

REQUEST FOR BIDS

BID DETAILS

BID NUMBER:		FB-SETA (24-25) T0006	
CLOSING	Date:	23 April 2025	
	Time:	12:00 pm	
DESCRIPTION:		The appointment of a cyber security service provider for a period of three (3) years.	
TECHNICAL QUERIES			
EMAIL ADDRESS:		scm@foodbev.co.za	
COMPULSORY BRIEFING SESSION:	Date:	04 April 2025	
	Time:	10:00am to 11:00am via Microsoft Teams	
Validity Period		120 Days	

DETAILS OF BIDDER

Organisation /individual:

Contact person:

Telephone/ Cell number:

E-mail address:

TOTAL BID PRICE (inclusive of VAT)

GLOSSARY

AWARD	Conclusion of the procurement process and final notification to the effect to the successful bidder
B-BBEE	Broad-based Black Economic Empowerment in terms of the Broad-based Black Economic Empowerment Act, 2003 (Act No. 53 of 2003) and the Codes of Good Practice issued thereunder by the Department of Trade and Industry
BID	Written offer in a prescribed or stipulated form in response to an invitation by FOODBEV SETA for the provision of goods, works or services
CONTRACTOR	Organisation with whom FOODBEV SETA will conclude a contract and potential service level agreement subsequent to the final award of the contract based on this Request for Bid
CORE TEAM	The core team are those members who fill the non-administrative positions against which the experience will be measured.
DUE DILIGENCE	A verification of information that has been received during application to assess the applicant's operational capacity.
FOODBEV SETA ("FBS")	Food and Beverage Manufacturing Sector Education and Training Authority
ORIGINAL BID	Original document signed in ink, or Copy of original document signed in ink,
ORIGINALLY CERTIFIED	To comply with the principle of originally certified, a document must be both stamped and signed in original ink by a commissioner of oaths.
SCHEDULE 3A ENTITY	As per the classification by National Treasury these refer to other National public entities
SCM	Supply Chain Management
SLA	Service Level Agreement

TABLE OF CONTENTS

GLOSSARY	2
SECTION A	4
1. INTRODUCTION	4
2. PURPOSE	4
3. SCOPE OF WORK	4
4. DELIVERABLES	5
5. PRICING SCHEDULE	5
6. VALIDITY PERIOD	6
SECTION B	6
7. BID EVALUATION PROCESS	6
7.1.1. Stage 1: Administrative Requirements	6
7.1.2. Stage 2: Mandatory Requirement	7
7.1.3. Stage 3: Functionality Evaluation Criteria	7
7.1.4.1. Stage 4: Preference Points system	10
SECTION C	11
8. TENDER SUBMISSION INSTRUCTIONS	11
9. AUTHORISATION	13
10. ANNEXURES	14

INVITATION TO BID FOR THE APPOINTMENT OF A CYBER SECURITY SERVICE PROVIDER FOR A PERIOD OF THREE (3) YEARS.

SECTION A

1. INTRODUCTION

The Food and Beverages Manufacturing SETA (“FoodBev SETA”) is a Schedule 3A Public Entity established in terms of the Skills Development Act 97 of 1998. FoodBev SETA is currently operating in Johannesburg at Number 7 Wessel Road, Rivonia Sandton. FoodBev SETA’s function is to promote, facilitate and incentivize skills development in the Food and Beverages Manufacturing Sector. FoodBev SETA is one of the 21 Sector Education and Training Authorities (SETAs) across the economy mandated to implement the National Skills Development Plan (NSDP) outcomes.

2. PURPOSE

FoodBev SETA seeks proposals from qualified cyber security service providers to implement, manage, and enhance its cyber security posture over a three-year period. The selected provider will ensure compliance, risk mitigation, and proactive defense against evolving cyber threats.

3. SCOPE OF WORK

Bidders must submit a detailed implementation plan outlining how they will deliver the following services:

1. Cyber Security Framework & Compliance
 - a. Align with industry standards (e.g., ISO 27001, NIST, POPIA, GDPR) and regulatory requirements.
 - b. Conduct a gap analysis and propose remediation strategies.
2. Threat & Vulnerability Management
 - a. Proactive risk assessments, threat intelligence, and mitigation strategies.
 - b. Regular vulnerability scanning and penetration testing (internal/external).
3. Security Operations & Monitoring
 - a. 24/7 Security Operations Centre (SOC) services for real-time threat detection.
 - b. Incident response and forensic investigation capabilities.
4. Data Protection & Access Control
 - a. Data encryption, classification, and loss prevention (DLP) strategies.
 - b. Identity and Access Management (IAM) with role-based controls.
5. Security Awareness & Training
 - a. Customized training programs for staff to mitigate phishing and social engineering risks.

- 6. Patch & Configuration Management
 - a. Automated patch deployment and system hardening.
- 7. CISO-as-a-Service (CISOaaS)
 - a. Strategic guidance on cyber governance, policies, and risk management.

4. DELIVERABLES

The successful bidder must provide measurable outcomes, including but not limited to:

- Cyber Security Roadmap (Year 1-3 strategy with clear milestones).
- Quarterly Vulnerability & Penetration Test Reports (with remediation plans).
- Real-time Threat Monitoring & Monthly SOC Reports.
- Incident Response Playbooks and post-incident reviews.
- Annual Security Awareness Training (with pre/post-assessment metrics).
- Compliance Audits against POPIA, ISO 27001
- Quarterly Presentations to the ICT Steering Committee on security posture.
- Monthly Reporting and Quarterly Presentations to the ICT Steering Committee.

5. PRICING SCHEDULE

No.	Item Description	Monthly rate (Year 1)	Monthly rate (Year 2)	Monthly rate (Year 3)	Total rate for 3 years (incl vat)
1.	Cybersecurity Services				
	Monthly rate				
	Vat				
	Total monthly rate				

- a. Bidders must complete the above pricing table for full price evaluation. The table illustrates the price breakdown required, the pricing must be vat inclusive.
- b. Other expenses must be clearly stipulated on an itemised basis
- c. Bidders should indicate number of project team members that they propose for the project

6. VALIDITY PERIOD

The Bidder is required to confirm that it will hold its proposal valid for 120 days from the closing date of the submission of proposals, during which time it will maintain without changing the personnel proposed for the services together with their proposed rates.

SECTION B

7. BID EVALUATION PROCESS

7.1. The Bid evaluation process will be undertaken in accordance with the following staged approach:

Stage 1:	Administrative requirements
Stage 2:	Mandatory Criteria
Stage 3:	Functionality Criteria
Stage 4:	The Preferential Procurement Policy Framework Regulation using the 80:20 points system.

7.1.1. Stage 1: Administrative Requirements

Stage	Criteria	Requirements
Stage 1	Administrative requirements	<p>The potential bidder must submit three (3) copies of the bid proposal as follows: i) Two (2) hard copies ii) One (1) electronic copy in PDF format saved on a USB memory stick</p> <p>Requirements for Hard Copies: i) The bid proposal must be securely bound, hole-punched, and sequentially numbered in accordance with the response format outlined in Section C of this bid document.</p> <p>Requirements for Electronic Copy: ii) The electronic copy must be saved in PDF format on a USB memory stick. iii) The files must be organized into clearly labelled, paginated, and indexed folders in accordance with the response format outlined in Section C of this bid document.</p> <p>Important Note: (a) FBS will not be responsible for any misinterpretation or misplaced information resulting from a proposal that is not properly labelled, paginated, and indexed</p>

7.1.2. Stage 2: Mandatory Requirement

Stage	Criteria	Requirement
Stage 2	Mandatory Requirement	<p>(a) Attendance of a compulsory briefing session. A virtual briefing session will be held from (10:00am) to (11:00am) via Microsoft Teams. The teams meeting link is provided on the FoodBev SETA website under this tender advert. Bidders can also request the meeting link by emailing: scm@foodbev.co.za</p> <p><i>(Failure to adhere to the above mandatory requirement will lead to the disqualification of the bidders bid)</i></p>

7.1.3. Stage 3: Functionality Evaluation Criteria

1. DETAILED FUNCTIONALITY EVALUATION CRITERIA:		WEIGHTING ALLOCATED
1.1. Project Team		
<p>This illustrates the minimum expected resources to be utilised in the project. The bidder must provide an organogram for the team members in the project with a comprehensive CV for each project member, qualifications and certifications.</p> <p>NB: Please note that points will only be awarded if the bidder submits both the CV demonstrating relevant experience, relevant qualifications and all required certifications. If CVs, qualification and certification are not submitted, no points will be allocated</p>		50.00
1.1.1. Project Manager		
<p>Minimum Requirements:</p> <ul style="list-style-type: none"> • NQF level 7 qualification or equivalent • Project Management Professional Certification (PMP) or PRINCE2 (Practitioner) or Certified Scrum Master (CSM) or MPI-ACP (Agile Certified Practitioner) • An abridged CV indicating a minimum of 5 years' ISO 27001 implementation experience. 		15.00
CV submitted demonstrating 5 or more years' experience in ISO 27001 implementation and have the required qualification and certification.		15.00

CV submitted demonstrating a minimum of 3 years but less than 5 years' experience in ISO 27001 implementation and have the required qualification and certification.	10.00	
CV submitted demonstrating a minimum of less than 3 years' experience in ISO 27001 implementation and have the required qualification and certification.	0.00	
1.1.2. Chief Information Security Officer		15.00
Minimum Qualification(s): <ul style="list-style-type: none"> • NQF 7 in computer science or information and communication technology related qualification. • Certification in Certified Information Systems Security Professional (CISSP) or Certified Chief Information Officer (CCSIO) or Certified Information Security Manager (CISM) or CompTIA Advanced Security Practitioner (CASP+) • An abridged CV indicating a minimum of 5 years' experience managing cyber security related projects. 		
CV submitted demonstrating 5 or more years' experience in cyber security related projects and have the required qualification and certification.	15.00	
CV submitted demonstrating a minimum of 3 years but less than 5 years' experience in cyber security related projects and have the required qualification and certification.	10.00	
CV submitted demonstrating less than 3 years' experience in cyber security related projects and have the required qualification and certification.	0.00	
1.1.3. Security Operation Center (SOC) lead		10.00
Minimum Qualification(s): <ul style="list-style-type: none"> • NQF 7 in Computer Science, Cyber Security or Information and Communication Technology related qualification. • Certified in Security+ and CompTIA CySA+ and Certified Ethical Hacker (CEH) • An abridged CV indicating a minimum of 5 years' in technical and management experience in SOC and/or in the field. 		
CV submitted demonstrating 5 or more years' experience in technical and management in SOC or related projects and have the required qualification and certification.	10.00	
CV submitted demonstrating a minimum of 3 years but less than 5 years' experience in technical and management in SOC or related projects and have the required qualification and certification.	5.00	
CV submitted demonstrating a minimum of 1 to 2 years' experience in technical and management in SOC or related projects and have the required qualification and certification.	3.00	
No CVS, qualification and certification submitted	0.00	

1.1.4. Cyber Security Architect		10.00
Minimum Qualification(s):		
<ul style="list-style-type: none"> • NQF 7 in Computer Science, Cyber Security or Information and Communication Technology related qualification • Certification in Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM) or Certified Cloud Security Professional (CCSP) and SABSA or TOGAF/ Microsoft Certified; Cybersecurity Architect Expert or GIAC certifications i.e. GDSA • An abridged CV indicating a minimum of 5 years' experience in cyber security related projects. 		
CV submitted demonstrating 5 or more years' experience in cyber security related projects and have the required qualification and certification.	10.00	
CV submitted demonstrating a minimum of 3 years but less than 5 years' experience in cyber security related projects and have the required qualification and certification.	5.00	
CV submitted demonstrating a minimum of 1 to 2 years' experience in cyber security related projects and have the required qualification and certification.	3.00	
No CVS, qualification and certification submitted	0.00	
2. Experience of the Bidder in Similar Work		
<p>Bidders must provide written reference letters (dated not older than five (5) years) on the bidder's client letterhead, to whom cyber security services are/were provided. The reference letters must include:</p> <ol style="list-style-type: none"> Contact people and contact details. Confirmation of services rendered; and whether the client/s were satisfied with the service rendered The reference letter must be signed and dated. 		30.00
• Three (3) reference letters	30.00	
• Two (2) reference letters	20.00	
• One (1) reference letter	10.00	
• No reference letter	0.00	
3. Methodology and approach		
The proposal should include an implementation plan that demonstrates the bidder's capacity to deliver the project within the stipulated time frame and budget. The proposal should sufficiently cover the scope of the work.		20.00
<ul style="list-style-type: none"> • Excellent: The proposal is unambiguous and demonstrates a thorough understanding of the requirements and provides full details of how each requirement will be met 	20.00	
<ul style="list-style-type: none"> • Good: The proposal meets most of the requirements and is sufficiently detailed to demonstrate a good understanding and provide details of how requirements will be met. 	15.00	

<ul style="list-style-type: none"> • Acceptable: The proposal meets some of the requirements and shows an acceptable level of understanding of requirements and provides some satisfactory level of details on how the requirements will be met. 	10.00	
<ul style="list-style-type: none"> • Unacceptable: The proposal does not meet any of the above requirements or comply with and/or insufficient/no information provided. 	0.00	
TOTAL POINTS		100.00

7.1.4. Bidder must meet the minimum functionality of **75,00** points out of 100 points in order to be evaluated further. Any bid that does not meet the minimum threshold will not move to the next stage of evaluation.

7.1.5. **Stage 4: Preference Points system**

The 80/20 preference points system will be utilized for this bid. This preference points system is for the acquisition of goods or services with a Rand value up to R50 million as follows:

Criteria	Means of verification	Points
Price	Proposed Bid Price	80.00
Preference points	Specific Goals	20.00
Total Points		100.00

7.1.4.2. Specific Goals

The following allocation will determine the specific goals for this tender process

Criteria	% Allocation for each category	Points
Black People Ownership (> 51% blacks)	60%	12.00
Women Ownership	30%	6.00
Black Youth Ownership	10%	2.00
Total Points	100%	20.00

7.1.4.3. Bidders must submit the following documents as a means of verification for specific goals:

- a) CIPC documents (company registration documents),
- b) A copy of a BBBEE verification certificate or signed affidavit indicating ownership levels.

- c) Shareholder certificates, and
- d) Copy(ies) of Identity document(s) for shareholder(s).
- e) Central Supplier Database (CSD) full report. (*Not a summary*)

SECTION C

8. TENDER SUBMISSION INSTRUCTIONS

- 8.1.1. Tenders should be submitted in triplicate consisting of two hard copies and one electronic copy, all bound in a sealed envelope endorsed, **BID NO: FB SETA (24-25) T0006. THE APPOINTMENT OF A CYBER SECURITY SERVICE PROVIDER FOR A PERIOD OF THREE (3) YEARS.** The sealed envelope must be placed and be deposited in the FoodBev SETA Tender Box, Ground Floor, 7 Wessel St, Rivonia, Sandton, 2128 no later than closing time and date.
- 8.1.2. Bids must be submitted in a prescribed response format herewith enclosed as 'Response Format'.
- 8.1.3. The closing date, company name and the return address must also be endorsed on the envelope.
- 8.1.4. If a courier service company is being used for delivery of the tender document, the tender description must be endorsed on the delivery note/courier packaging and the courier must ensure that documents are placed / deposited into the tender box. FoodBev SETA will not be held responsible for any delays where tender documents are handed to the FoodBev SETA Receptionist and/or arrives late.
- 8.1.5. No bids received by telegram, telex, email, facsimile, or similar medium will be considered.
- 8.1.6. Where a tender document is not in the tender box at the time of the tender closing, such a tender document will be regarded as a late tender. FoodBev SETA reserves the right not to consider/evaluate any late tender response.
- 8.1.7. All the documentation submitted in response to this bid must be in English.
- 8.1.8. The bidder is responsible for all the costs that they shall incur related to the preparation and submission of the tender document.
- 8.1.9. Bids submitted by bidders must be signed by a person or persons duly authorised thereto by a resolution of a Board of Directors (if applicable), a copy of which Resolution, duly certified be submitted with the Tender
- 8.1.10. Bidders should check the numbers of the pages to satisfy themselves that none are missing or duplicated. No liability will be accepted by FoodBev SETA regarding anything arising from the fact that pages are missing or duplicated.
- 8.1.11. A valid tax clearance certificate or confirmation of pin must be included in the bid response.
- 8.1.12. A copy(s) of certificates from the organizations/ bodies that the bidder is affiliated to must be included in the bid response.
- 8.1.13. FoodBev SETA reserves the right to call bidders for further presentations before awarding.

8.1.14. The onus is on the bidder to provide FB SETA with SAQA evaluation for foreign qualifications. Foreign qualifications not accompanied by SAQA evaluation will not be considered.

8.2. RESPONSE FORMAT

8.2.1. Bidders are requested to note that this is a guidance to responding to the evaluation criteria as detailed above. The soft and hard copy responses from all bidders must be prepared in line with the following section (each schedule must be clearly marked, indexed and /or numbered):

8.2.2. Cover Page: The cover page must clearly indicate the bid reference number, bid description and the bidder's name.

8.2.3. Schedule 1:

8.2.3.1. Executive Summary/Cover Letter – The cover letter should be brief (not more than two pages maximum). Describe why your company/consortium considers it to be best qualified to achieve any of the services listed in scope of work

8.2.3.2. Brief company profile

8.2.3.3. Qualifications and Experience – This section shall contain relevant information on qualifications and experience related to the relevant profession.

8.2.3.4. List of Project team – This list should include the identification of the contact person who will have primary responsibility for the FoodBev SETA contracts, other personnel to be used for project planning, documentation, and supervision, including partners and/or sub-consultants.

8.2.3.5. Reference letters in previous client's letterhead, signed and dated by authorized personnel.

8.2.3.6. Methodology and approach including an implementation plan that demonstrates the bidder's capacity to deliver the project within the stipulated time frame and budget

8.2.3.7. Signature Requirements: All bids must be signed. A bid may be signed by an officer or other agent of a registered vendor, if authorised to sign contracts on its behalf; a member of a consortium or joint venture or other agent authorised by a Power of Attorney. The name and title of the individual(s) signing the bid must be clearly shown immediately below the signature.

8.2.3.8. Rejection of bids: FoodBev SETA reserves the right not to proceed with the award of the proposal.

8.2.4. Schedule 2:

- 8.2.4.1. Valid tax clearance certificate
- 8.2.4.2. Certified copies of the bidders CIPC / or company registration documents listing all members with percentages, in case of a CC. Or latest certified copies of all share certificates in case of a company.
- 8.2.4.3. Original certified copy of the company’s professional accreditation (not a certified copy)
- 8.2.4.4. Certified ID copies of all directors.
- 8.2.4.5. A certified copy of the B-BBEE certificate (or an original affidavit signed by a Commissioner of Oaths regarding the B-BBEE status)
- 8.2.4.6. Submission of proof of the bidder’s registration on the CSD (Full report)
- 8.2.4.7. All tender submissions must include standard bidding documents (SBD documents) duly completed and signed.

Note: If a Consortium, Joint Venture or Subcontractor, the documents listed above must be submitted for each Consortium/ JV member or subcontractor. A consolidated B-BBEE certificate is required for Joint Venture bidders.

9. AUTHORISATION

The BAC committee hereby confirms that the information included in this bid document is agreed upon by all members, compliant, accurate and complete.

SIGNATORIES:

Recommended by the BAC Chairperson: Mr Sinaye Mgidi

Signature: _____ Date: _____

Approved by the CEO: Ms Nokuthula Selamolela

Signature: _____ Date: _____

10. ANNEXURES

ANNEXURE A - GENERAL CONDITIONS OF CONTRACT (GCC)

ANNEXURE B –COMPLIANCE DOCUMENTS AND CONDITIONS TO TENDER

ANNEXURE C- SBD FORMS