

THE NATIONAL CREDIT REGULATOR

NOVEMBER 2023

**TERMS OF REFERENCE FOR THE APPOINTMENT OF A
SERVICE PROVIDER FOR THE RENEWAL OF TREND CYBER
SECURITY SOLUTION FOR 3 YEARS.**

RFP NUMBER: NCR 884.11.2023

**DUE DATE: 08 DECEMBER 2023 AT 11H00
SHARP CAT
HAND DELIVERY TO NCR OFFICES**

SECTION 1

GENERAL TERMS OF CONDITIONS

1. General Information for Bidders

The National Credit Regulator (NCR) was established in terms of Section 12 (1) of the National Credit Act (Act 34 of 2005) and came into being on 1 June 2006.

The NCR will determine which bidding organisation (“bid participant”), if any, is appointed in response to this request for submission as stipulated in section 2 of this document.

1.1. General Terms

This tender is issued in terms of the Public Finance Management Act 1 of 1999 (PFMA), the Preferential Procurement Policy Framework Act 5 of 2000 (PPPFA), the Preferential Procurement Regulations, 2017 (PPR), Supply Chain Management Regulations issued by the National Treasury and BBBEE Act.

Parties that wish to submit proposals are required to indicate that they are willing to accept the General Conditions and Procedures of the NCR (see Section 4 below and Annexure B.1). Please read this document carefully prior to submitting your proposal.

1.2. The Proposal Format

1.2.1. Economy of proposal preparation

The proposal should be prepared simply and economically, providing a straightforward and concise description of the bid participant’s ability to meet the requirements of the proposal request.

Clear factual responses are required. The content of the proposals shall determine the merit of each participant, not brochures or other marketing material. To facilitate the review of proposals, participants are required to organise their responses according to the format presented below. Should a participant wish to provide additional information, that information should be referred to, and provided for, in a file of Annexures.

1.2.2. Validity of proposals

The proposals must include a statement as to the period for which the proposal remains valid. The proposal must be valid for at least ninety (90) days from the due date for the submission of all bids. Refer to the quarters in the terms of reference (TOR).

1.2.3. Number of proposals

Each bid participant must provide **two (2) hard copies and 1 memory stick** of their entire

proposal, including all the documentation referred to in 4 below, in the format specified in that section. All submitted proposals will become the property of the NCR, and will not be returned. Receipt of all proposals will be recorded in a register at the point of receipt. One copy of the proposal must be signed and dated in black ink by the bidder or authorized representative of the bidder and initialled on each page.

2. Submission of proposals

2.1. Proposals must reach the offices of the NCR before **11:00 on 08 December 2023, @11H00am** and must be enclosed in a sealed envelope which must be clearly labelled/addressed on the outside:

(a) RFP No: NCR 884.11.2023

(b) TERMS OF REFERENCE FOR THE APPOINTMENT OF A SERVICE PROVIDER FOR THE RENEWAL OF TREND CYBER SECURITY SOLUTION FOR 3 YEARS

(c) CLOSING DATE: 0 DECEMBER 2023 AT 11H00 SHARP

2.2. Proposals are to be submitted in the marked tender box, in the reception area, National Credit Regulator, 127-15th Road, Randjiespark, Halfway House, Midrand. The tender box will only be available for the depositing of proposals between 08h00 and 16h30 on weekdays (excluding public holidays).

2.3. Please note that this RFP closes punctually at **11h00 on 08 DECEMBER 2023**. No late submissions will be considered under any circumstances.

2.4. All the documentation referred to in Section 4 below must be submitted. Failure to submit all the documentation referred to in this section may result in a submission being discarded, and not considered for evaluation.

2.5. If responses are not delivered as stipulated in this Section 2.1, such responses will be considered “late”, and will not be considered for evaluation.

2.6. The NCR shall not disclose any details pertaining to the responses received, to any other participant, as this is regarded as confidential information.

2.7. Envelopes must not contain documents relating to any RFP other than the one referred to in this RFP.

2.8. The responses to the RFP will be opened as soon as is practical after the expiry of the time advertised for receiving them.

2.9. Only the participants that are short-listed after the evaluation process will be informed of the results of the submission adjudication process.

- 2.10.** After the evaluation process is completed, the Evaluation Committee may, prior to making a final selection, draw up a shortlist of participants and require them to make a detailed presentation to the Adjudication Committee. A minimum of 2 days' notice will be given to relevant participants in advance of the presentation date.

3. Timetable

Date	Activity
17/11/2023	Advertisement of the RFP
08/12/2023	Closing date @ 11h00
08/12/2023	Preliminary evaluation
11/12/2023	Evaluations by the Evaluation Committee
24/01/2024	Adjudication Committee meeting
01/02/2024	Appointment

The National Credit Regulator reserves the right to determine the structure of the process, the right to determine the number of short-listed participants, the right to withdraw from the proposal process, and the right to change this timetable at any time without notice.

4. Documentation to be submitted.

Please Note

All of the documentation described below must be submitted, with no omissions whatsoever. Where a particular form or format of documentation is stipulated, this is the only form or format in which these documents must be submitted. Failure to adhere to these requirements may result in the rejection of the entire submission.

All of the documentation referred to below (in Parts One – Eleven) must be acknowledged and submitted. For ease of reference and to facilitate the evaluation process, you are requested to clearly mark each part of the submitted documentation as it is referred to below.

4.1. Table of content

Introductory letter by the bidder with authorized contact person and details for this specific tender

4.2. SBD 1 – should be the completed and inserted after the introductory letter

One – Proposal drafted in response to Terms of Reference

Section 2 of this document below, contains the terms of reference (TOR) for the above

mentioned tender. Bid participants are required to draft a proposal that will clearly indicate to the Evaluation Committee how they will fulfil the requirements as set out in the TOR.

Bid participants should include the following information when drafting their proposals:

- Proposals should make clear the relevant skills, experience and capacity of the participant, in respect of this particular TOR. This is an important evaluation criterion. Bid participants should ensure that their proposals focus on how they will address the requirements of this TOR, rather than on achievements.
- Proposals must contain the details of the proposed approach to be adopted in order to deliver the service in accordance with the TOR.
- Proposals should clearly indicate whether or not bid participants have the internal capacity to meet the requirements of the TOR.

4.3. One – Pricing Proposal- SEPERATE ENVELOPE

SBD 3.1 Pricing Schedule together with signed off detailed pricing on the company's letter head. They must be completed on the original and signed, all in black ink. Forms with photocopies and/or other reproductions of signatures may be rejected. Additional information may be added on a separate page if necessary.

The total price that the participant will charge to deliver services in accordance with the TOR must be clearly indicated. The pricing proposal should contain sufficient information to allow the Evaluation Committee to estimate the cost of the service, to a high degree of accuracy.

Please note that a financial proposal must be submitted in a separate sealed envelope together with your submission. The financial Proposal will be opened once all technical proposals have been evaluated. This appointment will be made in line with QBS. All prices provided must be inclusive of Value-Added Tax (VAT).

Please note that the prices contained in the pricing proposal are the only charges that may be levied if the participant's proposal is successful, unless explicitly agreed to in writing by the National Credit Regulator, and in terms of the General Conditions of Contract, no additional cost will be accepted after the bidding documents have been submitted and the tender closing date has expired. Any cost for additional parts and peripherals needed for the successful implementation of the project shall remain and form part of the bidding price.

4.4. Three – General Conditions and Procedures of the NCR

Annexure B and B1 - General Conditions and Procedures of the NCR. Bid participants must indicate clearly that they have read this document, and have no objections to being bound by its contents. In cases where any provisions of the General Conditions and Procedures

conflict with this General Information for Bidders and/or Terms of Reference, the latter will take precedence over the General Conditions of Contract.

4.5. Four – Contract Form: Rendering of Services

Annexure C - Contract Form: Rendering of Services. This will only be completed by the successful bidder once a selection has been made by NCR. Participants do not, therefore, need to complete this form at the bidding stage but their proposals must clearly indicate that they have read this form, and have no objections to signing it as is, if selected as the successful participant.

4.6. Five – Tax status

Annexure D - Please attach CSD showing Tax status

A CSD print out must also be attached.

4.7. Six – Preference Points Claim Form

Annexure E – form SBD 6.1. Bid participants must complete Sections 8 and 9 in full. DO NOT RETYPE THESE FORMS. They must be completed on the original and signed, all in black ink. Forms with photocopies and/or other reproductions of signatures may be rejected. *## Please note that a **BBEE certificate/ sworn affidavit** must also be attached to the bid documents*

The following pointers are key in determining the validity of a sworn affidavit:

- Name/s of deponent as they appear in the identity document and the identity number.
- Designation of the deponent as either the director, owner or member must be indicated in order to know that person is duly authorised to depose of an affidavit
- Name of enterprise as per enterprise registration documents issued by the CIPC, where applicable, and enterprise business address.
- Percentage of black ownership, black female ownership and designated group. In the case of specialised enterprises as per Statement 004, the percentage of black beneficiaries must be reflected.
- Indicate total revenue for the year under review and whether it is based on audited financial statements or management account.
- Financial year end as per the enterprise's registration documents, which was used to determine the total revenue.
- B-BBEE Status level. An enterprise can only have one status level.
- Empowering supplier status must be indicated. For QSEs, the deponent must select the basis for the empowering supplier status.
- Date deponent signed and date of Commissioner of Oath must be the same.

- Commissioner of Oath cannot be an employee or ex officio of the enterprise because, a person cannot by law, commission a sworn affidavit in which they have an interest.

4.8. Seven – Declaration of Interest

Annexure F – form SBD 4. DO NOT RETYPE THESE FORMS. They must be completed on the original and signed, all in black ink. Forms with photocopies and/or other reproductions of signatures may be rejected.

4.9. Eight – Non-Disclosure Agreement

Annexure G – Non-Disclosure Agreement. Participants must indicate clearly that they have read this agreement, and have no objections to signing it, as is.

4.10. nine – SLA draft version for supplier review

Annexure H – SLA draft version for supplier review. The participants must indicate clearly that they have read this agreement, and have no objections to signing it, as is. If not objections should be outlined separately in a letter. NB: all the SBD documents can be downloaded from our website - <https://www.ncr.org.za/tenders-download/current-tenders>

4.11. Pre-qualification Criteria

Without limiting the generality of the NCR's other critical requirements for this Bid, bidders must submit the documents listed in **Table 1** below. All documents must be completed and signed by the duly authorised representative of the prospective bidders. During this phase, Bidders' responses will be evaluated based on compliance with the listed administration and mandatory bid requirements. The bidders' proposals may be disqualified for non-submission of any of the documents.

Table 1: Documents that must be submitted for Pre-qualification

Document that must be Submitted	Guideline		Consequence of Non-submission
Invitation to Bid – SBD 1	Yes	Complete and sign the supplied pro forma document	Disqualification from process
Tax status SBD 1	Yes	Written confirmation that SARS may on an ongoing basis during the	Disqualification from process

Document that must be Submitted		Guideline	Consequence of Non-submission
		<p>tenure of the contract disclose the bidder's tax compliance status.</p> <p>Proof of Registration on the Central Supplier Database</p> <p>Vendor number</p>	
Declaration of Interest – SBD 4	Yes	Complete and sign the supplied pro forma document	Disqualification from process
Preference Point Claim Form – SBD 6.1	Yes	Non-submission will lead to a zero (0) score on Specific goals	Zero points awarded for specific goals
Registration on Central Supplier Database (CSD)	Yes	<p>The Service Provider must be registered as a service provider on the Central Supplier Database (CSD). If not registered, to complete the registration of company prior to submitting the proposal.</p> <p>Visit https://secure.csd.gov.za/ to obtain your vendor number starting with MAAA. Submit proof of registration.</p>	Disqualification from process
Pricing Schedule SBD 3.1	Yes	Submit full details of the pricing proposal in a separate envelope	Disqualification from process
General terms and conditions	Yes	Bidders are required to read and accept the terms as outlined	Disqualification from process

5. Evaluation Criteria

Proposals will be evaluated on the 80/20 preference points scoring system: that is, 80% of the points awarded will be based on price, as indicated in the table below; and 20% of the points awarded will be based on specific goals, allocated as indicated in the table below:

B-BBEE status level of contributor	Specific goals	Price
Total maximum points	20	80

The points system is outlined for the 80/20 and 90/10 to address the preferential procurement as followed:

Specific goals and price points based on 80/20 score calculation.

1.1 SMME's which are owned by Black people

SPECIFIC GOAL	ACHIEVEMENT LEVEL	TOTAL NUMBER OF
Persons historically disadvantaged on the basis of race	81%- 100% black ownership	7
	51% - 80% black ownership	5
	31% - 50% black ownership	3
	0 – 30% black ownership	1

1.2 SMME's which are owned by People with disability

SPECIFIC GOAL	OWNERSHIP LEVEL	POINTS
Persons historically disadvantaged on the basis of disability	50 %- 100% owned by persons living with disabilities	3
	30% - 49% owned by persons living with disabilities	2
	0 – 29% owned by persons living with disabilities	1

1.3 SMME's which are owned by Women.

SPECIFIC GOAL	ACHIEVEMENT LEVEL	POINTS
Persons historically disadvantaged on the basis of gender – Women	81% - 100% owned by women	7
	51% - 80% owned by women	5

	31% - 50% owned by women	3
	0 – 30% owned by women	1

1.4 SMME's which are Youth owned business.

SPECIFIC GOAL	OWNERSHIP LEVEL	POINTS
Persons historically disadvantaged based on age	50%- 100% owned by persons who are youth	3
	30% - 49% owned by persons who are youth	2
	0 – 29% owned by persons who are youth	1

Functionality will be evaluated in terms of Section 2 point 4

NB: FIRMS THAT MEET THE BELOW PERCENTAGE ARE ENCOURAGED TO TENDER:

KEY JOINT PERFORMANCE INDICATOR:			
INDICATOR	YES	NO	ATTACH EVIDENCE
40% owned by women			
40% owned by youth			
100% SA companies			
Share certificate			
ID Copies stamped by the commissioner of oath			
Sworn affidavits			
BBBEE certificates			

6. Conflict of interest

Service providers are required to provide services that are professional, objective and impartial. Service providers must ensure that there is no conflict of interest between existing assignments, obligations and responsibilities to other clients and the services set out in the TOR. In the event of any uncertainty in this regard, full disclosure in the submitted proposal

should be considered. Non-disclosure of a conflict of interest may be grounds for termination of any contract.

7. Confidentiality agreement

The successful service provider may have access to confidential data or information. The appointment of a successful bidder is subject to that bidder agreeing to the contents of, and signing, the NCR's standard Non-Disclosure Agreement.

8. Contact details

This no-contact policy does not apply to any information deemed to be in the public domain, or which is readily available from organs of State, which are repositories of such information. All communications and enquiries/requests for clarification relating to this proposal should be directed to procurement@ncr.org.za.

Fraud / Anti-Corruption Hotline

**Report any incidents of wrong doing
to the KPMG Ethics Line**

0800 20 53 17 (Toll Free)

SECTION 2

TERMS OF REFERENCE (TOR)

1. BACKGROUND:

The NCR has adopted Trend Micro cybersecurity solution as its standard choice, driven by the evident advantages it offers. Over the past three years, Trend Micro solution has consistently demonstrated its effectiveness and efficiency against evolving threats, aligning seamlessly with the NCR's stringent security benchmarks.

As the current licensing period approaches its expiration date, the need to renew it has become crucial. Ensuring uninterrupted security coverage is paramount, prompting the requirement for timely renewal.

2. SCOPE OF WORK:

NCR is herein inviting a qualified and accredited Trend Micro Service Provider and / or Partner to renew its Anti-Virus Software Licenses and provide managed services for a period of three (3) years.

3. OBJECTIVES:

The following objectives to be met through this service:

- Managed support on the Cyber Security solution, Deployment, Configuration & Maintenance
- Reduce the risk of virus outbreaks within National Credit Regulator network through early detection and removal of viruses using preventative and detection technology.
- Response to virus alerts, malware, spyware, callbacks and behavioral triggers.
- Knowledge Transfer and Cyber Security awareness and training
- Quarterly Cyber Security Awareness and Training – both Online and Physical;

4. TECHNICAL EVALUATION CRITERIA

CATEGORY	DESCRIPTION	WEIGHT (%)
Compliance and Certifications	Valid Proof of Accreditation with Trend Micro must be submitted. - Valid Accreditation submitted = 5 - No valid accreditation submitted = 0	20
Experience and Expertise of the Support & Maintenance Team Leader	The bidder must provide at least 1 CV of Team Leader who will be responsible for the Trend Cyber Security Support Services and Maintenance Project in partnership with Trend Micro OEM. 1. Availability of Team Leader: >1 Team Leader provided = 5 points 1 Team Leader provided = 4 points; 0 Team Leader provided = 0 points; 2. Experience (implementation and support & maintenance of Trend Micro Solution) of Resources: > 4 years = 5 points; 3 -4 years = 4 points; 2-3 years = 3 points; 1-2 years = 2 points; 1 year = 1 points; Less than 1 year = 0 points;	30
Experience and Expertise of the Support & Maintenance Consultants	The bidder must provide at least 3 CVs of consultants with relevant ICT Security Qualification (Trend Micro will be an advantage): 1. Qualifications of Consultants: > 3 Consultant provided have accredited ICT Security qualification / Trend Micro = 5 points; 2 – 3 Consultants provided have accredited ICT Security qualification / Trend Micro = 4 points; 1 - 2 Consultants provided have accredited ICT Security qualification / Trend Micro = 3 points; 1 Consultant provided have accredited ICT Security qualification / Trend Micro = 2 points;	10

	0 Consultant provided have accredited ICT Security qualification / Trend Micro = 0 points	
Portfolio and Track record	<p>The service provider must submit at least four (4) signed reference letters on the client letterhead for the last 5 years where the Trend Cyber Security Support and license renewal service were provided.</p> <p>Bidder submitted more than 4 reference letters =5 Bidder submitted 4 reference letters =4 Bidder submitted 3 reference letters =3 Bidders submitted 2 reference letter =2 Bidders submitted 1 reference letter =1</p> <p>If no information is provided a scoring of zero will be allocated.</p>	30
Training and Knowledge Transfer	<p>Assess the service provider's plan for training internal teams on security best practices and technologies.</p> <p>A. Plan must include Training Content (relevant to TOR), B. Delivery methods (workshops, webinars etc.), C. Expertise of trainers, D. Participant feedback (assessments, surveys) and Timelines (when, where, how).</p> <ul style="list-style-type: none"> - Plan includes all four (4) of the above-mentioned aspects (A to D) of the skills transfer = 5 - Plan only includes 3 of the above-mentioned aspects = 4 - Plan only includes 2 of the above-mentioned aspects = 3 - Plan includes 1 of the above-mentioned aspects = 2 - Plan is submitted and includes <u>none</u> (0) of the above-mentioned aspects = 1 <p>If no information is provided a scoring of zero will be allocated.</p>	10
TOTAL		100

The bidders must score **70%** on the evaluation criteria to be eligible to be evaluated for Price and BBBEE.

5. DELIVERABLES

The following must be delivered for the duration of the contract:

- Monitoring and Optimization of the Endpoint & Server Environment;
- Version and Patch Management, ensure that National Credit Regulator is on the latest versions of the licensed Trend Micro Cyber security products;
- Alert Management and Incident Management;
- Configuration Management;
- Request Management;
- Anomaly Management;
- Deployment of add on technology;
- One health check per quarter;
- Adhoc remote support as and when required by National Credit Regulator;
- Support (telephonic and electronic);
- Monthly and Quarterly Reporting.
- Support for high priority incidents
- Product should have 24x7 vendor support
- Threat Hunting
- Create playbooks for Threat Hunting
- Virtual patching
- Security Operations Platform with Vulnerability dashboards

The solution must be able to support legacy server environments including Windows server:

- Windows Server 2008 (SP2) and 2008 R2 (SP2) (x64) Editions
- Windows Server 2012 and 2012 R2 (x64) Editions
- Windows MultiPoint Server 2012 (x64) Editions
- Windows Storage Server 2012 (x64) Editions
- Windows Server 2016 (x64) Editions
- Windows Server 2019 (x64)
- Windows Server 2022 (x64)

The solution must be able to support legacy desktop and laptops with:

- Windows 8 and 8.1 (x86/x64) Editions

- Windows 10 (32-bit and 64-bit)
- Windows Server 2008/2008 R2 Failover Clusters (Active/Passive)
- Windows Server 2012 and 2012 R2 (x64) Editions
- Windows Server 2016 (x64) Editions
- Windows 8 and 8.1 Embedded (x86/x64) Editions
- Windows Server 2019 (X64)

The solution must include the below functionality for Application Control:

- Agent Installation from Windows or the Command Prompt
- Agent Self-Protection
- Agent Windows Interface and Notification Controls
- AIR Score
- Application Usage
- Certified Safe Software Service
- Control Applications and DLLs
- Dynamic Application Lists
- Key Performance Indicators Dashboard Widget
- Manually Update Policy from the Agent
- Process Blocking
- Also known as kernel-level or driver-level blocking
- System Lockdown
- Trusted Sources for Applications
- User-Based and Endpoint-Based Policy Management
- Application Control functionality that includes device and user policies for application blacklisting, whitelisting, and device lockdown.
- Application Control policies can use constantly updated comprehensive application-categories supplied by the vendor, for ease of administration.
- Application Whitelisting policies for prohibiting any unauthorized applications from running, with automatic whitelisting of already existing/running applications.
- The solution should support integration with breach detection system to apply policies based on-the-fly on-premise created suspicious objects.
- Application Control functionality that includes device and user policies for application blacklisting, whitelisting, and device lockdown.
- Application Control policies can use constantly updated comprehensive application-categories supplied by the vendor, for ease of administration.

- Application Whitelisting policies for prohibiting any unauthorized applications from running, with automatic whitelisting of already existing/running applications.
- The solution should support integration with breach detection system to apply policies based on-the-fly on-premise created suspicious objects.
- Integration with Advanced Threat protection system to provide custom defence against identified threats
- Protects against users or machines executing malicious software
- The Solution Should Further simplifies deployment when used with OfficeScan
- The Solution Should Provide advanced features for centralized enforcement of corporate policies with central management console
- The Solution Should Utilizes extensive categorized application catalog (analyzed and correlated threat data from billions of files in the global threat intelligence network)
- The Solution Should Employs dynamic policies to allow users to install valid applications based on many reputation-based variables such as prevalence, regional usage, and maturity
- Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files)
- The Solution Should Provide global and local real-time threat intelligence based on good file reputation data correlated across a global network
- The Solution Should Interconnects with additional layers of security to better correlate threat data and stop more threats, more often
- The Solution Should Leverages threat data analyzed and correlated from 347 million unique files and 4+ billion good file records global threat intelligence network)
- The Solution Should Integrates with complete user protection to complement antivirus, host intrusion prevention, data loss prevention, mobile security, and more
- The Solution Should Increases convenience of implementing granular control with a customizable dashboard and management console
- The Solution Should Uses intelligent and dynamic policies that still allow users to install valid applications based on reputation-based variables like the prevalence, regional usage, and maturity of the application
- The Solution Should Provide greater insight into threat outbreaks with user-based visibility, policy management, and log aggregation. Enables reporting across multiple layers of security through central management software
- The Solution Should Easily deployed using existing own vendor endpoint security or other third-party deployment tools

- The Solution Should Categorizes the applications and provides regular updates to simplify administration using Certified Safe Software Service
- The Solution Should Uses application name, path, regular expression, or certificate for basic application whitelisting and blacklisting
- The Solution Should Contains broad coverage of pre-categorized applications that can be easily selected from application catalog (with regular updates)
- The Solution Should Ensures that patches/updates associated with whitelisted applications can be installed, as well as allowing your update programs to install new patches/updates, with trusted sources of change
- Solution Should support Features to roll-your-own application whitelisting and blacklisting for in-house and unlisted applications
- The Solution Should Delivers unparalleled breadth of applications and good file data
- The Solution Should Limits application usage to a specific list of applications supported by data loss prevention (DLP) products for specific users or endpoints
- The Solution Should Collects and limits application usage for software licensing compliance
- The Solution Should support Features system to lockdown to harden end-user systems by preventing new applications from being executed

The solution must include integrated data loss prevention on endpoints:

- Product should include Data Loss Prevention functionality, integrated in the endpoint security solution with no additional hardware.
- Product has the capability to restrict the copy or upload of certain data, based on keywords, regular expressions, or file types to external storage or to the Internet.
- Speeds audits and enforcement with real-time reporting of integrated DLP violations, and the option of recording forensic data capture of DLP violations.
- Product should simplify regulatory compliance with out-of-the-box data protection compliance templates.
- Product must be able to apply granular device control policies to specific endpoints, to control/block access to unauthorized USB storage, 3G modems, and mobile devices.
- Device Control USB storage control includes the ability to create specific exceptions based on make and serial number of the USB storage device.
- The solution should not be standalone solution. It should be integrated in the following security Solution solutions with no additional hardware:
 - ❖ Endpoint
 - ❖ Mail Servers

- ❖ Messaging Gateway
- ❖ Web Gateway
- The Solution Should Offers granular device control, including the ability to create specific rules based on make and serial number of the device
- The Solution Should Empowers IT to restrict the use of USB drives, CD/DVD writers, and other removable media
- The Solution Should Tracks and documents sensitive data flowing through network egress points
- The Solution Should Detects and reacts to improper data use based on keywords, regular expressions and file attributes
- The Solution Should Educates employees on corporate data usage policies through alerts, blocking and reporting
- The Solution Should Simplifies regulatory compliance with out-of-the-box compliance templates
- The Solution Should Speeds audits and enforcement with forensic data capture and real-time reporting
- The Solution Should Improves visibility and control with a centrally managed software console

Solution must include Cloud Application Security:

- The Solution Should Protects Office 365 email and other cloud file-sharing services
- The Solution Should Enhances built-in security with sandbox malware analysis
- The Solution Should Give visibility into sensitive data use with cloud file-sharing services
- The Solution Should Detects advanced malware hidden in Office 365 or PDF documents
- The Solution Should Supports all user functionality, on any device, with simple API integration
- The Solution Should Investigates the behavior of suspect files by detonating in a virtual sandbox, not just through static pattern matching
- The Solution Should Uses document-exploit detection to find malware hidden in common Office file formats such as Word, PowerPoint®, and Excel®.
- The Solution Should Guards against malicious URLs not only within the message body, but also within attachments

- The Solution Should Offers the only third-party advanced threat-protection Solution should for Office 365 that protects internal email (in addition to external email) to uncover attacks already in progress
- The Solution Should Protects hybrid Office 365 and on-premises Exchange architectures
- The Solution Should Provide DLP and advanced malware protection for Box, Dropbox, Google Drive, SharePoint Online, and OneDrive for Business
- The Solution Should Enables consistent DLP policies across multiple cloud-based applications
- The Solution Should Simplifies setup with more than 200 pre-built compliance templates, user/group policies, and support for Microsoft Rights Management services
- The Solution Should Seamlessly extends Office 365, Box, Dropbox, and Google Drive security
- The Solution Should Preserves full user and administrator functionality
- The Solution Should Provide direct cloud-to-cloud integration via vendor APIs for high performance and scalability
- The Solution Should Minimizes latency impact by assessing the risk of files before sandbox malware analysis
- The Solution should cloud-to-cloud API integration doesn't rely on redirecting email or web proxies.
- The Solution Should Add security without burdening IT with changing devices or user settings, installing software, setting up a web proxy, or changing the MX record to reroute email
- The Solution Should Integrates quickly and automatically with Office 365 and other cloud services
- The Solution Should Uncovers ransomware and other malware in office files: Uses document exploit detection to find hidden malware inside common office file formats like Word, PowerPoint, and Excel as was seen in 60% of targeted attacks

6. SKILLS TRANSFER

The successful bidder will work with **NCR** ICT Employees for the duration of this contract in order to effect skills transfer, bi-annual Cyber Security Awareness and Training.

7. REPORTING

The appointed service provider will report to the NCR ICT Manager.

8. PRICING SCHEDULE

	Quantity	Unit Price	Total
Trend Micro Smart Protection Complete (12 months)	400		
Trend Micro Cloud One (12 months)	40		
XDR & Threat Hunting, including credits for Email xdr, Mobile xdr (12 months)	3		
Monthly Managed Services for (12 months)	12		
Deployment - Installation and Configuration, Create Policies + Knowledge Transfer (Once off per annum)	4		
Cyber Security Awareness and Training as a service (once off per annum)	400		
	Sub Total		
	Vat		
	Total		

Important Note:-

The payment for licenses will be paid on annual basis whereas the Managed Support Services will be paid monthly in line with the SLA that will be signed between the appointed bidder and NCR.

9. TIMELINES:

- The software licenses are expected to be renewed timeously on or before the expiration of the current coverage and annually;
- The expected timeline for the installation or implementation of the other services MUST be within one (01) week after the issuing of the Purchase Order;
- The cyber security awareness and training will be done in accordance with the Cyber Security Awareness and Training Annual Plan;

10. COMPULSORY REQUIREMENTS

- a. Bidders are expected to provide the **proof of accreditation** with Trend-Micro OEM;
- b. Appointed service provider must ensure that the license keys are provided or submitted to NCR after the successful installation;
- c. Three (03) **reference letters** for previous successful installation in the past 3 years must be submitted. The letters must be in the letterhead of the company / client and signed by the relevant person/s;
- d. **Pricing** must be all inclusive, captured on the company's letter head and SBD3.1 for a period of three (3) years