

REQUEST FOR INFORMATION

RFI NUMBER:	JW RFI 19 07 2024	CLOSING DATE:	26 July 2024 @16H00
DESCRIPTION:	PROVIDE ONLINE CYBERSECURITY TRAINING AND BRANDED MATERIAL.		
ISSUE DATE	19 JULY 2024		
Submit via Email to:	Sinna.hlongwane@jwater.co.za		

ENQUIRIES MAY BE DIRECTED TO:

Bidding procedure enquiries <u>must</u> be sent to		Technical enquiries must be directed to	
CONTACT PERSON	Sinna Hlongwane	CONTACT PERSON	Rubens da Silva
TELEPHONE NUMBER	011 688 1410	TELEPHONE NUMBER	011 688 6666
E-MAIL ADDRESS (Submissions must be made to this address)	Sinna.hlongwane@jwater.co.za	E-MAIL ADDRESS	rubens.dasilva@jwater.co.za

SUPPLIER INFORMATION

NAME OF BIDDER			
STREET ADDRESS			
TELEPHONE NUMBER	CODE		NUMBER
CELLPHONE NUMBER			
E-MAIL ADDRESS			
VAT REGISTRATION NUMBER			
CENTRAL SUPPLIER DATABASE No:	MAAA		
MANUFACUTER OR THIRD PARTY (If Applicable)			

1. PURPOSE OF THE REQUEST FOR INFORMATION

Johannesburg Water invites service providers to submit a request for information proposal to provide online cybersecurity training and branded training material for a period of thirty-six (36) months. This RFI is strictly to solicit financial information from potential bidder(s) for the online cybersecurity training and branded training material for a period of thirty-six (36) months. This RFI does not constitute; an offer; or any impression none so ever to do business with Johannesburg Water. The RFI response proposals is enquired to assist the organisation with business decision making purposes.

2. BACKGROUND

Johannesburg Water invites service providers to respond to a Request for Information to provide **ONLINE CYBERSECURITY TRAINING AND BRANDED TRAINING MATERIAL**. This RFI is strictly to solicit market related information from potential bidder(s). This RFI does not constitute; an offer; or any impression none so ever to do business with Johannesburg Water.

3. SCOPE OF WORK AND SPECIFICATIONS

The scope of work shall be the following:

1. Provide cybersecurity training through an online platform accessible via the Internet. The platform must be secured, and access controlled via a registered username and password or via a password less link (email). Only employees of Johannesburg Water, including Board members, are permitted to access the online cybersecurity training. The training must accommodate 1500 employees.
2. The cybersecurity training must be structured around themes. A training theme will run over a period of three (3) months. The training should cover at least (minimum) the following cybersecurity topics:
 - Phishing attacks
 - Ransomware
 - Removable media
 - Passwords and authentication
 - Physical security
 - Mobile device security
 - Working remotely
 - Public Wi-Fi
 - Cloud security

- Social media use
- Data protection and privacy
- Internet and email use
- Social engineering, and
- Security at home

Note. A theme may combine different topics, e.g. Working remotely and Social engineering. The volume of content for any theme will be planned upfront for the quarter.

3. Training reports. The platform must provide reporting capability on the cybersecurity training. The reports must be downloadable (exportable) and support the following formats: .pdf or .csv. The training reports can be filtered based on the following criterion:
 - Training theme
 - Individual user
 - User department, e.g. Supply Chain
 - Company
 - Risk profile
 - Completed or uncompleted training
 - Date range
4. Risk Rating. The platform must provide Risk Rating information in respect of training activity and responses, and responses to phishing scams. The Risk Rating must be granular; company, department, and individual.
5. Training Alert Notification. The platform must support Training Alert Notifications, Managers receive alerts on training progress for their department and similarly, users receive email notifications on training events such as upcoming training, training completed, etc.
6. Training content. The training can consist of a combination of different content such as videos, quizzes, games, policy documents, etc.
7. Phishing scams and simulated attacks. The training platform must be able to simulate a phishing attack and provide reports on the simulated attacks.
8. The training platform must provide individual, department and company-wide, risk assessments based on training completed, simulated phishing attacks, etc.

9. Onsite cybersecurity training awareness sessions for Employees. The service provider must develop and provide twelve (12) onsite cybersecurity sessions at Johannesburg Water's Head Office. The sessions can cover any topic or theme on cybersecurity. The sessions should not exceed two (2) hours.
- Note. Multiple sessions will need to be held on the day to accommodate staff's availability and working hours. Therefore, the service provider will be expected to provide 2-3 sessions a day.
10. Onsite cybersecurity awareness session for Executives. The service provider must develop and provide six (6) Cybersecurity awareness sessions for the Executive team over the duration of the contract (twice a year). The sessions can cover any topic or theme on cybersecurity. The sessions should not exceed two (2) hours and are to be held at Johannesburg Water's Head Office.
11. Branded cybersecurity material (electronic). The service provider will be required to design and develop electronic branded material on cybersecurity. The branded material must include:
- Desktop wallpaper. The design of the wallpaper must conform to Johannesburg Water's Communications standards and aligned to the cybersecurity training theme and topics for the quarter.
 - Quantity: 12 Desktop wallpapers over the duration of the contract (one per quarter, i.e. one every three (3) months).
12. Branded cybersecurity material (printed). The service provider will be required to design, and supply printed branded material (posters) on cybersecurity. The posters must conform to the following specifications:
- Material: Colour and glossy finishing
 - Size: A4
 - Quantity: 100 posters per quarter.
- Note. The design of the posters must be aligned to the cybersecurity theme and topics for the quarter.
13. Training gifts. The service provider will be required to supply training gifts for top achievers in the cybersecurity training. The gifts can comprise:
- Buttons

- Mugs
- Coasters
- Keychains
- Pens
- Box of mints

4. PRICING SCHEDULE

Prices must include transport, labour, and any other costs.

SCHEDULE 1 – CYBERSECURITY ONLINE TRAINING PLATFORM

#	Description	UNIT PRICE EXCL VAT	PRICE INCLUDE VAT	UNIT PRICE INCL VAT
1	<p>Provide an online Cybersecurity training platform accessible via the Internet. The platform must support 1500 users. The Cybersecurity training must cover, minimum, the following topics:</p> <ul style="list-style-type: none">• Phishing attacks• Ransomware• Removable media• Passwords and authentication• Physical security• Mobile device security• Working remotely• Public Wi-Fi• Cloud security• Social media use• Data protection and privacy• Internet and email use• Social engineering, and• Security at home			

	Note. The platform must include training reports and simulated phishing scams as per Scope of Work and Specification.			
--	---	--	--	--

SCHEDULE 2 – ONSITE CYBERSECURITY AWARENESS SESSIONS

#	Description	UNIT PRICE EXCL VAT	VAT @ 15%	UNIT PRICE INCL VAT
1	<p>Onsite cybersecurity training awareness sessions for Employees. The service provider must develop and provide onsite Cybersecurity sessions at Johannesburg Water's Head Office. The sessions can cover any topic or theme on cybersecurity. The sessions should not exceed two (2) hours.</p> <p>Note. Multiple sessions will need to be held on the day to accommodate staff's availability and working hours. Therefore, the service provider will be expected to provide 2-3 sessions on the planned day.</p>			
2	<p>Onsite cybersecurity awareness session for Executives. The service provider must develop and provide Cybersecurity awareness sessions for the Executive team over the duration of the contract (twice a year). The sessions can cover any topic or theme on cybersecurity.</p> <p>The sessions should not exceed two (2) hours and are to be held at Johannesburg Water's Head Office.</p>			

SCHEDULE 3 – BRANDED CYBERSECURITY MATERIAL

#	Description	UNIT PRICE EXCL VAT	VAT @ 15%	UNIT PRICE INCL VAT
1	<p>Branded cybersecurity material (electronic). The service provider will be required to design and develop electronic branded material on cybersecurity. The branded material must include:</p> <p>Desktop wallpaper. The design of the wallpaper must conform to Johannesburg Water's Communications standards and aligned to the cybersecurity training theme and topics for the quarter.</p> <p>Note. One desktop wallpaper per quarter, i.e. one every three (3) months.</p>			
2	<p>Branded cybersecurity material (printed). The service provider will be required to design, and supply printed branded material (posters) on cybersecurity. The posters must conform to the following specifications:</p> <ul style="list-style-type: none"> • Material: Colour and glossy finishing • Size: A4 <p>Note. The design of the posters must be aligned to the cybersecurity theme and topics for the quarter.</p>			

4. SCHEDULE 4 – BRANDED CYBERSECURITY TRAINING GIFTS

The training gifts will be handed out to the top training achievers.

#	Description	UNIT PRICE EXCL VAT	VAT @ 15%	UNIT PRICE INCL VAT
1	Button			
2	Mug			
3	Coaster			
4	Keychain			
5	Pen			
6	Box of mints			
7	Subtotal:	-		

5. SUPPLIER COMPANY DETAILS

Suppliers to complete the below according to their company details.

INFORMATION FOR SPECIFIC GOALS ANALYSIS	
BUSINESS OWNED BY 51% OR MORE -BLACK PEOPLE	
1. Percentage (%) of Black Ownership)	
2. Is Black Ownership 51% or more? (Yes or No)	
BUSINESS OWNED BY 51% OR MORE – BLACK YOUTH	
3. Percentage (%) of Ownership by Black Youth	
4. Is the percentage of Black Youth Ownership 51 % or more? (Yes or No)	
BUSINESS OWNED BY 51% OR MORE-WOMEN	
5. Percentage (%) of Ownership by People who are Women	
6. Is the percentage of People who are Women 51 % or more? (Yes or No)	
BUSINESSES LOCATED WITHIN THE BOUNDARIES OF A REGION IN COJ, COJ MUNICIPALITY OR IN GAUTENG PROVINCE	
7. Is your business located in the Gauteng Province? (Yes or No)	
8. Is your business located in the COJ Municipality? (Yes or No)	
9. Is your business located within the region of the COJ? (Yes or No)	
BUSINESS OWNED BY 51% OR MORE - BLACK PEOPLE WHO ARE MILITARY VETERANS	
10. Percentage (%) of Ownership by Black People Who Are Military Veterans	
11. Is the percentage of Ownership by Black People Who Are Military Veterans 51% or more? (Yes or No)	
BUSINESS OWNED BY 51% OR MORE-BLACK PEOPLE WITH DISABILITIES	
12. Percentage (%) of Ownership by Black People With Disabilities	
13. Is the percentage of Ownership by Black People with Disabilities 51% or more? (Yes or No)	
SMME (AN EME OR QSE) OWNED BY 51% OR MORE - BLACK PEOPLE	
14. What is the Enterprise Type? EME – turnover is less than R10m QSE – Turnover between R10m and R50m Generic – Turnover is R50M of more	

JOINT VENTURE (JV), CONSORTIUM OR EQUIVALENT	
15. What is the percentage (%) of ownership for each party?	
SUBCONTRACTING WITH COMPANIES AT LEAST 51% OWNED BY HISTORICALLY DISADVANTAGED INDIVIDUAL (HDI) GROUPS MENTIONED ABOVE	
16. What is the percentage (%) that will be sub-contracted to companies that are at least 51% owned by Historically Disadvantaged Individual (HDI) groups mentioned above?	

6. INFORMATION PRICE BREAKDOWN

DESCRIPTION	BREAKDOWN IN PERCENTAGE	APPLICABLE INDEX	IMPACTED BY ROE (YES/NO)
Raw materials			
Direct Labour			
Direct Overheads			
Transport			
Indirect Labour			
Indirect Overheads			

Total	100%		

provide the following information (if Applicable)

TYPICAL PRICE ADJUSTMENT FORMULA INCLUDING INTERVALS

SUBMITTED DOCUMENTATION IN SUPPORT OF A REQUEST FOR A PRICE ADJUSTMENT

SOURCE OF RAW MATERIAL	
DESCRIPTION	COUNTRY OF ORIGIN
Raw materials	

ASSOCIATED RISKS	
RISK CATEGORY	RISK MITIGATION
Economic:	
Security of Supply	
Supply and Demand	
Rate of Exchange	
Operational:	
Capacity	
Logistics	