional (CCSP)) |
| * 1. Cyber Security Remediation Expert CV reflecting a minimum of five (05) years’ Cyber Security experience   2. Provide copies of qualifications (Diploma/ Degree in Information Technology/Computer Science or one of the below Certificates: * Certified Information Security Manager (CISM) * Certified Information Systems Security Professional (CISSP) * SANS GIAC Security Essentials (GSEC) * Certified Ethical Hacker (CEH) * Offensive Security Certified Professional (OSCP) * Certified Cloud Security Professional (CCSP))   (The CVs and qualifications may be verified by the SANC) |
| 1. Methodology and Project Approach:   2.1 Proposal that addresses the following:  2.1.1 Software, Hardware and Service Capability  (Provide a service capability proposal, software, and hardware to be used)  2.1.2 Risk Management, asset management and reporting (Provide reporting templates)  2.1.3 Vulnerability Assessment and remediation  2.1.4 Penetration Testing, and  2.1.5 Knowledge and skills transfer.  (NB: The service provider is required to provide the SANC with the proposal in line with the above-mentioned activities) | **Minimum required points (20)**  **5**  **5**  **5**  **5**  **5** | **25** |
| 1. Relevant Experience of the Organisation:  * Bidders must attach copies of three (03) reference letters from clients that they have successfully provided Cyber Security services, in the past five (05) years. The reference letters must be in a client’s letterhead, clearly indicating the type of services provided, contract duration, relevant contact person’s name, surname, position, email address & contact number/s   Points Scoring for Reference Letters:   * 0 reference letter * 2 reference letters * 3 reference letters   NB: Should the reference letters fail to have the indicated aspects and the information above not being verifiable, bidders will score zero points. References should not be older than three (03) years. | **0**  **10**  **15** | **15** |
| 1. Presentation on five (5) types of Cyber Security solutions you will provide to the SANC:  * Critical Infrastructure Cybersecurity * Network Security * Cloud Security * Internet of Things Security (IoT) * Application Security | **25** | **25** |
| Total points | | **100** |

* + 1. **Step 3: Price and BBBEE**
       1. Bids will be evaluated in terms of the 80/20 Preference Point System (80 points for price and 20 points for BBBEE).
       2. The following formula will be applied to calculate the points for price:



Where

Ps = Points scored for price of bid under consideration

Pt = Rand value of bid under consideration

Pmin = Rand value of lowest **acceptable** bid

* + - 1. The **following formula will be used to calculate the points for B-BBEE:**
         1. Bids from non-compliant B-BBEE contributors will not be disqualified. Any B-BBEE qualifying contributor who does not submit a substantiating certificate will be allocated zero points, but the bid will not be disqualified.
         2. Points will be awarded to a tenderer for attaining their B-BBEE status level of contributor in accordance with the table below:

|  |  |
| --- | --- |
| B-BBEE Status Level of Contributor | Number of points (80/20) |
| 1 | 20 |
| 2 | 18 |
| 3 | 16 |
| 4 | 12 |
| 5 | 8 |
| 6 | 6 |
| 7 | 4 |
| 8 | 2 |
| Non-compliant contributor | 0 |

**COMPILED BY:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**MR J HATTINGH**

**MANAGER: ICT OPERATIONS**

**DATE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**RECOMMENDED BY: APPROVED BY / NOT APPROVED BY:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**MR M MAKGOLANE DR K KISSOONDUTH**

**SENIOR MANAGER: ICT CORPORATE SERVICES EXECUTIVE**

**DATE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ DATE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ANNEXURE 1: PRICE SCHEDULE**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Description/Item** | **Quantity** | **Fixed price per unit (year one)** | **Total price excluding VAT** | **Total price including VAT** |
| 1. | **Remediation of known risks Provide**   * Fixed price quotation for the once off implementation of the remedial actions / findings for the known risks / threats. |  |  |  |  |
| 2. | **Human Resources:**   * Project Manager / Account Manager, * Cyber security expert, * Cybersecurity remediation expert, |  |  |  |  |
| 3. | **Methodology and Project Approach:**   * Software, Hardware and Service Capability, * Risk Management, asset management and reporting, * Vulnerability Assessment and remediation, * Penetration Testing, and * Knowledge and skills transfer. |  |  |  |  |
| 4. | Software license price as required  (provide detailed information of software, licencing conditions and related information which includes annual software assurance fees). |  |  |  |  |
| 5. | Hardware price if required  (provide detailed information of hardware, operating system, data base software, licencing conditions, and related information).  It must be noted that only hardware which is to be provided by the SANC and which it does not have available for use at this time is to be referenced. |  |  |  |  |
| **Total price for year 1 including VAT (year 1 prices must be fixed)** | | | | | **R** |
| **Total price for year 2 including VAT** | | | | | **R** |
| **Total price for year 3 including VAT** | | | | | **R** |
| **Grand Total for 3 years including VAT** | | | | | **R** |

**NB: PRICING**

**1. The service provider must:**

1.1. Provide a fixed price quotation for the once off implementation of the remedial actions / findings for the known risks / threats, and

1.2. Provide a fixed price quotation for the first year to deliver the services as reflected in section 3 of the TOR.

**2**. **The quotation must be valid for a period of 120 days after the closing date of the RFP, for the following:**

2.1. Provision of Cybersecurity services as per section 3;

2.2. Provision of Project Manager/Account Manager;

2.3. Provision of Cybersecurity Expert(s); and

2.4. Provision of Cybersecurity Remediation Expert(s).