



REQUEST FOR QUOTATIONS

RFQ Name: SUPPLY AND DELIVERY OF MANAGED SECURITY OPERATIONS CENTRE (SOC)

RFQ No: KHC/RFQ/20/2024

Technical Enquires: Mrs B. Sobekiwe

Contact Details: 047 401 6466

Email address: bsobekiwe@kinghintsacollege.edu.za

SCM Enquiries: Ms S. Nongomanzi

Contact No: 047 401 6400/6437

Email address: snongomanzi@kinghintsacollege.edu.za

REQUISITION SPECIFICATION

PLEASE REFER TO THE ATTACHED DOCUMENT FOR FULL SPECIFICATIONS!!!!!!!!!!!!

Important Information:

Please submit the following mandatory compliance documents:

1. Valid SARS Tax Clearance Certificate or pin
2. Copy of Central Supplier database (CSD) report (Full CSD report not summary)
3. Complete the declaration form (SBD 4 form) **(Obtainable from the website)**
4. Copy of Business Registration Document (CIPC)
5. Copy of watchguard Authorization Letter

Please submit the following additional documents to claim points for specific goals

1. Complete the attached SBD 6.1 for preferential points claim as outlined on Specific goals document, **(Obtainable from the website)**
2. Certified copy of ID of director(s), (Certification must not be older than 6 months)

All quotations and compliance documents MUST be emailed to the following address: snongomanzi@kinghintsacollege.edu.za

Closing Date of quotations: 27 August 2024, TIME: 16:30PM

PLEASE NOTE THAT NO LATE QUOTATIONS WILL BE ACCEPTED

REQUISITION SPECIFICATION

No	Item	Qty
1	Managed SOC Service 1 year	1
2	<p>Service must include the below:</p> <p>ZERO TRUST APPLICATION SERVICE 24X7 X365 KHTC looks to embrace the zero-trust model and requires an advanced zero-trust application service, reducing the attack surface and minimizing potential vulnerabilities facing our College.</p> <p>PROACTIVE THREAT HUNTING The service provider must proactively hunt down and neutralize potential threats with their threat-hunting service before they impact on our systems and operations.</p> <p>PROACTIVE & PRIORITISED PATCH MANAGEMENT Not all vulnerabilities are equal in terms of their potential risk. The service provider must prioritize patches based on their criticality, the potential impact on our organization, and the likelihood of exploitation.</p> <p>SUPPORT AND MAINTENANCE: The service provider should provide ongoing technical support and software maintenance for the watchguard endpoint protection, detection and response together with the watch guard patch management technology on the Security Operations Centre.</p> <p>Availability of software updates, bug fixes, and security patches should be included in the support package.</p> <p>DELIVERY AND IMPLEMENTATION: The service provider should: Provide details regarding the estimated delivery time and implementation process. Provide Training and documentation to facilitate the deployment should be included.</p>	<p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p>
3	The service provider must protect and patch all our Endpoints	720