



सत्यमेव जयते

प्रधान आयकर निदेशक का कार्यालय (अन्वे.)  
OFFICE OF THE PR. DIRECTOR OF INCOME TAX (INVESTIGATION)  
तीसरी मंज़िल, सी आर बिल्डिंग, क्वींसरोड, बेंगलुरु  
3RD FLOOR, CR BUILDING ANNEXE, QUEENS ROAD, BENGALURU

---

TENDERING DOCUMENT

For Empanelment of Digital Forensic and Financial Analysis Service providers for the office of the Pr. Director of Income Tax (Inv.), Income Tax Department, Bengaluru

---

INDEX

| Section | Type of document                       |
|---------|--|
|         | Notice Inviting Tender                 |
| I       | Domestic Competitive Bidding           |
| II      | Invitation to Bid                      |
| III     | Instruction to Bidders                 |
| IV      | Terms & conditions of contract         |
| V       | Scope of Empanelment& other conditions |
| VI      | Technical Bid                          |
| VII     | Financial Bid                          |
| VIII    | Evaluation Method of Bid               |
|         | Annexure – A (Profile of Organisation) |



प्रधानआयकरनिदेशक (अन्वे.) काकार्यालय  
OFFICE OF THE PR. DIRECTOR OF INCOME TAX (INVESTIGATION)  
तीसरीमंज़िल, सीआरबिल्डिंग, क्वींसरोड, बेंगलुरु  
3RD FLOOR, CR BUILDING ANNEXE, QUEENS ROAD, BENGALURU

F.No.62/DFS/Pr.DIT (Inv.)/BLR/2024-25

Date: 22.10.2024

**NOTICE INVITING TENDERING FOR EMPANELMENT OF DIGITAL FORENSIC SERVICES AND FINANCIAL ANALYSIS SERVICES**

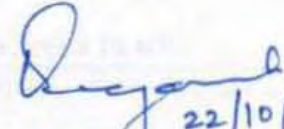
1. The Pr. Director of Income Tax (Inv.), Bengaluru invites tenders in sealed covers from eligible, bona-fide, reliable and resourceful service providers experienced in the field of Digital Forensic Services including Financial/Data Analysis Services for specific services for the office of the Pr. Director of Income Tax (Inv.), Bengaluru. The empanelment is for a period of **three year w.e.f 01.12.2024 to 30.11.2027** which may be extended by another two years, at the administrative convenience of the Pr. Director of Income Tax (Inv.), Bengaluru, subject to satisfactory performance.

2. Offer should be submitted in 2 (two) bid pattern, i.e. (i) **Technical bid** and (ii) **Financial bid** and both the bids are to be placed in two separate sealed envelopes (clearly superscribing 'Technical bid' and 'Financial bid' ) which in turn should be placed in **one single sealed cover**, duly superscribed "**Tenders for empanelment of Digital Forensic Services for the office of the PDIT (Inv.), Bengaluru**" and addressed to "**The Pr. Director of Income-tax (Inv.), Bengaluru**" so as to reach the Office of Pr. Director of Income-tax (Inv.), Bengaluru, **not later than 05:00 P.M. on 12<sup>th</sup> November 2024.**

3. The Tenders **Technical Bid** will be opened on **13<sup>th</sup> November 2024** at 11:30 A.M., and the **Financial Bid** on **14<sup>th</sup> November 2024** at 11:30 A.M in Room No. 203, 2<sup>nd</sup> Floor, Addl.DIT(Inv.), U-1 & HOO, O/o Pr.DIT(Inv.), CR Building (Annexe), Queen's Road, Bengaluru. The Financial Bid of only those Service Providers shall be opened whose technical bid (inclusive of profile of applicant Service Provider) are found eligible in the presence of the Vendors or their representatives who may likely to be present. Detailed information / terms and conditions for the purpose can either be downloaded from [www.eprocure.gov.in](http://www.eprocure.gov.in) and [www.incometaxkarnatakagoa.gov.in](http://www.incometaxkarnatakagoa.gov.in) or Tender Documents can also be collected from this office during the regular office hours i.e. 11:30 A.M. to 05:00 P.M., on payment of non-refundable tender fee of **Rs. 1,000/-by Demand Draft drawn in favour of The ZAO, CBDT, Bengaluru** payable at Bengaluru. In case the tender document is downloaded from the websites, a non-refundable tender fee of Rs. 1,000/- has to be paid by way of **Demand Draft drawn in favour of The ZAO, CBDT, Bengaluru, payable at Bengaluru**, at the time of submission of the duly filled tender application.

4. Critical dates of the tender is as under:-

|  |  |
|--|--|
| Last date of availability of tender documents for downloading  | 12 <sup>th</sup> November 2024   |
| Last date for submission of tender                             | 12 <sup>th</sup> November 2024   |
| Opening of tenders:-<br>(a) Technical Bid<br>(b) Financial Bid | 11:30 A.M. on 13 <sup>th</sup> November 2024<br>11:30 A.M. on 14 <sup>th</sup> November 2024 |

  
22/10/2024  
(D Sankar Ganesh, IRS)  
Addl. DIT (Inv.), Unit-1 & HOO  
Bengaluru

## SECTION – I

### DOMESTIC COMPETITIVE BIDDING

(Through call of open Tenders)

Tender No.F.No.62/DFS/Pr. DIT(Inv.)/BLR/2024-25

Date: 22.10.2024

|   |  |
|---|--|
| Period of Contract                        | From <b>01<sup>st</sup> December 2024 to 30<sup>th</sup> November 2027</b> , which may be extended by another two years, at the administrative convenience of the Pr. Director of Income Tax (Inv.), Bengaluru, subject to satisfactory performance.   |
| Earnest Money Deposit                     | Rs. 30,000/- by Demand Draft drawn in favour of ZAO, CBDT, Bengaluru payable at Bengaluru.   |
| The tender documents can be obtained from | May be downloaded from e-procurement website i.e., <a href="http://www.eprocure.gov.in">www.eprocure.gov.in</a> and <a href="http://www.incometaxkarnatakagoa.gov.in">www.incometaxkarnatakagoa.gov.in</a> or can be collected from this office during the regular office hours i.e. 10:00 A.M. to 05:00 P.M |
| Tender cost                               | Non-refundable. 1,000/-by Demand Draft drawn in favour of ZAO, CBDT, Bengaluru, payable at Bengaluru   |
| Last Date & Time for receipt of Bid       | Date: <b>12<sup>th</sup> November 2024</b><br>Time: 05:00 P.M.   |
| Time and Date of opening of Bids          | Technical Bid:11:30 A.M. on <b>13<sup>th</sup> Nov. 2024</b><br>Financial Bid: 11:30 A.M. on <b>14<sup>th</sup> Nov. 2024</b>  |
| Tenders addressed to                      | The Pr. Director of Income Tax (Investigation), Bengaluru  |
| Tender documents can be submitted to      | Office of the Pr. Director of Income Tax(Inv.), 4 <sup>th</sup> Floor, CR Building Annexe, Queens Road, Bengaluru  |
| Place of Opening of Bids                  | Room No. 203, 2 <sup>nd</sup> Floor, Addl.DIT(Inv.), U-1& HOO, Office of the Pr. Director of Income Tax(Inv.), CR Building Annexe, Queens Road, Bengaluru  |

## SECTION – II

### INVITATION TO BID

1. Income Tax Department, Bengaluru intends to invite tender in sealed covers from eligible, bona-fide, reliable and resourceful service providers experienced in the field of Digital Forensic Services for specific services for the office of the Pr. Director of Income Tax (Inv.), Bengaluru. This tender is for fixing the lowest eligible rate for the Digital Forensic services including Financial/Data Analysis Services the terms of which are elaborated in Section III & Section IV of this tender document. The eligible service providers shall provide the services at the rate fixed after finalisation of this tender.
2. **Summary of the job work :** At the outset, the Service Provider should have the capability to carry out Digital Forensics & Analysis and allied services including :
  - Forensic acquisition / Imaging of different types of storage media such as hard Drives, USB thumb drives, CDs/DVDs, Tablets, Servers etc. Gathering evidence and information including deleted files, cracking passwords from suspected computer/ source with hash value report generation and preparing separate working copy by using legal and most efficient and updated forensic tools
  - Email Forensics: Indexing of mails, time-line analysis, keyword searching.
  - Mobile Forensics : Logical and Physical extraction of mobile phones/ all kinds of smart phones including I-phones, I-pads etc, data extraction and analysis, SIM card analysis
  - On-site mapping and securement of IT infrastructure.
  - Detection of various accounting software systems per premise
  - ERP (SAP/Tally/others/custom ERP software) data acquisition
  - Live analysis and report generation on accounting/ERP database
  - Software code analysis to detect suppression of reported income
  - Enterprise wide data searches for specific search terms
  - Detection and analysis of Cloud Data sources
  - Automated backup of specific files types
  - Analysis of forensic artefacts for user activity mapping on computers
  - SQL scripting for relational database analysis.
  - Custom scripting for mobile data analysis.
  - Acquisition and analysis of CCTV dumps.
  - Recovery of deleted data. Analysis of deleted/Non deleted data of Excel files/Doc files/PDF files/Scan images. Data files for TALLY or any other accounting application. Data hidden in unallocated sectors/Data hidden in pictures.
  - Analysis of electronic data/electronic evidence assigned to it by the Income tax Department (“ITD”) and submit a report in writing for the purposes of The Bharatiya Sakshya Adhiniyam,2023.
  - Analysis report shall also specify the location of files. Resources shall also carry out such investigation as required by Investigation Officer including password breaking & Text to Speech converters.

- Password-breaking in all possible OS environments, mobile platforms. This may include springboarding and jailbreaking for iOS devices, and Rooting for Android devices to access data when the target person is non-cooperative.
- Remote access of databases through VPN/SSID based applications or other such architecture in use by present day businesses spread over distant geographical locations for storage and recovery of financial data,
- Review and Analysis of Data shall include, but not be limited to, Bank Statement Analysis, Analysis of emails, social media chats, financial data on applications like Tally, Tally ERP, SAP, Oracle or any other customised RDBMS application using software tools, database Analysis through software tools etc., relationship resolution & presentation of analysed data. Discovery of patterns in the data including the financial data using AI based or any other relevant tools. This in turn may include small pieces of software coding

3. **The Qualification/professional skill requirements of resources personnel** : Service Provider resource person required for Onsite Evidence Collection & Off-site restoration and Investigation, should possess minimum of following skill sets:

- (a) Degree/ MS in Computer Forensic from a recognized institute.
- (b) Proficiency in using FORENSIC Hardware (H/W) & Software(S/W).
- (c) Proficiency in using Tableau duplicators, Encase forensics, Password, write-blockers.
- (d) Database knowledge about different Operating Systems.
- (e) Knowledge of RDBMS based Oracle/Microsoft SQL etc.,
- (f) Knowledge of MS SQL & MySQL.
- (g) Knowledge of TALLY and other book keeping softwares.
- (h) The forensic team should have at least one member from financial background like CA/CFA/CS to assist in digital forensic analysis.
- (i) Ability to gather, view, and analyse large volume of data that may be present in various disparate formats.
- (j) Proficiency in spreadsheet programs like MS Excel.
- (k) Knowledge of Python, Power BI, SQL, R and MATLAB.
- (l) Skilled at data visualisation and capability to present reports in a format as required. Should be skilled at creating clean, visually compelling charts that will help understand the data.
- (m) Strong logical skills and statistical knowledge

4. The service provider is expected to prevent any unethical usage of data of the Directorate and requires confidentiality and complete integrity on part of service provider as well as its resource persons
5. The Earnest Money Deposit (Refundable, if the bid is not successful) of Rs. 30,000/- (Rupees Thirty Thousand only) in the form of Demand Draft in favour of **ZAO, CBDT, Bengaluru** payable at Bengaluru, has to be remitted along with bid forms.
6. Initially, the empanelment will be for a period of three year (from **01<sup>st</sup> December 2024 to 30<sup>th</sup> November 2027**), which may be extended by another two years at the

administrative convenience of The Pr. Director of Income Tax(Inv.), Bengaluru, subject to satisfactory performance.

7. The bid document can be downloaded from e-procurement website i.e., [www.eprocure.gov.in](http://www.eprocure.gov.in) and [www.incometaxindia.gov.in](http://www.incometaxindia.gov.in). or Tender Documents can also be obtained from the Administrative Officer, Grade-III, Cash Section, O/o Principal Director of Income Tax (Investigation), Bengaluru during the regular office hours i.e. 11:30 A.M. to 05:00 P.M., on payment of **non-refundable tender fee of Rs. 1,000/-** by Demand Draft drawn in favour of ZAO, CBDT, Bengaluru payable at Bengaluru. In case the tender document is downloaded from the websites, a non-refundable tender fee of Rs. 1,000/- has to be paid by way of Demand Draft drawn in favour of ZAO, CBDT, Bengaluru, payable at Bengaluru, at the time of submission of the duly filled tender application.
8. The Income tax Department makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone. This tender does not constitute an offer by the department. The bidder's participation in this process may result in selecting the L-1 bidder and further to invite other bidder for empanelment at L-1 rates subject to individual items where they have offered lower rates. The commencement of such empanelment does not, however, indicate any commitment by the department to award the bid. The department also reserves the right to accept or reject any bid, and to annul the bidding process at any time, without thereby incurring any liability to the affected Bidder or Bidders.
9. **The offer is only for empanelment and the same would not amount to any work contract or surety with reference to allotment of work.**
10. Offer should be submitted in two (2) bid pattern, i.e. **(i) Technical bid**, as per Section VI and **(ii) Financial bid**, as per Section VII, and both the bids are to be placed in two separate sealed envelopes (clearly superscribing 'Technical bid ' and 'Financial bid') which in turn should be placed in one single sealed cover, duly superscribed "**Tenders for Providing Digital Forensic Services for the office of the Pr.DIT (Inv.), Income Tax Department, Bengaluru**" and addressed to "**The Pr. Director of Income-tax (Inv.), Bengaluru**", so as to reach the office of the Principal Director of Income Tax (Investigation), Income Tax Department, Bengaluru, **not later than 05.00 P.M., on 12<sup>th</sup> November 2024.**
11. The bids of the Service Providers whose technical bid and financial bid are not placed in separate sealed envelopes or if they quote the rates in the technical bid, then such tender shall be rejected forthwith. **The Financial Bid of only those Service Providers shall be opened whose technical bid (inclusive of profile of applicant Service Provider) are found eligible.** The financial bid of the disqualified bidders after assessing technical bid shall be returned, unopened. The tender without earnest money will be disqualified. The Demand Draft submitted by unsuccessful Service Providers will be returned within 20 (Twenty) working days of opening the tender. **If the successful Service Provider refuses to provide the services as per the tender conditions, then the earnest money deposit will be forfeited.** The earnest money deposit of the successful Service Provider will be returned after one month from the date of providing the service.

The Tenders for the Technical Bid will be opened on **13<sup>th</sup> November 2024 at 11:30 A.M.**, and the Financial Bid on **14<sup>th</sup> November 2024 at 11:30 A.M** in Room No. 203, 2<sup>nd</sup> Floor, Addl.DIT(Inv.), U-1 & HOO, O/o Pr.DIT(Inv.), CR Building (Annexe), Queen's Road, Bengaluru. The Financial Bid of only those Service Providers shall be opened whose technical bid (inclusive of profile of applicant Service Provider) are found eligible in the Office of the Pr. Director of Income Tax, CR Building Annexe, Queens Road, Bengaluru the presence of the Bidders or their representatives who may be present. The tenders will be opened by the Tender Evaluating Committee constituted for this purpose. They will scrutinize the technical bids and determine the eligible bids. Thereafter, financial bids of only eligible bidders will be opened.

## SECTION-III

### INSTRUCTIONS TO BIDDERS

1. The Bidders are advised to study the tender document carefully. Submission of Tender shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications. Failure to furnish all information responsive to those mentioned in the tender documents or submission of a proposal not substantially responsive to tender conditions may result in rejection of the proposal.
2. Process: Selection of a successful Service Provider will involve a six (6) stage approach before issuance of Work Order/letter of appointment.
  - i. Issue of Notification.
  - ii. Issue of Bid Document
  - iii. Receipt of Bids
  - iv. Evaluation of Technical Bid
  - v. Selection of technically qualified bidders
  - vi. Evaluation of financial bids and finalisation of rates
  - vii. Offer to technically qualified bidders to offer services at such rates
  - viii. Finalisation of vendors to be empanelled.
3. The bidder is required to fill up the Profile of his Organization and submit other details in the format given as per **Annexure- A** of the Bid Document.
4. The bids are to be submitted in two parts in separate sealed envelopes, i.e., **Technical Bid and Financial Bid.**
5. **The Technical Bid submitted by the bidder shall include the following:**
  - i. Full particulars of Govt. or other organizations, where the Service Provider has provided Digital Forensic Services, Data Analysis Services (Self-attested copies of the relevant work orders are to be enclosed).
  - ii. Profile of his Organization and other details in the format given as per Annexure-A
6. **Sealing and Marking of Bids:**
  - (a) The Technical Bid (as per Section VI) along with EMD instrument and requisite documents shall be placed in one sealed envelope superscribed 'Technical Bid'. The Financial Bid (as per Section VII) shall be kept in a separate sealed envelope superscribed 'Financial Bid'. Both the envelopes shall then be placed in one single sealed envelope superscribed "**Tenders for Providing Digital Forensic Services for the office of the PDIT (Inv.), Income Tax Department Bengaluru**" and addressed to "**The Pr. Director of Income-Tax (Inv.), Bengaluru**". The bidder's name, telephone number and complete mailing address shall be indicated on the cover of the outer envelope
  - (b) Both the inner envelopes superscribed "Technical Bid" and "Financial Bid" shall have the name and address of the bidder so that if required, they may be returned to the bidder without opening them.

(c) If the outer and inner envelopes are not sealed and marked as required, the Income-tax department shall assume no responsibility for the bid's misplacement or premature opening.

(d) If for any reason, it is found that the Technical Bid reveals the Financial Bid related details in any manner whatsoever, or, the Financial Bid is enclosed in the envelope superscribed, "Technical Bid", the Bid document will be summarily rejected in the first instance itself.

(e) All the Bid documents submitted shall be serially page numbered and contain the table of contents with page numbers.

**7. Deadline for Submission of Bids:**

(a) The applicants should submit their bids in a sealed envelope, as described above to the Office of the Pr. Director of Income Tax, CR Building Annexe, Queens Road, Bengaluru by **05:00 P.M on 12<sup>th</sup> November 2024.**

(b) No acknowledgement, in respect of receipt of any bid, shall be issued.

(c) Bids must be received by the Income-tax department at the address specified not later than the time and date specified in the Invitation for Bids.

(d) In the event of the specified date for the submission of Bids being declared a holiday for the Income-tax department, the Bids will be received up to the given time on the next working day.

(e) The Income-tax department may, at its discretion, extend the deadline for submission of bids which will be binding on all the bidders.

(f) Any bid received by the Income-tax department after the deadline for submission of bids prescribed by the Income-tax department in the bid, document will be rejected and will not be opened.

**8. Modifications and Withdrawal of Bids:**

(a) No modification or substitution of the submitted application shall be allowed.

(b) An applicant may withdraw its Tender after submission, provided that written notice of the withdrawal is received by the Income-tax Department before the due date for submission of applications.

(c) The withdrawal notice shall be prepared in original only and each page of the notice shall be signed and stamped by authorized signatories. The copy of the notice shall be duly marked as "WITHDRAWAL".

**9. Opening and Evaluation of Technical Bids**

(a) The Tender Evaluating Committee appointed by the Income-tax Department / or a committee appointed for this purpose will open all Technical Bids in the first instance on the appointed date, time and venue.

(b) During evaluation of the bids, the Income-tax Department may, at its discretion, ask the Bidder for clarification of its bid. The request for clarification and response shall be in writing.

(c) No bidder shall contact the Income-tax Department on any matter relating to his bid from the time of the bid opening to the time the issue of work order. All bidders are strongly advised to furnish all material information in the bid itself.

- (d) Any effort by a Bidder to influence the Income-tax Department in its decisions on bid evaluation, bid comparison or work order decision will result in rejection of the bid.
- (e) The Financial Bid of only those Service Providers shall be opened whose technical bid (inclusive of profile of applicant Service Provider) are found eligible.

**10. Opening and evaluation of Financial Bids**

- (a) The results of the bid will be communicated in writing to the qualifying bidder. The unsuccessful bidders will be notified separately.
- (b) The Price Bid shall comprise the price component for all the services indicated in the Section-IV and other sections of this bid document. The price quoted by the bidders shall include all applicable taxes, wherever applicable. The bidder shall include Service tax and Surcharges etc. as applicable on the services that are provided under this contract in the lump sum rates quoted and Income-tax Department would not bear any additional liability on this account.
- (c) Income-tax Department shall however, deduct such tax at source as per the rules and issue necessary certificates to the Service Provider. The prices once accepted by the Income-tax Department shall remain valid till the contract remains in force.
- (d) Rates shall include statutory obligations as may be applicable.
- (e) Amounts/Prices shall be quoted in Indian Rupees only.
- (f) Arithmetical errors will be rectified on the following basis: - If there is a discrepancy between words and figures, the amount written in words shall be taken as the bid price.

**11. Requests for Information :**

- Bidders are required to direct all communications related to this document through the designated Contact person Administrative Officer, Gr-II, Cash Section, O/o PDIT (Inv.), Bengaluru. All queries relating to the Bid, technical or otherwise, must be in writing only to the designated contact person. The Department will not answer any communication initiated by Respondents later than five business days prior to the due date of opening of the bids. If the Department, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then department reserves the right to communicate such response to all Respondents
- 12. The Income-tax Department, without assigning any reasons, reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time, without thereby incurring any liability to the affected Bidder or Bidders or any obligations to inform the affected Bidder or bidders of the grounds for the action of the Income-tax Department
  - 13. The Bidder shall sign his bid with the exact name of the concern whom the Income Tax Department has empanelled as Service Provider. The Bid document filed by the bidder shall be typed or written in indelible ink. No overwriting or cuttings shall be permitted.
  - 14. The Income-tax Department reserves the right to reject the bid having deviations from the prescribed terms and conditions.

15. The Service Provider shall not subcontract or permit anyone other than himself to perform any of the work, service or other performance required of the Service Provider under the contract.
16. Making misleading or false representation in the bid document will lead to disqualification of the Bidder at any stage.
17. Where the bid has been signed by the Authorized Representative on behalf of the concern, the bidder shall submit a certificate of authority and any other document consisting of adequate proof of the ability of the signatory to bind the bidder to the contract. (Income-tax department may out rightly reject any bid, which was not supported by adequate proof of the signatory's authority).
18. Department reserves the right to negotiate the price with the finally short listed bidder before awarding the contract. It may be noted that Income Tax Department will not entertain any price negotiations with any other bidder

Read and accepted.  
Signature and stamp of  
Bidder or Authorized Signatory

## SECTION-IV

### TERMS & CONDITIONS OF CONTRACT

1. In the event of bid being accepted, the bid will be converted into a contract between Income Tax Department (ITD) and the successful bidder (Service Provider/Vendor). Such contract shall be governed by the terms and conditions given in the following paragraphs.
2. **Summary of the job work :** At the outset, the Service Provider should have the capability to carry out Digital Forensics & Analysis and allied services including :
  - Forensic acquisition / Imaging of different types of storage media such as hard Drives, USB thumb drives, CDs/DVDs, Tablets, Servers etc. Gathering evidence and information including deleted files, cracking passwords from suspected computer/ source with hash value report generation and preparing separate working copy by using legal and most efficient and updated forensic tools
  - Email Forensics: Indexing of mails, time-line analysis, keyword searching.
  - Mobile Forensics : Logical and Physical extraction of mobile phones/ all kinds of smart phones including I-phones, I-pads etc, data extraction and analysis, SIM card analysis
  - On-site mapping and securement of IT infrastructure.
  - Detection of various accounting software systems per premise
  - ERP (SAP/Tally/others/custom ERP software) data acquisition
  - Live analysis and report generation on accounting/ERP database
  - Software code analysis to detect suppression of reported income
  - Enterprise wide data searches for specific search terms
  - Detection and analysis of Cloud Data sources
  - Automated backup of specific files types
  - Analysis of forensic artefacts for user activity mapping on computers
  - SQL scripting for relational database analysis.
  - Custom scripting for mobile data analysis.
  - Acquisition and analysis of CCTV dumps.
  - Recovery of deleted data. Analysis of deleted/Non deleted data of Excel files/Doc files/PDF files/Scan images. Data files for TALLY or any other accounting application. Data hidden in unallocated sectors/Data hidden in pictures.
  - Analysis of electronic data/electronic evidence assigned to it by the Income tax Department ("ITD") and submit a report in writing for the purposes of The Bharatiya Sakhshya Adhinyam, 2023.
  - Analysis report shall also specify the location of files. Resources shall also carry out such investigation as required by Investigation Officer including password breaking & Text to Speech converters.

- Password-breaking in all possible OS environments, mobile platforms. This may include springboarding and jailbreaking for iOS devices, and Rooting for Android devices to access data when the target person is non-cooperative.
  - Remote access of databases through VPN/SSID based applications or other such architecture in use by present day businesses spread over distant geographical locations for storage and recovery of financial data,
  - Review and Analysis of Data shall include, but not be limited to, Bank Statement Analysis, Analysis of emails, social media chats, financial data on applications like Tally, Tally ERP, SAP, Oracle or any other customised RDBMS application using software tools, database Analysis through software tools etc., relationship resolution & presentation of analysed data. Discovery of patterns in the data including the financial data using AI based or any other relevant tools. This in turn may include small pieces of software coding
3. The vendor should have the capacity to examine the digital devices (**including laptops, desktops, servers, smartphones and any electronic computing device which can store and process financial and business process data by whatever name called**) for suspected evidence. The vendor should have the capacity to do acquisition of digital evidence (involving backup, copying, Imaging and cloning) at the time of Search, Seizure and Survey Action or any other time as required by the ITD.
- 3.1 The vendor should have capability to do a fair **Forensic acquisition** involving collection of data in a forensically sound manner using licensed, open-sourced tools depending upon the operating system. The devices include servers, desktops, mobile phones, **cloud data in mobile phones and third-party cloud services**. The vendor should have capability to access remote/networks and determine hidden systems and servers which are being used for various purposes during the course of search action.
- 3.2 The vendor should have capability to do **Data Extraction and Data Remediation** which includes extraction of data from forensic formats such as **E01, EX01, DD, AFF, etc.** into native formats such as **Word, Excel, PDF, SQL, etc.** as and when required by the ITD The vendor should have capability to do Data Remediation including de- duplication of data, removal of system files, culling of files based on files types and partition wise reduction of repeated data and presentation of data in readable formats (Native files) as and when required by the ITD.
- 3.3 **The forensic engineers of the vendors have to be qualified to stand as expert witness in courts** to describe and defend the methodologies adopted during any of the stages involved in **Data Acquisition, Processing, Analysing, and Presenting.**
- 3.4 The Vendor should have capability to do **Basic Data presentations** in which the forensic vendor is expected to perform comprehensive restructuring of data and provide the data which is usable by the Authorized officer for his

investigative requirements. This includes providing metadata information, file signature information, and deleted data information and data reconstructed information.

- 3.5 The vendor should have the capability to locate, identify and analyse encrypted files. Further, the vendor should also have the capability to break encryption, crack password and access hidden data; the vendor should also be able to provide such recovered decrypted/password-cracked/unhidden data in a readable format.
- 3.6 The vendor should have capability to do **Forensic acquisition** involving collection of data from mobiles, tablets in a forensically sound manner using licensed/open-sourced tools depending upon the operating system. The Vendor should have capability to do **Data Remediation of mobile data** which includes extraction of text messages, voice notes, call records, documents, and mobile notes. The vendor should have capability to do **Data retrieval from mobile applications** (wherever possible and applicable), logical examination of mobile phones and determining whether logical backups or physical backups to be taken and perform the specified activity with concurrence from the Authorized Officer.
4. **Recovery of Deleted files:** The vendor should have capability to do Data retrieval services from computers which include retrieving data from servers where data has been deleted and where databases have been modified, using retrieval techniques from the log files. Where log files are not available, reconstruction of respective databases using third party tools may be adopted
  - 4.1 The vendor should also have capability to **recreate the original data from partial recovered data** in areas of file signatures, deleted files, recreation of partially broken files, carving of partially overwritten files, and reconstruction of broken databases
5. **Analysis of data:** The vendor should have capability to do basic **Investigative analytics** in which, wherever required, the authorized officer may seek the assistance of the forensics team to perform database interpretations, email keyword searches, normal Web searches, or any other relevant support activities relating to electronic devices and evidences during the conduct of search and vendor should be capable of same.
  - 5.1 The vendor should have the capability to handle large volume of data in disparate forms; the vendor should also have the tools to index the large volume of data so that the data from disparate sources in various file formats becomes query-abled. The vendor should have the capability to identify relationships between various data items and provide deep insight into the data being analysed. Such large data may include Stock Exchange Trade Data/ Commodity Exchange data related to shares, debentures, scrips, futures and options etc.; bank statements; cash flows / fund trails.

5.2 The vendor should have the capability to present the analysed data in appealing, intuitive and illustrative visualisations. The vendor should be in a position to employ various visualisation tools that may require custom coding as well

6. **Special Requirements:** Over many years of experience with digital data retrieval and analysis ITD officers have become well- acquainted with the possible situations faced by search teams for locating and accessing relevant data and the technology deployed by target persons to conceal data. It is therefore expected of the prospective service providers to match the organizational skill set and to augment it with technical know-how and latest software (s/w) and hardware(h/w) tools to deal with difficulties faced in getting timely access to financial data, which is at the core of any successful search action by the ITD. Some possible scenarios have been outlined below to give a fair idea to the Service Providers of the level and scope of forensic support expected of them. It may be clearly understood here that **these anecdotal accounts of the data forensic scenarios are just a few examples of the nature of job requirements to give a perspective to the Service Providers. The scope of work is certainly broader and much varied but not limited to these scenarios**

6.1 **Scenario 1 : Password Breaking :**

6.1.1 ITD usually find encryption in different type of devices and files like mobiles, desktops, laptops, hard drives, document files and tally data. In these cases, password breaking starts with the use of a forensic software like Passware, Access data FTK etc. which have their own dictionaries (thousands of possible passwords which can be alphabets, alphanumeric, numbers, symbols, uppercase and lowercase, spaces etc.) and using several permutations and combinations, they recover the underlying passwords.

6.1.2 Since, password can vary from weak to strong, the software decryption timeline is a challenge and the skills and experience of the forensic team becomes a determining factor in real-time resolution of the encryption and hence, not just the s/w tools deployed but also the active skilled intervention of the forensic manpower is of utmost importance in getting a quick match. There will be situations where vendor has to add their own dictionaries to enhance the decryption process.

6.1.3 The software tools deployed so far automatically detect the file type and complexity level of the password and offer all possible types of attacks including but not limited to dictionary attack, brute force attack, xieve attack etc. The task of the forensic manpower is to decide on the trade-off between no. of types of attacks to be selected and the time taken by the recovery/decryption process

6.2 **Scenario 2: Servers Outside India :**

6.2.1 It is not unusual nowadays to find that database servers of target persons are situated outside India and data has to be retrieved/backed up using our own

processes and methods. The forensic team should, firstly, be able to identify if any server is maintained outside India using IP addresses. Then, the forensic team can take access of the live/running remote server using the credentials which are gathered by asking the target person but in this process, it is for the forensic team to identify the admin who controls the maximum rights of the server.

- 6.2.2 Once the server data (Accounting, Finance, Stock etc.) is accessed we identify its validity and put checks on the last updation of the data in the server. This is the most significant part of the exercise because evidentiary value of the data has to be ensured and the Forensic team should be able to document the process deployed for accessing the data and categorically ensure that the correct data retrieval and data integrity checks have been put in place while backing up the data.
- 6.2.3 An important task for the forensic team in such cases is to check if the host of the server is a third- party entity like AWS (Amazon), Microsoft Azure, Salesforce etc. While the host can be the same organization entity/target group but very often such remote servers are hosted by data service providers or cloud service providers. The forensic team should be well-conversant with the procedures/Industry practices for obtaining access to database servers from such third party hosts
- 6.2.4 Once the host is identified, the forensic have to check the configuration of the server as in size of database, application size, machine infrastructure, client-side configuration. Since, database is running on the live server, it is usually in raw form and size is voluminous, which makes it necessary to create a backup of the database which is then compressed for its use. After this compressed database is backed up, it is essential for the forensic team to verify and certify the validity of the database i.e. the backup matches with the live data and contains all the updated transactions and summary as required.
- 6.2.5 The compressed back-up of the database is downloaded by the forensic team along with the application setup files (where application is executable setup file) which are connected to the server side. Most importantly, for the evidence purpose, the forensic team has to do the hashing of the application and database downloaded.
- 6.2.6 After the data and front end is downloaded the target persons/organization are asked to arrange an idle machine where this downloaded database and application can be run to create a cloned/dummy/temp server which will replicate the original server. This arrangement has to be achieved during the search action so as to allow for accessing and analysis/investigation by the search team. The forensic manpower has the pivotal role in obtaining and providing data access in readable form to the search team.

### **6.3 Scenario 3: If the remote database uses an Application which is web based**

**6.3.1** A greater level of complexity is posed by remote servers if the application is web based, and in such situations, we have to create a cloud instance to make a live environment for the database application to run. The database will be separated and isolated and is restored on the cloud space. The server-side application is installed and connected with the database. A major difference in the process deployed here is that the linkage established between the application and database is based on hostname-based configuration and not IP-based configuration. Thereafter, the application is run and tested to check if the database connection is foolproof. Sometimes, all modules and reporting features in the application may not work properly, and the forensic team should have the expertise for troubleshooting or coding required in the backend

**6.3.2** Finally, the working of the server and data validity has to be verified from the client-side and query reports and data have to be checked against the live server.

### **6.4 Scenario 4: When Database is present in India but at different location and size of database is large to be downloaded locally**

**6.4.1** A peculiar situation was faced in the case of an organization which was using two different servers for different time periods, specifically for financial years 2010-2020 a database server, say V1 and from financial year 2020 onwards another server, say V2. The V1 server database was hosted by a CSP (Cloud service provider) which was in India at a Mumbai location. V2 was with another third Party CSP (Cloud service provider) in India, say AWS.

**6.4.2** The combined size of the databases of both V1 & V2 servers was 1 TB approx. and could not be downloaded at the premises because of technical and network difficulties. The database was downloaded at the Mumbai data center after proper hashing and validation, and it was then brought to the main premise in Delhi. V2 server database (back-up) was uploaded in cloud and web-based application was linked to this server and it was made up and running.

**6.4.3** Now, in the case of V2 server, the application setup files were readily available since it was up and running, but due to migration from V1 to V2, the older application was not available for running operations and it was difficult to obtain the setup files. Also, since the V1 server was an older version and not in use, it was found full of bugs and issues like missing modules.

**6.4.4** Therefore, for the V1 database, a local server was created by restoring the database and installing the necessary application. But due to the bugs which were found in the application program, some reporting features were not working properly for which backend queries had to be run and reports were fetched manually using DB Queries.

## 6.5 Scenario 5: ERP Environment

- 6.5.1 Increasingly, all financial data is found stored and managed on ERP solutions and the forensic teams are frequently called upon to create an ERP environment (temp server) for retrieval of imaged data on the customized application taken from the assessee i.e. tables and codes of each database/master files of the ERP application. The backend of such ERP temp server can include but is not limited to Oracle, SAP and other commonly known ERP solutions.
- 6.6 Further, the vendors should have technical experts well-versed with Basic Cloud Services like Compute Service, Storage Service, Network Service, Database Service, Security Service, Support Service ; Advanced Cloud Services consisting of Container Service, Managed Database as a Service, Content Delivery Network, MPLS Connectivity, HSM, DDoS, TLS / SSL Certificate Management, Dual / Multi Factor Authentication, Monitoring Services, Analytics Services ; and Managed Services consisting of Disaster Recovery as a Service and Backup as a Service. The data forensic service providers should have thorough knowledge of cloud deployment models especially Virtual Private Cloud (VPC), and cloud service models including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)
7. The vendor should have the ability to document Data Forensic analysis for the purposes of The Bharatiya Sakshya Adhiniyam,2023.
- 7.1 **Data Forensics and Data Analysis Report** : The Service Provider shall carry out forensic analysis of electronic data/electronic evidence assigned to it by the ITD and submit a report in writing.
- 7.2 Service Provider shall carry out restoration & analysis as per Standard Operating Procedure as issued by o/o PDIT(Inv.) Bangalore from time to time for handling of digital evidence, and as per legal requirements to preserve the legal sanctity and evidentiary value of the data/electronic evidence. Service Provider shall carry out forensic acquisition, restoration & analysis as per prevailing industry technical standards for handling digital data and devices. The standards should meet the legal requirements of Bhartiya Sakshya Adhiniyam,2023 and any guidelines that may be issued by the ITD to preserve the legal sanctity and evidentiary value of the data/electronic evidence. A fair extraction of the data should be carried out. **Any deviation from the standards shall lead to penal actions which can range from blacklisting of the vendors to prosecution under the relevant laws**
- 7.3 The report, after analysis, will, inter alia, categorize/group electronic data as under :

### 7.3.1 Deleted data :

- All types of files including mails/excel files/Doc. files/ PDF files/Scanned Images/Pictures etc.
- Data files for TALLY or any other accounting software like ERP Packages.
- Data Files with respect to any database software like SQL, Post GRESQL, Microsoft Access etc.
- Data hidden in unallocated sectors/Data hidden in pictures or scanned images.
- Data in mobile phones, tablets, pen drives or any other electronic devices.
- Encrypted Data/Password Protected Data including excel files/Doc Files/PDF Files/RAR Files/ZIP Files etc
- Log Files including Circular Logs/Flat Logs

### 7.3.2 Non-deleted data:

- All types of files including mails/excel files/Doc. files/ PDF files/scanned Images/Pictures etc.
- Data files for TALLY or any other accounting software like ERP Packages.
- Data Files with respect to any database software like SQL, Post GRESQL and Microsoft Access etc.
- Data hidden in unallocated sectors/Data hidden in pictures or scanned images.
- Data in mobile phones, tablets, pen drives or any other electronic devices.
- Encrypted Data including excel files/Doc Files/PDF Files/RAR Files/ZIP Files etc
- Log Files including Circular Logs/Flat Logs

7.4 Report shall specify the exact path of the files, salient features/ peculiar characteristics /time signatures, hash values etc

7.5 The Service Provider shall also aid in carrying out such investigation as required by Investigation Officer including password removal and breaking, text Search, forensic analysis of software system and incorporate the outcome along with its basis in the report

8. **Specific requirements for Manpower and Technical Resources** : In respect of the above, the service provider shall deploy qualified Manpower & utilize latest software and hardware tools

8.1 The Service Provider shall use original, authentic and licensed/authorized hardware and software tools for the purpose of legally sound forensic analysis of electronic data/electronic evidence for fair extraction of data. The service

provider shall not use pirated software or unlicensed tools. The tools should be state of the art with licenses purchased for automatic upgrades as and when they are rolled out. The tool(s) should have full capability for the following:

- i. Analysis of mobile data including images, screenshots, voice messages etc and extraction of data including WhatsApp/Telegram/Other messaging app messages (or a method to access all such messages) in all devices including Apple, Android and Blackberry devices (to the maximum possible extent of breaking encryptions).
- ii. Recovery and restoration of all data from all sectors of the electronic media and devices.
- iii. Recovery and restoration of all forms of email on the cloud and mail servers or laptops in OST, PST, DBX, MBOX, MSG, EML, TXT, RTF, HTML, MHTML and other formats.

8.2 Irrespective of the tools utilized for data extraction and analysis, the service provider shall ensure that the forensic analysis data is provided to the investigation officer in a readable and accessible digital format on the device specified by the investigating officer.

8.3 The vendor should have at their disposal the following tools (or similar priced ones) as shown in the in the table below :

| Sl. No | Tools   | Same or similar globally accepted tools  |
|--------|---|--|
| 1      | Hardware Write Blockers                         | CRU Write blocker/Tableau write blocker  |
| 2      | Software write blockers                         | Safe Block   |
| 3      | Forensic <i>Hardware</i> based Imager & cloners | Falcon imager/ Logic Cube Tableau Imager TD3/Tableau Imager, Magnet, Paraben, TX 1   |
| 4      | Forensic <i>Software</i> Imagers/ Cloners       | Encase 7 & above, Forensic Tool kit, Magnet axiom, Paraben forensic replicator etc.  |
| 5      | Forensic Software Imagers/ Cloners for Apple    | Macquisition for Mac, Recon imager for Mac, Paladin for Mac  |
| 6      | Forensic Data Extraction Platforms              | Xways Forensics, OS Forensics, Encase, Forensic Tool Kit, Magnet Axiom etc.  |
| 7      | Data recovery                                   | X-Ways Forensics/ Encase/Forensic Tool Kit   |
| 8      | Mobile Phone Acquisition and platforms          | Cellebrite UFED touch/ UFED 4PC; Oxygen Investigator/ detective; MobileEdit Express/ MagnetAxiom with Mobile Forensics module, Paraben Device seizure, Encase Mobile |

|    |  |  |
|----|--|--|
| 9  | Licensed mobile data/backup tools  | UFED Physical analyzer/ Oxygen detective   |
| 10 | Mobile Phone Data Recovery tools for Apple, android and other Mobile OS  | Phone Rescue, Dr.Fone, etc.  |
| 11 | Data recovery and Deleted file recovery tools                            | Ontrack data recovery, Stellar Data Recovery, 7 safeData Recovery, Disk driller for Mac, etc.  |
| 12 | Cloud Data acquisition tools   | Intella, Mail Xaminer, Nuix analyser, SPF, Magnet Cloud, F response, UFED cloud analyser, Encase Cloud, FTK Cloud                                |
| 13 | Non forensic Backup tools  | Macrium Reflect, Acronis True Image, NortonGhost etc.  |
| 14 | Email acquisition tools  | Paraben Email analyser, Mail Xaminer, OS forensicSoftware, Intella email Platform etc.   |
| 15 | Other Relevant Tools including Database Migration                        | SQL rebuilder/ Oracle Extractor, DB2 Analyser etc.   |
| 16 | AI based Data Analysis Tools for data mining, analysis and visualisation | RapidMiner, Tableau, Microsoft Azure Machine Learning, KNIME, Google Cloud AutoML, PyTorch, DataRobot, Talend, H2O.ai, IBM Watson Analytics etc. |

**8.3.1** Tools given above are only a representative list. Alternative tools with same or similar capability can be considered as replacement with approval of the Department. The Vendor should provide proof of the existence of the above-mentioned tools or provide financial viability to purchase the required licenses and provide proof that such tools have been procured within 2 weeks from the work order. The vendor should be able to provide ad hoc tools that may be required from time to time during the period of the existence of the Contract.

**8.3.2** It is emphasised here that preference shall be given to Data Analysis service providers who can deploy AI based tools using deep learning algorithms to find patterns in the Dataset which have immediate value to the investigation, or using machine learning to enable more accurate and self-improving keyword search and, since common themes and modus operandi are seen across different searches, such tools should enable utilisation of machine learning/deep learning acquired during one search in subsequent searches/projects

9. **Qualifications/skill requirements of Service Provider Personnel :**

9.1 The Service Provider should have qualified digital forensic specialists with minimum 3 years of experience preferably handling the cases relating to Investigation Wing of Income tax Department or other Central/State Enforcement Agencies and should possess all updated forensic instruments such as oxygen forensic, encase etc.

9.2 The vendor should provide the **list of engineers** (with their qualifications and experience) who are part of the team with the tender. Any new person will have to be cleared by the department before being inducted into the team.

9.3 **Forensic Analysis :**

9.3.1 The Service Provider shall carry out the acquisition/imaging, restoration & analysis as per the Standard Operating Procedure of the department and as per the legal requirement to preserve the legal sanctity of the data. The Service Provider shall carryout following work as assigned by this Directorate and submit a report in writing :

- i. Forensic acquisition / Imaging of different types of storage media such as hard Drives, USB thumb drives, CDs/DVDs, Tablets, Servers etc. Gathering evidence and information including deleted files, cracking passwords from suspected computer/ source with hash value report generation and preparing separate working copy by using legal and most efficient and updated forensic tools.
- ii. Email Forensics: Indexing of mails, time-line analysis, keyword searching.
- iii. Mobile Forensics : Logical and Physical extraction of mobile phones/ all kinds of smart phones including I-phones, I-pads etc, data extraction and analysis, SIM card analysis.
- iv. On-site mapping and securement of IT infrastructure.
- v. Detection of various accounting software systems per premise.
- vi. ERP (SAP/Tally/others/custom ERP software) data acquisition.
- vii. Live analysis and report generation on accounting/ERP database.
- viii. Software code analysis to detect suppression of reported income.
- ix. Enterprise wide data searches for specific search terms.
- x. Detection and analysis of Cloud Data sources.
- xi. Automated backup of specific files types.
- xii. Analysis of forensic artefacts for user activity mapping on computers.
- xiii. SQL scripting for relational database analysis.
- xiv. Custom scripting for mobile data analysis.
- xv. Acquisition and analysis of CCTV dumps.
- xvi. Analysis of deleted/Non deleted data of Excel files/Doc files/PDF files/Scan images. Data files for TALLY or any other accounting application. Data hidden in unallocated sectors/Data hidden in pictures.

- xvii. Analysis report shall also specify the location of files. Resources shall also carry out such investigation as required by Investigation Officer including password breaking & Text Speech.

**9.3.2** The Service Provider personnel required for forensic analysis of electronic data/electronic evidence which include off-site restoration and examination of electronic data/electronic evidence must possess at least the minimum knowledge and skills required for this purpose as enumerated below.

- i. Degree/ MS in Computer Forensic from a recognized institute.
- ii. Proficiency in accountancy including proficiency in financial statements, financial tables/charts/excel based files and jobs of similar nature.
- iii. Proficiency in using forensic hardware and software tools like Lazesoft, Windows Shell, bash, Nirxlauncher, FTK Imager, Belcasoft, Dumpit, Password Recovery, Oxygen, Cellebrite, hardware based forensic cloners and imagers like Tableau TX1, Tableau TD2u, Magnet Axion, OpenText Encase, Mobile phone acquisition, backup, data recovery tools for Apple, Android based devices like Cellebrite UFED 4PC etc.
- iv. Well versed with relevant laws applicable to the area of electronic evidence including relevant provisions of the Information Technology Act, The Bharatiya Sakshya Adhiniyam, 2023.
- v. Proficiency in using Tableau duplicators, Encase forensics, Password, write-blockers and other latest tools.
- vi. Proficiency in Relational Database Management Systems like Oracle/Microsoft SQL, etc. Knowledge of MS SQL & MySQL.
- vii. Proficiency in TALLY/ERP and similar accounting software tools including latest tools such as SAP, etc.
- viii. The personnel deployed should be proficient in usage of various types of digital systems including mobile phones, memory chips/cards, cloud computing systems, servers, other remote data systems/networks/ Nirxlauncher etc
- ix. Proficiency in assessing electronic data/files/records/emails/chats/communications/images i-cloud etc. including by way of breaking of passwords and forensic & financial analysis of the same.
- x. The forensic team at its backend should have members from financial background like CA/CFA/CS to assist in digital forensic analysis
- xi. Proficiency in various versions of Operating Systems like Windows, Linux, MacOS, Android, Ios etc

**9.3.3** The forensic team provided by each Service Provider shall preferably have at least 10 (ten) members comprising of :

- i. At least 5 (five) technical persons with necessary qualifications and having knowledge of accounting, forensic and computer.
- ii. No under trainee personnel shall be deployed to execute the project work

9.4 **Data Analysis** : The Service Provider personnel required for data analysis must be qualified data analysts and possess at least the minimum knowledge and skills required for this purpose including the following :

- i. Ability to gather, view, and analyze large volume of data that may be present in various disparate formats.
- ii. Proficiency in spreadsheet programs like MS Excel.
- iii. Knowledge of Python, Power BI, SQL, R and MATLAB.
- iv. Skilled at data visualization and capability to present reports in a format as required. Should be skilled at creating clean, visually compelling charts that will help understand the data.
- v. Strong logical skills and statistical knowledge

9.4.1 The Service Provider should be able to perform Review and Analysis of Data which shall include, but not be limited to, Bank Statement Analysis, Analysis of emails, social media chats, financial data on applications like Tally, Tally ERP, SAP, Oracle or any other customised RDBMS application using software tools, database Analysis through software tools etc., relationship resolution & presentation of analysed data. Discovery of patterns in the data including the financial data using AI based or any other relevant tools.

10. **State-of-the-Art Cyber Forensics Lab and training of ITD officials:**

10.1 **Cyber Forensics Lab and the requirement to meet state-of the art best practices:** Preference will be given to Service Providers who can deploy servers/solutions on which data of multiple projects/ searches as available with the investigating officers can be kept for an all data or device-cluster keyword search using big data analytics. The PDIT(Inv.) Bangalore charge will be establishing/upgrading a Cyber Forensics Lab to meet all requirements of data extraction and analysis using high end servers for simultaneous processing using device clusters for faster and more accurate and high-fidelity data analysis and retrieval/turnaround. Prospective Service Providers should have the capacity to seamlessly integrate their data forensics and analysis tools with the platforms made available at the CFL and work in compliance with the SOPs/guidelines in place and/or as issued from time to time by the o/o PDIT(Inv.) Bangalore, and the work environment conditions with a view to optimally utilize the processing possibilities of the CFL.

10.2 **Training of ITD officials :** ITD human resource has had a long learning curve by way of years of collective experience in data forensics, there are frequent and continuous changes/improvements in the state of the Art, which requires that the learning curve should be steeper. In order to build synchrony with the Investigation teams, the Forensic service providers shall take up free-of-charge training sessions to give hands-on training to ITD officers/officials so as to acquaint them with the latest technological advancements in the areas of data imaging, extraction and analysis, covering various architectural designs of databases, procedural issues, and software tools for all requirements of data

retrieval, integrity, back-up, and analysis. Every month a minimum 3 such sessions shall be taken at the CFL by qualified/certified trainers engaged by the Service Providers using live examples from situations faced during searches.

**11. Capacity to deploy Forensic teams at distant geographical locations anywhere in the Country at short notice and perform Onsite forensic analysis of electronic evidence/during search operation :**

- 11.1** In addition to the forensic analysis of electronic data/electronic evidence which the Service Provider would generally be required to do in the Income-tax Office, it may be required to do these activities at the site out of the office as well. For this purpose, whenever required, Service Provider should be able to depute sufficient number of technically qualified personnel with requisite hardware and software tools at short notice for onsite forensic analysis. Further, Onsite Forensic analysis may include sites out of Bengaluru (anywhere in the Country). Accordingly, the Service Provider shall ensure that adequate number of technically qualified personnel are made available as and when required by the ITD at the site located anywhere in the country.
- 11.2** The Service Provider personnel are required to use their own hardware excluding storage devices (hard disk, pen drive etc.) and software tools for imaging/back up etc. for the above purpose. The Service Provider shall ensure that the hardware and software tools are of high quality. The storage devices (hard disk, pen drive etc.) shall be provided by the ITD
- 11.3** Further, for onsite acquisitions/ Out of office duties :
- i. No prior notice may be given to service provider for out of office duty. They may be moved to any site without prior notice. The service provider is to be ready to provide services at short notice at any time including odd hours
  - ii. The Service Provider personnel may have to accompany the search & survey teams for the above purpose. The Directorate shall arrange for transport of resources for out of office duties. Such arrangements, to the extent possible, shall be at par with what is usually arranged for Inspectors of Income Tax
  - iii. For out of office premises duty, no additional remuneration or charges shall be payable to the Service Provider/Service Provider personnel.
  - iv. Out of office duty may stretch multiple days at a time. Service Provider shall ensure that the personnel are made available for the entire duration for proper conduct of official work of ITD.
- 11.4** It is also highly necessary that the successful Forensic service providers once empanelled at Bangalore, should be able to engage with their counterparts empanelled by other DGIT Charges so as to get their services with the same procedural rigour and quality as has been mandated by PDIT(Inv.) Bangalore. In other words, in case services of another vendor engaged by another DGIT Charge anywhere in India, are necessitated to be hired for the reason that the

search premises lies in the other jurisdiction /or any remote station, where the Bangalore Service provider is unable to provide its manpower, then the Bangalore Service provider shall be responsible for ensuring that the quality of service provided by the other/outside vendor is at par with that expected of the Service provider at Bangalore and all SOPs and other guidelines for handling digital evidence as issued by the o/o PDIT(Inv.) Bangalore are strictly adhered to by that other /outside vendor.

**12. Other mandatory conditions and general Instructions for the prospective service providers**

- 12.1 The Service Provider should have qualified digital forensic specialists with minimum 3 years of experience preferably handling the cases relating to Investigation Wing of Income tax Department or other Central/State Enforcement Agencies and should possess all updated forensic instruments such as oxygen forensic, encase etc. Number of digital forensic specialists available with the applicant should be indicated with the bid.
- 12.2 The Service Provider should have a reputed client base. The client list should be submitted with the bid
- 12.3 The Service Provider should ensure that the resource persons are made available as and when required by the officers of the office of the Principal Director of Income Tax (Investigation), Bangalore. The vendor should make available full time resources (which is typically 10 people) plus additional resources as required during the course of search and survey operations.
- 12.4 As and when required, the Service Provider's resource person should be ready to travel to any premises within India, and assist them for acquiring of data, retrieval, analysis etc., including requisition at very short notice.
- 12.5 The Service Provider should ensure compliance of strict confidentiality of data and procedures, as the matter dealt with will be of high sensitivity and utmost importance.
- 12.6 The Income Tax Department reserves the right of accepting the whole or any part of the quotation received and the Bidder shall be bound to perform the same at the rates quoted.
- 12.7 A consolidated bill will be submitted after completion of the work for payment. The bills will be countersigned by the relevant officers before submitting the same for financial sanction. The bills will be cleared within a reasonable time. However, in case of any unexpected delay, the contractor should be in a position to offer credit facility for the period. The guidelines and SOP issued in this regard shall be compiled with by the Service Provider. Also, Service Provider shall mandatorily comply with the Feedback form and payment methodology binded to the feedback form.
- 12.8 TDS will be made as per law.

- 12.9 The contract can be terminated at any time after giving one-month notice without assigning any reason by the Department and two months' notice by the contractor.
- 12.10 If the performance of the personnel provided by the Service Provider is not found satisfactory, the Principal Director of Income-tax (Inv), Bangalore shall have power to terminate the contract with one month's notice.
- 12.11 The Service Provider shall not subcontract or permit anyone other than himself to perform any of the work, service or other performance required of the Service Provider under the contract.
- 12.12 Once the project has concluded/or contract is terminated, the Service Provider shall not keep any data or metadata pertaining to it in any format or in a medium which can be recovered or restored through any means. The certificate and evidence to this effect shall be presented to the department in every project and the violation of the same shall attract severe penal action against the Service Provider. The service provider shall enter into a separate Non-disclosure agreement with the O/o PDIT(Inv.), Bangalore

**13. Indemnity Conditions and termination conditions**

- 13.1 Any change in the constitution of the concern of the Service Provider shall be notified forthwith by the Service Provider in writing to the Income-tax Department and such change shall not relieve any former member of the concern from any liability under the contract.
- 13.2 The Service Provider shall acknowledge that it has made itself fully acquainted with all the conditions and circumstances under which the services required under the contract will have to be provided and the terms, clauses and conditions, specifications and other details of the contract. The Service Provider shall not plead ignorance on any matter as an excuse for deficiency in service or failure to perform or with a view to asking for increase of any rates agreed to the contract or to evading any of its obligations under the contract. In the event of the Service Provider failing to fulfil or committing any breach of any of the terms and conditions of this contract or indulge in following omission or commission then without prejudice to the Income-tax department's rights and remedies to which otherwise, Income-tax department, shall be entitled, the contract shall be terminated forthwith.
- 13.3 The ITD shall have the right to blacklist such defaulting Service Provider and execute the work or arrange otherwise, at the Service Provider's risk and at the absolute discretion of the Income- tax Department. The cost of such works together with all incidental charges or expenses shall be recoverable from the Service Provider:
- If the Service Provider or its agents or employees are found guilty of fraud in respect of the contract or any other contract entered into by the

Service Provider or any of his partners or representatives thereof with the Income-tax Department; or

- If the Service Provider or any of its partner becomes insolvent or applies for relief as insolvent debtor or commences any insolvency proceedings or makes any composition with its/their creditors or attempts to do so; or if
- At any time during the pendency of the contract, it comes to the notice of the Income-tax Department that the Service Provider has misled it by giving false/incorrect information

**13.4** The Service Provider shall comply with all statutory liabilities and obligations of State and Central Government. The Income-tax Department shall not be liable for any contravention/non-compliance on the part of the Service Provider. Any contravention/non-compliance on the part of the Service Provider would be construed as a sufficient ground for termination of the contract at the discretion of the Income-tax Department. Notwithstanding, in the event of the Income-tax Department being imposed with any penalty/fine etc., by any Service Provider/authority due to the non-compliance/contravention on the part of the Service Provider to any statutory laws/rules/regulations etc., the Income-tax Department reserves the right to recover such fine/penalty etc., from the Service Provider by way of recovery from the bills raised by the Service Provider or by any other means.

**13.5** The Income-tax Department may discontinue the contract at any point of time, by giving a notice at least 30 days before the intended date of discontinuation, without assigning any reason and will not be liable to any additional charges or compensation payable to the Service Provider or any other person.

**13.6** The Service Provider may discontinue the contract at any point of time, by giving a notice at least 60 days before the intended date for discontinuation. But, in case of discontinuation without a notice or a notice less than 60 days prior to the intended date of discontinuation, the Income-tax Department will have the right to claim damages, and recover them from the payments due to the Service Provider or by any other means.

#### **14. Security Deposit/ Bank Guarantee :**

**14.1** The ITD reserves the right to impose any such other conditions on the Service Providers who are finally empanelled for the works in order to safeguard the interest of the Department and the Govt. of India. Such **administrative and financial conditions** may include, inter alia, **additional indemnity clauses** and the pre-requisite of a **Earnest Money Deposit /Security Deposit/ Bank Guarantee** for enforcement of necessary discipline and to effect recovery of damages in the event of non-performance and /or violation on the part of the service provider. Such other conditions shall be enumerated and elaborated and the same shall be complied with by the Service Provider.

15. **Tenure of the contract :** Initially, this agreement shall remain in force for a period of **36 months with effect from 01<sup>st</sup> December 2024 to 30th November 2027**, with the provision of extending it by another two years at the administrative convenience of the Pr. Director of Income Tax (Inv.), Bengaluru, subject to satisfactory performance
16. **Arbitration :** In the event of any dispute or differences arising as to the execution of the contract or as to the respective rights or liabilities of the parties hereto or interpretation of any of clause thereof on any condition of agreement (except as to any matters the decision of which is specially provided for or the special conditions), the dispute shall be resolved in accordance with the provisions of the Arbitration & Conciliation Act, 1996 and the Rules there under and any statutory modifications thereof, for the time being in force, shall deemed to apply to the arbitration proceedings. The award of the arbitrator shall be final and binding on parties to the agreement
17. **Terms of Payment :**
- 17.1 The Service Provider shall keep a proper and comprehensive account of the resources deployed for the forensic analysis of electronic data/electronic evidence which will have to be verified by the Investigating Officer. **The details of the resources deployed should be presented for accounting for the verification of time spent each resource along with justification for the time spent by each resource on the concerned project. Only after this verification and presentation of proper justification, the invoices will be cleared for payments. The payments shall be on the basis of Feedback form and the payment methodology linked to it.**
- 17.2 The Service Provider shall conduct daily meetings at the end of each work day with the investigating officer to present him with the progress made in the analysis and submit a report of the major findings and the man hours spent and charged to the department. The Service Provider shall also conduct a meeting with the Unit head on a weekly basis and present him with the major findings and the amount charged to the department and the resources deployed in the week. No payment shall be made to the Service Provider if it is found that such meetings have not been conducted and the Investigating officer as well as the unit head have not been kept duly informed about the progress of the project find major findings made.
- 17.3 The Service Provider shall maintain a worklog at mid action points verified by the Authorized Officer at the premises. Similarly, for post search activity, a worklog is to be maintained and verified by processing Investigating Officer. The work log should capture the work performed, the name of person from the service provider who is performing the work, the start time, the end time, the tools utilised etc., the worklog should match the bill raised by the service provider.
- 17.4 Once the project has concluded, the Service Provider shall not retain with it any data or metadata pertaining to it in any format or in any medium which can be later recovered or restored through any means. The Service Provider

should actively eliminate and destroy any traces of data relating to the project undertaken immediately after the completion of project. Further, a certificate to this effect shall be presented to the ITD in every action along with the bill and any violation of the same shall attract severe penal action against the Service Provider, including cancellation of the empanelment. Also, recovery of damages from the Security Deposit shall be made in the event of non-performance and /or violation on the part of the service provider.

- 17.5 A consolidated bill will be submitted after completion of the work for payment. The bills will be countersigned by the relevant Officers before submitting the same for financial sanction. The bills will be cleared within a reasonable time. However, in case of any unexpected delay, the contractor should be in a position to offer credit facility for the period. **The payments shall be on the basis of Feedback form and the payment methodology linked to it.**
- 17.6 Bills pertaining to mid-search actions and post-search actions should be put up separately, clearly stating the nature of actions carried out.
- 17.7 For out of office duty, no additional remuneration or charges shall be payable to the Service Provider/Service Provider personnel.

#### 18. Non-Disclosure Clauses :

- 18.1 **Prohibition on illegal and/or unauthorized usage of Income Tax ITD data:**  
It must be clearly understood that all data imaged/retrieved/extracted/taken/acquired/accessed from the search premises and/or provided by the officer concerned for data retrieval/storage/extraction/clustering/analysis/any service (by whatever name called) to the Service provider shall be **termed as ITD data and shall belong only and only to the ITD or o/o the PDIT(Inv.), Bangalore.** Such data shall in no way or form be kept in the personal custody of the service provider / personnel deployed by service provider, shall not be copied/printed without the explicit approval and direction of the concerned officer, shall not be taken/moved/transmitted/deleted/modified/manipulated/merged/removed by the service provider.
- 18.2 The Service Provider personnel shall act for and on behalf of the PDIT and shall not make any copy of data held by the ITD in any form and/or manner, in an unauthorized way.
- 18.3 The Service Provider personnel shall not hold data of the ITD with them independently at any point of time. Such possession will tantamount to illegal and/or unauthorized usage whether actually used or not.
- 18.4 If Service Provider personnel misuse the data or indulge into illegal and/or unauthorized usage of data or cause a deliberate act of omission or commission, they/Service Provider shall be liable for prosecution under applicable laws in addition to **cancellation of the empanelment** and other consequences, without any notice. Further, they/Service Provider may be blacklisted **from providing any service to the PDIT in future.**

- 18.5 The clauses regarding illegal and/or unauthorized usage of data are very important and may be noted by Service Provider with due care, as the PDIT office attaches great importance to sensitivity and confidentiality of the data.
- 18.6 The service provider and its resources are expected to ensure complete confidentiality and integrity of the ITD data. Hence, any breach or likely event which may damage the reputation of the Department of integrity of the search/survey operations of the Department would be make the service provider liable for damages, without prejudice to other actions that may be initiated by the department
- 18.7 The (Indian) Information Technology Act, 2000 deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data and the Service Provider and its personnel shall be accountable for any lapses.
- 18.8 Further, under section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances. This shall also be applied for the Service Provider and its personnel and shall be accountable for any lapses. Section 43A of the (Indian) Information Technology Act, 2000 is hereby reproduced for more clarification in this regard

*[43A Compensation for failure to protect data. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, Such body corporate shall be liable to pay damages by way of compensation to the person so affected.*

*Explanation. - For the purposes of this section:*

- (i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities:*
- (ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or*

*impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the*

*Central Government in consultation with such professional bodies or associations as it may deem fit;*

*(iii) "Sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.*

- 18.9** Section 66 of the (Indian) Information Technology Act, 2000 provides that if any person, dishonestly or fraudulently does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to Rs. 5,00,000) or with both. This shall also be applied for the Service Provider and its personnel and shall be accountable for any lapses.
- 18.10** If any misconducts/malpractices of the Service Provider or and any of its personnel caused any loss/embezzlement of revenue to the government exchequer, the Service Provider shall be accountable for making this loss good and the PDIT (Inv.), Bangalore shall be empowered to recover it or take necessary action as deemed fit and or refer the case to the suitable enforcement agency for taking remedial action, if any, in this regard.
- 18.11** The Service Provider shall ensure that the evidentiary value of the devices/data imaged/seized/backed up is protected as per the requirements of Bharatiya Sakshya Adhiniyam,2023 and any other laws in place with regard to digital evidence and shall provide necessary certificate/documents as mandated by law to that effect. The Service Provider shall also provide the certificate for admissibility of electronic records/data under Section 63(4)(c) of the Bharatiya Sakshya Adhiniyam,2023.
- 18.12** If the service provider comes to know that its services are being utilized by the PDIT (Investigation) in the case of its works of clients or otherwise related to it. The service provider shall immediately inform the PDIT (Investigation) of possible conflict of interest and immediately disposes of all the data related to the case and refrain from providing services in the given case.
- 18.13** The service provider shall enter into a separate Non-disclosure agreement with the O/o PDIT(Inv.) Bangalore.

- 18.14 The SOP/guidelines issued for service providers by the PDIT(Inv.) Bangalore shall be followed by the Service Providers and any violation of the same may attract cancellation of their empanelment
19. No alteration shall be made in any of the terms and conditions of the bid document by scoring out. In the submitted bid, no variation in the conditions shall be admissible. Bids not complying with the terms and conditions listed in this section are liable to be ignored.
20. In the event of bid being accepted, the bid will be converted into a contract, which will be governed by the terms and conditions given in the bid document. The instructions to bidders shall also form part of the contract.
21. The terms and conditions given in Section-III & IV, along with profile of the applicant Service Provider, as prescribed in the **Annexure-A** of this tender document, shall be signed and returned in the envelope marked as '**Technical Bid**', otherwise the tender will be rejected.
22. The Income-tax Department does not bind itself to accept the lowest bid.

Read and accepted.  
Date Signature and stamp of the Bidder  
or Authorized signatory, Place

## **SECTION- V**

### **SCOPE FOR EMPANELMENT AND OTHER CONDITIONS**

1. The Tender is for Empanelment of Vendors.
2. If the different companies quote least prices in different categories. All the companies should be ready to match with the lowest prices quoted by other companies and should provide the service in lowest quoted price and also the company quoted the least should not have any objection of their price to be matched.
3. The Pr.DIT (Inv.), Bengaluru makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone. This Tender does not constitute an offer by the department. The bidder's participation in this process may result in selecting the L-1 bidder and further to invite other bidder for empanelment at L-1 rates. The commencement of such empanelment does not, however, signify a commitment by the department to award the bid. The department also reserves the right to accept or reject any bid, and to annul the bidding process at any time, without thereby incurring any liability to the affected Bidder or Bidders.
4. The offer is only for empanelment and the same would not amount to any work contract or surety with reference to allotment of work.

**SECTION-VI**

**TECHNICAL BID DOCUMENT**

|     |  |  |
|-----|--|--|
| 1.  | Name and address of the registered Agency  |  |
| 2.  | Name & Address of the Owner(s)   |  |
| 3.  | PAN & Service Tax Registration No.<br>(Proof to be enclosed)   |  |
| 4.  | Year of Commencement of Agency<br>(with evidence for having experience in Digital Forensic Services)   |  |
| 5.  | Copies of IT Returns along with Tax Audit Report in Form 3CD for AYs. 2022-23 and 2023-24  |  |
| 6.  | Year of formation/Year of Incorporation<br>(Proof to be enclosed)  |  |
| 7.  | Number of Digital Forensic Specialists available with qualification (to be enclosed with evidence of education qualifications and experience in Digital Forensic Services) |  |
| 8.  | Client list to be enclosed (with evidence of providing Digital Forensic Services)  |  |
| 9.  | Enforcement agencies who had taken services of the applicant in last 3 years<br>(Proof to be enclosed)   |  |
| 10. | Any other remarks  |  |

If response to any of the items mentioned at Sl.No. 1-9 above is not furnished or if any response to any item at Sr. No. 1-9 is negative, the bid may be rejected.

Signature of the Authorised Signatory

**DECLARATION**

I / We hereby certify that the information furnished above is full and correct to the best of my/our knowledge and belief. I/We understand that in case any deviation is found in the above statement at any stage, the agency will be blacklisted and may not be permitted to bid in future.

Signature of Authorized Signatory with date)

**SECTION-VII**

**FINANCIAL BID DOCUMENT FOR DATA FORENSIC WORK**

1. Name and address of the registered Agency :  
with telephone number of the applicant contractor
2. Permanent Account Number (PAN) :
3. Names and Addresses of the Proprietor/Partners/  
Directors and their PAN
4. Rate Chart (Exclusive of GST) :

**PART A**

(Rate for Forensic Services)

| S.No. | Category of Forensic Digital Device  | Device size/<br>Criteria            | Rate (in figures) | Rate (in words) |
|-------|--|-------------------------------------|-------------------|-----------------|
| 1.    | <b>PEN DRIVE:-</b>   |                                     |                   |                 |
| (a)   | Imaging/ Cloning of Pen drive data   | Any size/ Rate per device           |                   |                 |
| (b)   | Carving, Extraction, Indexing & Keyword filter of Pen drive data                       | Any size/ Rate per device           |                   |                 |
| (c)   | Analysis of Pen Drive data   | Any size/ Rate per hour             |                   |                 |
| 2.    | <b>E-MAIL:-</b>  |                                     |                   |                 |
| (a)   | Imaging/ back up of E-mail data irrespective of Domain (stored at local/ cloud server) | Up to 75 Gigabyte / Rate per device |                   |                 |
| (b)   | Imaging/ back up of E-mail data irrespective of Domain (stored at local/ cloud server) | Above 75 Gigabyte/ Rate per device  |                   |                 |
| (c)   | Carving, Extraction, Indexing & Keyword filter of E-mail data                          | Up to 75 Gigabyte/ Rate per device  |                   |                 |
| (d)   | Carving, Extraction, Indexing & Keyword filter of E-mail data                          | Above 75 Gigabyte/ Rate per device  |                   |                 |
| (e)   | Header and Data analysis of E- mail data   | Up to 75 Gigabyte/ Rate per hour    |                   |                 |
| (f)   | Header and Data analysis of E- mail data   | Above 75 Gigabyte/ Rate per hour    |                   |                 |
| 3.    | <b>MOBILE PHONES AND TABLETS:-</b>   |                                     |                   |                 |

|     |   |                                   |  |  |
|-----|---|-----------------------------------|--|--|
| (a) | Imaging/ Cloning of data of Mobile Phones and Tablets   | Any size/ Rate per device         |  |  |
| (b) | Carving, Extraction, Indexing & Keyword filter of data of Mobile Phones and Tablets                   | Any size/ Rate per device         |  |  |
| (c) | Analysis of data of Mobile Phones and Tablets   | Any size/ Rate per hour           |  |  |
| 4.  | <b>HARD DISK DRIVES, LAPTOPS AND DESKTOPS:-</b>   |                                   |  |  |
| (a) | Imaging/ Cloning of data of Hard Disk Drives, Laptops and Desktops etc.                               | Up to 1 Terabyte/ Rate per device |  |  |
| (b) | Imaging/ Cloning of data of Hard Disk Drives, Laptops and Desktops etc.                               | Above 1 Terabyte/ Rate per device |  |  |
| (c) | Carving, Extraction, Indexing & Keyword filter of data of Hard Disk Drives, Laptops and Desktops etc. | Up to 1 Terabyte/ Rate per device |  |  |
| (d) | Carving, Extraction, Indexing & Keyword filter of data of Hard Disk Drives, Laptops and Desktops etc. | Above 1 Terabyte/ Rate per device |  |  |
| (e) | Analysis of data of Hard Disk Drives, Laptops and Desktops etc.                                       | Up to 1 Terabyte/ Rate per hour   |  |  |
| (f) | Analysis of data of Hard Disk Drives, Laptops and Desktops etc.                                       | Above 1 Terabyte/ Rate per hour   |  |  |
| 5.  | <b>SERVER:-</b>   |                                   |  |  |
| (a) | Imaging/ Cloning, Extraction, Carving and Indexing  | Rate per Hour                     |  |  |
| (b) | Analysis of Server Data   | Rate per Hour                     |  |  |

Signature of the Authorised Signatory

## SECTION-VIII

### EVALUATION METHOD OF BID

#### **The criteria of selection as well as rejection.**

1. The bidder should fulfil eligibly criteria mentioned in Section-III of this document to be able to qualify for consideration at the stage of technical evaluation: i.e. Only those Bid(s) shall be treated as responsive bid(s) which fulfils all the criterion/parameters
2. Incomplete tenders would be rejected.
3. Tendering process shall be finalized only when there are at least three responsive bids.
4. In a normal situation, the contract shall be awarded to the lowest responsive bidder. However, mere lowest rates are not the sole criteria of selection. Income-tax department, Bengaluru, is not bound to accept the lowest rates.
5. Without affecting the sanctity of the above criterion, Income-tax department, Bengaluru reserves rights to relax any condition of eligibility criteria qualifying the bid(s) based on merit of each case and if the situation so warrants in the interest of the department.
6. Income-tax department, Bengaluru reserves the right to accept or reject any or all bids without assigning any reasons.
7. Income-tax department, Bengaluru also reserves the right to reject any bid (including the lowest one) which in its opinion is not responsive or violating any of the conditions/specifications or which is found to be adopting unethical business practices; without bearing any liability or any loss whatsoever it may cause to the bidder in the process.

#### **The parameters and process for Evaluation.**

1. The technical bids will be evaluated by the screening committee on the basis of following parameters.
  - (a) Past performance.
  - (b) Credentials.
  - (c) Financial capacity with respect to gross receipt.
  - (d) Evaluation of competency done by Tender Committee.
  - (e) Fulfilment of provisions of legal obligations.
2. Evaluation of these parameters shall be based on documents and information submitted by the bidders without recourse to extrinsic evidence.
3. Financial bids of those who qualify after the evaluation of technical bids by screening committee would be opened.

**PROFILE OF ORGANIZATION**

(To be submitted along with Technical Bid)

| Sl No. | Particulars  | Details |
|--------|--|---------|
| 1.     | Name of the Firm   |         |
| 2.     | Permanent Account Number/TIN No. (enclose copies)  |         |
| 3.     | Service Tax Registration No. (if any)  |         |
| 4.     | Full address, with email, Phone, Fax, Mobile Number  |         |
| 5.     | Name and address of Proprietor/Partners/Directors and their PAN  |         |
| 6.     | Year of Establishment of the Firm  |         |
| 7.     | Period of experience in the field of providing Digital Forensic Services   |         |
| 8.     | Details of services provided (enclose documentary proof of the same) with satisfactory completion certificates of the concerned organisations)                           |         |
| 9.     | Details of Demand Draft in respect of Earnest Money Deposit  |         |
| 10.    | Any other information in support of their past antecedent, present experience, approach & methodology of work, competency to execute contract, financial capacity etc... |         |

**Note:** Please attach extra sheet in support of your information, if space in the column is insufficient. It is requested to visit the site and ascertain the quantum of work before submitting the tender.

Also, the bidder is requested to submit the following:

- (a) Copy of the statement of accounts viz. balance sheet, Profit and Loss Account, audited if applicable, and Income tax return particulars of the bidder for the financial years 2021-22 & 2022-23 is to be submitted highlighting financial standing and turnover of the service provider.
- (b) A copy of PAN Card, GST Registration.
- (b) Information regarding any litigation, current or during the last three years in which the bidder was/is involved, the opposite Service Provider/party(s) and the disputed amount.
- (c) Details regarding any work order that was abandoned at any stage, prematurely terminated or resulted in inordinate delay along with reasons for the same (copies of relevant documents to be enclosed).
- (d) Details of similar works carried out in the last 3 years, including name of the organization, receipts Financial Year wise.
- (e) Letters if any, from concerned organization for outstanding work.
- (g) Earnest Money Deposit (EMD) of Rs. 30,000/- by means of demand draft drawn in favour of ZAO, CBDT, Bengaluru payable at Bengaluru.

Signature & Seal of bidder