

SCHEDULE Q (SUPPLEMENTARY TERMS)

NOTE TO SUPPLIER/TENDERER: FOR THE PURPOSES OF THE RFP, THIS DOCUMENT REQUIRES RESPONSES TO THE ITEMS SPECIFIED BELOW IN PART B. AS THIS DOCUMENT IS INTENDED TO BE APPLICABLE TO ALL SERVICE PROVIDERS AND GIVEN THAT EACH SUPPLIER MAY HAVE A DIFFERENT OFFERING, THE CONTENT OF THIS SCHEDULE WILL BE BASED ON SUPPLIER RESPONSES AND ESKOM MINIMUM REQUIREMENTS SET OUT IN PART A, WHICH WILL BE LEGALLY BINDING TERMS.

SUPPLIER NAME:	
TENDER NUMBER:	
TENDER DESCRIPTION:	
SUBMISSION DATE:	

This document contains confidential and proprietary information of Eskom and is “Eskom Confidential Information” for the purposes of the non-disclosure agreement entered into between Eskom and Supplier in relation to this Project. It is furnished for contract evaluation and award purposes only. Except with the express prior written permission of Eskom, this document and the information contained herein may not be published, disclosed, or used for any other purpose.

INSTRUCTIONS FOR RESPONDING TO THIS DOCUMENT:**General Guidelines**

- These RFP documents contain the key legal terms and conditions that the Supplier will be required to comply with in relation to this Project.
- Eskom requires the Supplier to comply with the requirements as written, and compliance with these RFP documents will be a critical component of Supplier's response to the RFP.
- The Supplier must complete Schedule Q (Supplementary Terms), as it is a mandatory requirement. Non-compliance will result in the Supplier being disqualified from further evaluation.

INTRODUCTION

This Schedule Q (Supplementary Terms) is, for purposes of the RFP, split into two parts, with Part A being minimum terms and conditions which the Supplier is required to adhere to and Part B being a questionnaire which the Supplier is required to complete. Based on the responses to Part B, and if agreed by Eskom, Part A will be supplemented and/or amended. For purposes of the ultimate agreement to be signed by the Parties, Part B will be removed, and the final agreed terms will be contained as in Part A.

PART A

1. PURPOSE

- 1.1. This Part A sets out the mandatory minimum requirements applicable to the provision of any hosted, outsourced, cloud based, hybrid or remotely accessed information technology services to Eskom.
- 1.2. This Schedule constitutes the minimum operating standards and shall apply in addition to, and not in substitution for, the provisions of the Agreement.
- 1.3. **No deviation** from this Schedule shall be of any force or effect unless expressly approved in writing by Eskom.

2. COMMENCEMENT OF SERVICES AND GO LIVE (IF APPLICABLE)

- 2.1. **[Drafting note: This clause will be updated at the time of contracting to reflect Eskom's requirements that the gap between Service implementation and go-live date be specified and that the Supplier will not be entitled to charge for ongoing/run Services until go-live.]**

3. SUSPENSION AND WITHHOLDING OF SERVICES

- 3.1. The Supplier shall not be entitled to suspend the Services under any circumstances, save only where such suspension is strictly required on an emergency basis to prevent or mitigate the effects of a disabling code.
- 3.2. Any emergency suspension shall be subject to:
 - 3.2.1. immediate escalation to Eskom;
 - 3.2.2. agreement on a defined restoration timeframe; and
 - 3.2.3. continuous communication until full-service restoration.
- 3.3. The Supplier shall not withhold or suspend the Services for any other reason whatsoever, including any dispute between the Parties.

4. RIGHTS IN RESPECT OF DATA

- 4.1. Eskom shall be and remain the Responsible Party and holder of all rights (including any Confidential Information, Personal Information to the extent applicable and other proprietary rights) in respect of all Eskom Data stored, transmitted, processed or generated by Eskom through use of the Services, including all derived data and outputs, shall at all times remain the exclusive property of Eskom.
- 4.2. The Supplier acquires no ownership, licence, usage or other rights in respect of Eskom Data, save strictly to the extent necessary to perform the Services.

5. PROHIBITED USE OF ESKOM DATA

- 5.1. The Supplier is strictly prohibited from using Eskom Data for advertising, marketing, analytics, artificial intelligence training, commercial exploitation or service improvement purposes.
- 5.2. The Supplier shall not anonymise, pseudonymise, de-identify, aggregate, sell, monetise or otherwise repurpose Eskom Data unless expressly authorised in writing by Eskom under separate agreed terms.

6. METADATA

- 6.1. All metadata generated through the upload, management, processing, migration, access or storage of Eskom Data shall vest exclusively in Eskom and shall remain the Confidential Information and proprietary information of Eskom.
- 6.2. Eskom shall be entitled to full access to such metadata during the Term and following Termination.

7. AVAILABILITY AND REGULATORY ACCESS

- 7.1. The Supplier warrants that the Services shall at all times meet Eskom availability, resilience and continuity requirements.
- 7.2. The Supplier warrants that availability shall be sufficient to enable Eskom to comply with all applicable access to information, regulatory, audit, records management, investigation and privacy obligations.
- 7.3. The Supplier shall permit lawful access to Eskom Data by competent authorities upon valid legal request.

8. DATA RESTORATION AND LIABILITY

- 8.1. The Supplier shall maintain documented and tested procedures for restoration of Eskom Data following any outage, corruption, loss or deletion.
- 8.2. In the event of any accidental deletion, corruption or loss of Eskom Data, the Supplier shall:
 - 8.2.1. immediately commence restoration;

8.2.2. restore the data at its cost; and

8.2.3. bear full liability without limitation for the consequences thereof.

9. **DATA STORAGE SECURITY**

9.1. The Supplier shall ensure that all Eskom Data is stored within a physically and logically secure environment which provides protection against unauthorised access, modification, misuse, theft, corruption and destruction.

9.2. The Supplier shall implement industry recognised technical and organisational safeguards which shall, at a minimum, comply with ISO 27001, ISO 27002 and SOC 2 standards.

9.3. Eskom reserves the right to specify additional security requirements at any time, acting reasonably and in accordance with applicable law.

10. **BACKUP OBLIGATIONS**

10.1. The Supplier shall perform backups of Eskom Data at intervals meeting or exceeding Eskom minimum requirements.

10.2. Backups shall be encrypted using cryptographic standards approved by Eskom.

10.3. Eskom shall have the right to audit the performance, frequency, integrity and recoverability of all backups.

10.4. The Supplier shall bear full responsibility for the recovery of Eskom Data following any accidental deletion, corruption, loss or failure, without limitation of liability.

11. **DATA INTEGRITY AND AUDIT TRAILS**

11.1. The Supplier shall implement controls to preserve the usability, reliability, authenticity and integrity of Eskom Data for the full duration of the Agreement.

11.2. File integrity controls, including checksum validation or equivalent controls, shall be implemented for all transfers of Eskom Data.

11.3. The Supplier shall maintain full system audit trails in respect of all access to, processing of, modification of and transmission of Eskom Data.

11.4. Eskom shall be entitled to access all audit trails during the Term and following termination for regulatory, investigation and evidentiary purposes.

12. **DATA RETENTION**

12.1. The Supplier shall comply with all Eskom Data retention policies as amended from time to time.

- 12.2. Eskom shall be entitled to direct the Supplier in writing to retain specified Eskom Data for legal, regulatory or investigation purposes.

13. SECURE DESTRUCTION OF DATA

- 13.1. Upon Termination or expiry of the Agreement for any reason, and once Eskom has confirmed successful migration, the Supplier shall immediately and permanently destroy:

13.1.1. all Eskom Data;

13.1.2. all copies;

13.1.3. all backups; and

13.1.4. all associated metadata.

- 13.2. Destruction shall be performed in a manner that prevents reconstruction.

- 13.3. The Supplier shall provide Eskom with a signed certificate of destruction confirming full compliance.

14. GENERAL SECURITY OBLIGATIONS

- 14.1. The Supplier shall ensure that its systems prevent unauthorised access to Eskom Data at all times.

- 14.2. Eskom reserves the right to audit the Supplier environment, including unannounced penetration testing.

- 14.3. The Supplier shall immediately notify Eskom of any security compromise, vulnerability, suspected breach or system malfunction.

15. SUBCONTRACTORS

- 15.1. The Supplier shall not appoint any subcontractor who will have access to Eskom Data without Eskom prior written approval.

- 15.2. All approved subcontractors shall be bound by back-to-back confidentiality, security, POPIA and data protection obligations.

- 15.3. The Supplier shall remain fully liable for all acts and omissions of its subcontractors.

16. INFORMATION SECURITY STANDARDS

- 16.1. The Supplier shall maintain current security certifications including ISO 27001 and SOC 1 Type II and SOC 2 Type II.

16.2. The Supplier shall conduct annual penetration testing and red team exercises and remediate all identified vulnerabilities.

16.3. The Supplier shall make all its security policies, procedures and standards available to Eskom for review.

17. POPIA AND PRIVACY COMPLIANCE

17.1. The Supplier warrants that it shall comply with all applicable privacy and data protection laws including POPIA.

17.2. The Supplier shall process personal information only on documented instructions from Eskom.

17.3. The Supplier shall implement appropriate technical and organisational measures to secure personal information.

17.4. The Supplier shall not transfer personal information to third parties without Eskom prior written consent.

18. CLOUD SECURITY CONTROLS

18.1. The Supplier shall ensure that:

18.1.1. Eskom Data shall be encrypted at rest and in transit using industry recognised encryption standards.

18.1.2. Multi factor authentication shall be mandatory for all privileged and production access.

18.1.3. Role based access control shall be enforced at all levels.

18.1.4. Administrator activity shall be fully logged and auditable.

18.1.5. Segregation of duties shall be enforced between development and production environments.

19. DATA LOCALISATION

19.1. All Eskom Data shall be stored and processed within borders of the Republic of South Africa unless expressly approved in writing by Eskom.

19.2. Offshore data transfers are prohibited except as a mere conduit.

20. FOREIGN JURISDICTIONS

20.1. Eskom reserves the right to prohibit transfers to specified foreign jurisdictions.

20.2. The Supplier shall remain fully liable for all foreign processing risks.

21. DATA CENTRE OPERATORS

21.1. Where any third-party data centre is used, the Supplier shall be jointly and severally liable for all acts and omissions of such operator.

21.2. Eskom reserves the right to reject any proposed data centre.

22. EXIT ASSISTANCE

22.1. Upon termination, the Supplier shall provide full exit assistance to enable seamless migration of Eskom Data and Services.

22.2. The Supplier must ensure that data shall be transferred in interoperable formats at no additional cost.

22.3. The Supplier shall provide sufficient lead time to avoid service interruption.

23. DISASTER RECOVERY

23.1. The Supplier shall maintain tested and documented disaster recovery and business continuity plans.

23.2. Recovery Time Objectives and Recovery Point Objectives shall be contractually agreed.

23.3. All disaster recovery sites shall comply with this Schedule in full.

24. INSOLVENCY AND FINANCIAL RESILIENCE

24.1. The Supplier shall provide financial viability reports upon request.

24.2. Eskom may terminate immediately upon business rescue or liquidation.

25. SERVICE LEVELS

25.1. The Supplier shall provide service levels addressing uptime, planned downtime, response times, resolution times, data return and service credits.

25.2. Failure to meet service levels shall trigger contractual remedies.

26. INSURANCE

26.1. The Supplier shall maintain cyber liability, technology errors and omissions and crime insurance.

26.2. Eskom shall be named as an additional insured.

27. INDEMNITIES AND LIABILITY

27.1. The Supplier shall defend, indemnify and hold Eskom harmless against all losses arising from:

- 27.1.1. data breaches;
- 27.1.2. cyber incidents;
- 27.1.3. privacy violations;
- 27.1.4. regulatory penalties; and
- 27.1.5. system compromise.

28. INTELLECTUAL PROPERTY INDEMNITY

- 28.1. The Supplier shall indemnify Eskom against all third-party claims of intellectual property infringement relating to the Services.

29. DEVIATIONS

- 29.1. Any deviation from this Schedule requires prior written approval from Eskom.
- 29.2. All mitigation arising from any approved deviation shall be implemented at no additional cost.

30. LEGAL STATUS

- 30.1. This Schedule constitutes mandatory minimum contractual standards.
- 30.2. Non-compliance with this Schedule shall constitute a material breach of the Agreement.

SUPPLIER ACCEPTANCE OF PART A

The Supplier acknowledges and confirms that:

1. It has read, understood and evaluated all provisions contained in **Part A** of this Schedule Q (Supplementary Terms);
2. It accepts and agrees to be bound by all provisions of **Part A** in full, without qualification, reservation or deviation, unless expressly approved in writing by Eskom;
3. It understands that **Part A** constitutes mandatory minimum contractual requirements and will form part of the final agreement between the Parties;
4. Any response provided in Part B does not amend, limit or override the provisions of Part A unless such deviation is expressly accepted in writing by Eskom;
5. The Supplier further confirms that no reliance will be placed on any standard terms, policies or conditions (including click-wrap, shrink-wrap or online terms) that are inconsistent with or purport to override the provisions of **Part A**.

Duly authorised representative of the Supplier:

Supplier Name:

Date:

Name:

Designation:

Signature:

PART B

[NOTE TO SUPPLIER: FOR THE PURPOSES OF THE RFP, THIS DOCUMENT REQUIRES RESPONSES TO THE ITEMS SPECIFIED BELOW. AS THIS DOCUMENT IS INTENDED TO BE GENERIC IN NATURE AND THEREFORE APPLICABLE TO ALL SERVICE PROVIDERS, AND GIVEN THAT EACH SUPPLIER MAY HAVE A DIFFERENT OFFERING, THE CONTENT OF THIS SCHEDULE WILL, BASED ON SUPPLIER RESPONSES AND ESKOM MINIMUM REQUIREMENTS, BE DRAFTED AMENDMENTS TO PART A TO ESKOM]

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
1. AGREEMENT		
Please provide an explanation of circumstances in which the services could be suspended.	Eskom will only agree to suspension on an emergency basis in the event of Supplier having to prevent or mitigate the effects of disabling code, subject to Supplier then escalating to Eskom and agreeing to a timeframe for restoration of services.	
2. DATA RIGHTS AND USE		
2.1. Please confirm that Eskom retains and will remain the Responsible Party and holder of all rights (including any Confidential Information, Personal Information to the extent applicable and other proprietary rights) in respect of all Eskom Data stored, transmitted, processed or generated by Eskom through use of the Services, including all derived data and outputs.	Eskom's Operator Agreement will be applicable and will set forth the permitted purpose which the Supplier is entitled to process Personal Information. In addition, the Supplier shall be required to adhere to paragraph 4 of Part B of this Schedule.	
2.2. Does the Supplier reserve any rights to use Eskom Data for the purposes of operating and improving the services?	Eskom prohibits this.	
2.3. Does the Supplier reserve the right to use Eskom Data for the purposes of advertising?	Eskom prohibits this.	
2.4. Does the Supplier reserve the right to use, or make Eskom Data available as anonymised open data (through standard APIs)?	Eskom prohibits this unless otherwise agreed in writing with Eskom and then under specific	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
	circumstances and separate terms being agreed.	
2.5. Does the Supplier's compliance with copyright laws and other applicable intellectual property rights restrict the type of content Eskom can store with the cloud service?		
2.6. Does Eskom retain all rights in respect of metadata generated by the cloud service system during procedures of upload, management, download, migration or otherwise?		
2.7. Does Eskom have the right to access these metadata during the contractual relationship as well as at the end of the contract period? Please see Section 8.		
3. AVAILABILITY, RETRIEVAL AND USE		
3.1. Are precise indicators provided regarding the availability of the service?	Refer to RFP requirements. See specific service level requirements contained in the RFP.	
3.2. Does the degree of availability of the data meet Eskom business needs as defined?	Supplier is required to warrant this.	
3.3. Does the degree of availability of the data allow Eskom to comply with access to information, data retention, audit and privacy laws?	Eskom reserves the right to audit the Supplier.	
3.4. Does the degree of availability of the data allow Eskom to comply with the right of persons to access their own personal information or authorities to legally access Eskom Data for investigation, audit, control or judicial purposes?	At minimum, the Supplier must allow the access to information in the instance of a Regulatory request.	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
3.5. Procedures for restoring Eskom Data following a service outage must be clearly stated.		
4. DATA STORAGE AND PRESERVATION		
4.1. Data Storage		
4.1.1. Does the Supplier create backups of Eskom's Data?	Refer to RFP requirements. Backup requirements may be defined in the RFP.	
4.1.2. If Eskom organisation manages external records (e.g. customer data), does the Supplier create backups of Eskom customer's data?		
4.1.3. Are there specific service levels around backup?	Refer to RFP requirements.	
4.1.4. Eskom will have audit rights to verify that backups have been done as contracted.	Eskom will have audit rights to verify that backups have been done.	
4.1.5. In the event of accidental data deletion, the Supplier should bear responsibility for data recovery.	No exception or exclusion of liability shall apply.	
4.1.6. How will Eskom's data be stored?	All Eskom Data must be stored in a physically and logically secure environment that protects it from unauthorised access, modification, theft, misuse, and destruction. In addition to the general standards set forth above, Supplier will maintain an adequate level of physical security controls over its facility. Further, Supplier will maintain an adequate level of data security controls.	
4.2. Data Preservation		

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
4.2.1. Are there procedures outlined to indicate that Eskom Data will be managed over time in a manner that preserves their usability, reliability, authenticity and integrity?	Please provide procedures.	
4.2.2. Are there procedures to ensure file integrity during transfer of Eskom Data into and out of the system (e.g. checksums)?	Procedure to be provided.	
4.2.3. Provide an explanation about how the service will evolve over time (i.e. migration and/or emulation activities)?		
4.2.4. Does the system provide access to audit trails concerning activities related to evolution of the service?	Eskom requires a full audit trail and audit rights.	
4.2.5. Will Eskom be notified by the Supplier of changes made to Eskom Data due to evolution of the service?	Eskom requires a pre-agreement for such change and the right to disallow such change.	
4.2.6. Does the Supplier offer any service levels related to data restoration in the event of data loss or corruption?	Eskom requires clearly defined service levels within which the Supplier will restore data (or data backup) in the event of data loss or corruption at its costs.	
4.2.7. Eskom requires notification of impending changes to the system related to evolution of the service that could impact Eskom Data.	A minimum of at least 90 days prior notice.	
5. DATA RETENTION AND DISPOSITION		
5.1. Eskom must be informed about the procedure and conditions for the destruction of Eskom Data.		
5.2. Eskom Data must (and all their copies, including backups) be destroyed in compliance with Eskom Data retention and disposition policies.	Refer to RFP requirements.	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
5.3. Eskom requires the Supplier to immediately and permanently destroy data in a manner that prevents their reconstruction, according to a secure destruction policy ensuring confidentiality of the data until their complete deletion.		
5.4. Is there information available about the nature and content of the associated metadata generated by the cloud service system?	Refer to RFP requirements.	
5.5. Will the Supplier destroy associated metadata upon disposition of Eskom Data?	Refer to RFP requirements.	
5.6. Will the Supplier deliver and/or give access to audit trails of the destruction activity?		
5.7. Will the Supplier supply an attestation, report or statement of deletion (if required by Eskom internal or legal destruction policies)?		
6. SECURITY, CONFIDENTIALITY AND PRIVACY		
6.1. Security		
6.1.1. Does the system prevent unauthorised access, use, alteration or destruction of Eskom Data?	Eskom reserves the right to specify its own requirements.	
6.1.2. Is Eskom Data secure during procedures of transfer into and out of the system?		
6.1.3. Does the system provide and give Eskom access to audit trails, metadata and/or access logs to demonstrate security measures?	Eskom reserves the right to audit the environment.	
6.1.4. Eskom must be notified in the case of a security breach or system malfunction.	This is a strict requirement.	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
6.1.5. Does the Supplier use the services of a Subcontractor?		
6.1.6. Does the Supplier offer information about the identity of the Subcontractor and its tasks?	Supplier to list the Subcontractors and their locations.	
6.1.7. Subcontractors must be held to the same level of legal obligations as the Supplier of the cloud service.	Supplier to warrant and confirm that the Subconsultants agree to the same level of undertaking in providing the cloud services. There should be a back-to-back undertaking to comply with the terms.	
6.1.8. Supplier must provide information regarding past performance with disaster recovery procedures.		
6.1.9. Please specify the location where all systems are located and advice regarding Eskom's access rights to such location and facilities.	Eskom reserves the right to access such facilities and to audit it.	
6.1.10. Supplier to make available all of its data security standards, policies, procedures and protocols for review by Eskom.	Proof of compliance with best security practise such as annual attestation documentation/ security certifications such as ISO 27001/2 or SOC or ISAE reports. Security controls library and other forms of evidence for information security compliance and alignment to best practise. Annual penetration test or red teaming exercises reports and remediations for service providers that are connected to our infrastructure and those that deal with extremely sensitive or special personal information.	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
	Results Static Application Security Test (SAST), Dynamic Application Security Test (DAST) Results Results of DR tests Any other form of further evidence that proves reasonable measures are applied.	
6.1.11. Supplier shall be required to adhere to any other specific data security requirements communicated to Supplier by Eskom alternatively to provide a gap analysis to Eskom where any gaps between Eskom requirements and Supplier policies exist, together with a risk mitigation plan to enable Eskom to manage and/or mitigate such risk.	To address data security issues, Eskom reserves the right to determine: the location of the data centre where the data will be physically stored; who may have access to the data; the operator of the data centre; and the Supplier's security practices.	
6.1.12. Supplier shall be required to strictly adhere to all clauses in the Agreement related to data security and the protection of personal information, and any associated Eskom policy.		
6.1.13. Supplier is required to provide specific details regarding baseline security measures, security incident management, hardware, software, and security policies. These details will be reviewed by Eskom. Supplier's policies should address security risks particular to cloud computing, and services being delivered over the Internet and accessible through a Web browser.	Refer to RFP requirements.	
6.1.14. To the extent that Supplier is unable to distribute copies of its security policies, Eskom requires the right to inspect such policies		

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
on site. Such policy inspection should be done, if the customer information at issue is extremely sensitive or mission critical.		
6.1.15. Supplier to confirm how it will maintain and enforce safety and physical security procedures with respect to its access and maintenance of Eskom's Data.	Supplier will maintain and enforce safety and physical security procedures with respect to its access and maintenance of Eskom Data that are: (1) at least equal to industry standards for such types of locations, (2) in accordance with Eskom security requirements, and (3) which provide reasonably appropriate technical and organisational safeguards against accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access of Eskom Data and all other data and information provided by Eskom and accessible by Supplier under this Agreement.	
6.1.16. Security Audits: During the Term, Eskom or its third-party designee may, but is not obligated to, perform audits of the Supplier or its third-party environment, including unannounced penetration and security tests, as it relates to the receipt, maintenance, use, or retention of Customer Information. Any of Eskom's regulators shall have the same right upon request. Supplier agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable time frames and at no additional cost.		
6.1.17. If a breach of security or confidentiality occurs, Supplier will be required to, in addition to any other remedies, reimburse Eskom for all costs associated with such breach.		

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
6.1.18. Supplier shall further be required to adhere to Eskom's data retention policies, and to make data and information available so as to ensure Eskom does not breach such policy or applicable law.		
6.1.19. Security Controls: System sharing		
6.1.20. Are system resources dedicated to Eskom or shared with other tenants? Provide more detail about the separation of application and database from other tenants.	Eg Database	
6.1.21. What is your standard data sharing interface? E.g., SFTP, HTTPS, etc.		
6.1.22. Do you have both batch (bulk) and real-time (messaging) interfaces?		
6.1.23. How is initial data load handled onboarded onto the service?		
6.1.24. Is Eskom Data shared with third-party or sub-processor? If yes, please provide details of the third party or sub-processor.		
6.2. Confidentiality		
6.2.1. Does the Supplier have a confidentiality policy with regards to its employees, partners, and subcontractors?	Supplier to provide or to confirm.	
6.3. Privacy		
6.3.1. Do the Supplier's terms include privacy, confidentiality, or security policies for sensitive, confidential, personal or other special kinds	Refer to RFP requirements	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
of data? If so, please confirm that these are aligned with Eskom's requirements.		
6.3.2. Is it clearly stated what information (including personal information) is collected about Eskom, why it is collected and how it will be used by the Supplier?		
6.3.3. Does the Supplier share this information with other companies, organisations, or individuals? If so, Eskom's consent must be obtained.		
6.3.4. Supplier to state the legal reasons for which they would share this information with other companies, organisations, or individuals.		
6.3.5. If the Supplier shares this information with their affiliates for processing reasons, is this done in compliance with an existing privacy, confidentiality, or security policy?		
6.3.6. Have there been any reported processing and/or privacy issues or unauthorised access to information and any cyber-attacks in the last two years?		
6.3.7. Describe the proposed flow of privacy related data?	Data flow should include Eskom entity and region (country specific) from which data will be collected. Data flow must also include all intended users and/or recipients of data and the region where data will be stored and used.	
6.4. Accreditation and Auditing		
6.4.1. Is the Supplier accredited with a third-party certification program?		

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
6.4.2. Is the Supplier audited on a systematic, regular and independent basis by a third-party in order to demonstrate compliance with security, confidentiality and privacy policies?		
6.4.3. Is such a certification or audit process documented?	Please describe the scope and frequency of audits. This refers to both SOC 1 Type II and SOC 2 Type II attestation reports.	
6.4.4. Eskom requires access to information such as the certifying or audit body, the expiration date and a copy of the certification.		
7. DATA LOCATION AND CROSS-BORDER DATA FLOWS		
7.1. Data Location		
7.1.1. Please advise where Eskom Data and their copies are located while stored in the cloud service. Supplier to advise the extent to which it intends to use offshore data centres to provide services.	Refer to RFP requirements: If South Africa, then 7.1.3 and 7.1.4 will not apply	
7.1.2. Does Supplier comply with the location requirements that might be imposed on Eskom organisation's data by law, especially by applicable privacy law?		
7.1.3. Does Eskom have the option to specify the location, in which Eskom Data and their copies will be stored?	The preferred Location is South Africa.	
7.1.4. Will Eskom be notified where metadata are stored and whether they are stored in the same location as Eskom Data?		
7.2. Location of Data Centers		
7.2.1. Eskom reserves the right to add a restriction against offshore work and data flow to foreign countries, including imposing a requirement that the data centre (including the hosted software, infrastructure, and data) be located and the Services be performed	Refer to RFP for specific requirements/prohibitions in this regard. Data centres located in foreign countries may:	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
in South Africa, and that no data be made available to those located outside South Africa.	reduce or eliminate Eskom's opportunity to inspect the location to ensure it complies with its information security requirements; or dictate the jurisdiction and law governing the data. For example, personal information located in Europe may be governed by European law, regardless of the contract terms. This is a concern even if the data centre is located in South Africa, but help desk personnel, for example, access the data from a foreign country with limited security and privacy laws.	
7.2.2. Where Eskom does provide permission for the use of offshore storage/processing, Eskom reserves the right to preclude the Supplier from transferring data to certain jurisdictions.		
7.3. Operator of the Data Centre		
7.3.1. Supplier is required to identify the operator of the relevant data centre. If Supplier is not operating the data centre itself (e.g., Supplier is the owner or licensor of the software and will be providing support, but is using a third-party data centre to host the software), then Supplier will be required to: 7.3.1.1. ensure that the third-party host complies with the terms of the agreement (including the data security requirements); 7.3.1.2. accept responsibility for all acts of the third-party host; and 7.3.1.3. be jointly and severally liable with the third-party host for any breach by the third-party host of the agreement.	Eskom reserves the right to object.	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
7.3.2. Eskom reserves the right to enter into separate direct confidentiality and non-disclosure agreements with the third-party host. Supplier will be required to facilitate such requirement at no additional cost to Eskom. Additionally, if Supplier ever desires to change the host, Supplier is required to provide Eskom with notice in advance. Eskom should be given time to conduct due diligence with regard to the security of the proposed host. Eskom reserves the right to reject any proposed host.	Refer to RFP requirements. Third party host only allowed if explicitly stated in the RFP documents.	
7.4. Cross-border Data Flows		
7.4.1. Will Eskom Data be sent out of the borders of the Republic of South Africa?	Refer to RFP requirements: Eskom will not permit any offshoring of data unless as a mere conduit.	
7.4.2. If so, will data be stored offshore, or will data merely be in transit out of country?	Eskom will not permit any offshoring of data unless as a mere conduit.	
7.4.3. Will Eskom be notified if the data location is moved outside Eskom jurisdiction?	Eskom will not permit any offshoring of data unless as a mere conduit.	
7.4.4. Is the issue of Eskom stored data being subject to disclosure orders by national or foreign security authorities addressed?	Eskom will not permit any offshoring of data unless as a mere conduit.	
7.4.5. Does the Supplier clearly state the legal jurisdiction in which the agreement will be enforced and potential disputes will be resolved in the event that data is stored or processed outside of South Africa?	Eskom will not permit any offshoring of data unless as a mere conduit.	
8. END OF SERVICE – CONTRACT TERMINATION		
8.1. In the event that the Supplier terminates the service, Eskom should be provided with sufficient lead time to migrate the service without service interruption.	Refer to RFP requirements.	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
8.2. If the contract is terminated, Eskom Data be transferred to Eskom or to another Supplier of Eskom's choice in a usable and interoperable format.	Eskom requires this at no additional cost.	
8.3. At the end of the contract and after complete acknowledgement of restitution of Eskom Data, will Eskom Data and associated metadata be immediately and permanently destroyed, in a manner that prevents their reconstruction?	Eskom requires the destruction of data in accordance with retention and destruction policies and a declaration signed off by the Supplier it has been executed.	
8.4. Eskom shall be entitled to terminate the service agreement without penalty in the event that the Supplier of the cloud service changes or for any reason at its convenience?	Eskom reserves the right to terminate.	
9. SERVICE OFFERING AND SERVICE AVAILABILITY		
9.1. Name of service being offered?		
9.2. Brief description of service?		
9.3. Is this an on-premises solution, cloud service or hybrid solution. Please describe the solution?		
9.4. What technology languages, platforms, stacks, and components are utilised in the scope of the service? (AWS, MySQL, Ruby on Rails, Go, and/or JavaScript etc?)		
9.5. Please provide details of your standard offering related to service availability.	Refer to RFP for specific requirements.	
9.6. Please advise how soon Eskom will access its data and the Services in the event of downtime which may be caused due to, <i>inter alia</i> :	Even in such instance, Eskom still requires access to its data.	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
9.6.1. a server being down; 9.6.2. data loss or corruption; 9.6.3. the failure of a telecommunications link; 9.6.4. a natural disaster causing damage to Supplier's data centre; or 9.6.5. the Supplier closing its business because of financial difficulties.		
9.7. Please advise what remedies are available to Eskom in the event of downtime.	Refer to RFP requirements.	
10. DISASTER RECOVERY AND BUSINESS CONTINUITY		
10.1. Supplier will be required to include detailed disaster recovery and business continuity plans requiring Supplier to demonstrate and promise that Supplier can continue to make the Services available even in the event of a disaster, power outage or similarly significant event.	Refer to RFP requirements. Do you have a standard RTO (Recovery time Objective) and RPO (Recovery Point Objective) for this service? Please provide detail.	
10.2. Supplier to also advise the degree to which redundancy has been built into Supplier's proposed solution.		
10.3. Supplier shall maintain and implement disaster recovery and avoidance procedures to ensure that the Services are not interrupted during any disaster. Supplier shall provide Customer with a copy of its current disaster recovery plan and all updates thereto during the term. All requirements of this Agreement, including those relating to security, personnel due diligence, and training, shall apply to the Supplier disaster recovery site.		
10.4. Withholding of Services		

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
10.4.1. Supplier will warrant that it will not withhold Services provided hereunder, for any reason, including but not limited to a dispute between the parties arising under this Agreement, except as may be specifically authorised herein.	Supplier is not allowed to withhold Services under any circumstances	Supplier is not allowed to withhold Services under any circumstances.
10.5. Bankruptcy Financial Wherewithal		
10.5.1. Supplier to advise what mechanisms it has in place to enable Eskom access to Services and Eskom Data in the event that Supplier commits an act of insolvency.		
10.5.2. Supplier may be required to deliver periodic reports on its financial condition. This enables Eskom to assess ahead of time whether Supplier is able to continue to provide Services.	Eskom reserves the right to terminate in the event of business rescue or liquidation.	
10.5.3. Quarterly, during the term, Supplier shall provide Customer with all information reasonably requested by Customer, to assess the overall financial strength and viability of Supplier and Supplier's ability to fully perform its obligations under this Agreement. In the event Eskom concludes that Supplier does not have the financial wherewithal to fully perform as required hereunder, Eskom may terminate this Agreement without further obligation or liability by providing written notice to Eskom.		
11. SERVICE LEVELS		
11.1. Eskom requires assurance from the Supplier that Eskom can rely on the Services. Supplier will be required to provide Eskom with (i) detailed service levels and (ii) appropriate remedies if Supplier fails to meet the agreed service levels.	Refer to RFP requirements. Requirements and remedies for service levels and service level breaches.	

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
	Eskom requires at a minimum the following to be addressed: Uptime (see specific Uptime requirements): • Details of planned downtime; • service response time; • simultaneous visitors; • problem response time and resolution time; • data return; and • remedies including service credits.	
12. INSURANCE		
12.1. Supplier is required to effect insurance which includes a cyber liability policy (at Suppliers own cost).	This is in addition to other types of insurance.	
12.2. At a minimum, such cyber insurance policy must cover damages arising from unauthorised access to a computer system, theft or destruction of data, hacker attacks, denial of service attacks, and malicious code. Such policy shall also cover privacy risks like security breaches of personal information, as well as reimbursement for expenses related to the resulting legal and public relations expenses.		
12.3. In addition, Supplier is required to take out insurance which includes:		

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
12.3.1. technology errors and omissions liability insurance; and 12.3.2. a commercial blanket bond, including electronic and computer crime or unauthorised computer access insurance.		
12.4. Such insurance must also cover damages that Eskom or others may suffer as a result of Supplier's professional negligence or intentional acts by others (the Supplier's employees, hackers, etc.).		
12.5. Eskom also requires the Supplier to list Eskom as an additional insured party on its policies; so as to allow Eskom to claim directly from the insurance company.		
13. INDEMNIFICATION AND LIABILITY		
13.1. Supplier must agree to defend, indemnify and hold harmless Eskom and its affiliates and agents from any claim where the Supplier breaches its confidentiality and data security obligations. Any intentional breach, including any cyber breach, should be fully indemnified, protecting the customer from out-of-pocket costs or expenses related to recovery of the data and compliance with any applicable notice provisions, fines and penalties, or other obligations required by data privacy laws.	Eskom requires this from the Supplier and will reserve this right in the agreement.	
13.2. Supplier must agree to defend, indemnify, and hold harmless Eskom, its employees, its affiliates and agents from any claim that the Services infringe the intellectual property rights of any third party.		

QUESTION / STATEMENT	ESKOM MINIMUM REQUIREMENTS, WHERE ADDITIONAL CLARIFICATION BEYOND COLUMN 1 IS REQUIRED	SUPPLIER RESPONSE
14. FINAL RISK ASSESSMENT		
14.1. Supplier will be required to assist Eskom in mitigating any risk in the event that Supplier's offering deviates from Eskom requirements and such shall be at no additional cost to Eskom.	Only applicable in exceptional circumstances approved by Eskom.	
15. SUPPORTING DOCUMENTATION (PLEASE ATTACH THE FOLLOWING DOCUMENTS OR LINKS TO DOCUMENTS, RELATED TO THE CLOUD SERVICES WHERE READILY AND ALREADY AVAILABLE)	YES/NO/N/A	SUPPLIER EXPLANATION
15.1. SOC 1 Type II and SOC 2 Type II are entry criteria and mandatory security requirements for all cloud services that store and process financial, PII and IP information. Bridge letter is required if the attestation report is more than six (6) months.		
15.2. Recent DRP and Backup Restore Plan Test Results		
15.3. Service Architecture/Network Architecture diagram		
15.4. Cloud Service and/or data security policy		
15.5. Security implementation guidelines and secure SDLC standard		
15.6. Please provide details on cloud service consumer (CSC) security responsibilities (T&C's or cloud shared responsibility model documentation)		
16. Data Protection and Access Controls	YES/NO/N/A	SUPPLIER EXPLANATION
16.1. Is data at rest and transit encrypted?		
16.2. Which encryption standards are used?		

16.3. Which groups of staff (individual contractors and full-time employees) have access to Eskom personal and sensitive information?		
16.4. Is MFA required for employees and contractors to log in to production systems employed?		
16.5. Is segregation of duties employed between developers and operation team?		
16.6. Are full-time employees and contractors regularly screened?		
17. Policies and Standards	YES/NO/N/A	SUPPLIER EXPLANATION
17.1. Do you have a dedicated information security team?		
17.2. Do you have a formal Information Security Program in place?		
17.3. Do your information security and privacy policies align with industry standards (ISO-27001/17/18, NIST Cyber Security Framework, ISO-22307, CoBIT, etc.)?		
17.4. How do you test the security of your network? Internal, third parties or both?		
17.5. Please summarise your network vulnerability management processes and procedures?		
17.6. Please summarise your application vulnerability management processes and procedures?		
17.7. How do you regularly evaluate patches and updates for systems used as part of the service?		
17.8. Are patches and application updates tested on development environment prior being deployed to production environment?		

17.9. Do you have operational breach detection system, deception solutions and/or anomaly detection with alerting?		
17.10. Do you have a network packet inspection tool?		
17.11. Is intrusion detection system (IPS) tool deployed?		
18. Reactive Security	YES/NO/N/A	SUPPLIER EXPLANATION
18.1. How do you log and alert on relevant security events? This includes the network and application layer.		
18.2. How will you authenticate Eskom users: If passwords are used, describe password complexity requirements, and how passwords are protected. If SSO is supported, please describe the available options. If different service tiers are available, please describe.		
18.3. Will you support Integration into Eskom existing identity providers (IdP's) Microsoft (MS) on-premises active directory (AD), Entra ID, MS Identity (MDI)? Please provide options and standards used.		
18.4. How will federation be done with existing Eskom identity store?		
18.5. What admin activities will be required by Eskom?		
18.6. What admin activities will be done by the Supplier?		
18.7. What level of tracking and auditing for administrator activities will be available and enabled?		
18.8. How will administrators be managed? Will Eskom do it or the Supplier?		
18.9. Are there role-based user access management capabilities available and enabled?		

18.10. Does your application enable custom granular permissions and roles to be created? Please describe the roles available.		
18.11. Which audit trails and logs are kept for systems and applications with access to Eskom Data?		
18.12. Are audit trails and logs encrypted, securely kept with limited access to administrators?		
18.13. Which encryption standards are used to encrypt backups?		
18.14. Is DDoS protection mechanism employed?		
19. Compliance	YES/NO/N/A	SUPPLIER EXPLANATION
19.1. How do you conduct internal audits (audits lead by your personnel) of the cloud service? What is the frequency?		
19.2. Do you seek a right to use or own Eskom derived information for your own purposes? Please describe the intent and purpose of use		
19.3. How will initial data be loaded. E.g., SAP Export and Import?		
19.4. Are REST APIs used for any integration requirements to other systems? It should be noted that point-to-point integration is not permitted as security, logging and monitoring is not available and enabled.		
19.5. What are your integration platforms you used? E.g., IBM Data Power, SAP CPI/PI/PO, Mulesoft, Oracle Service Bus, Connect Direct, HP Data Protector, IBM Data Power, Oracle Fusion Middleware, SAS Data Integration Studio, MS SQL Server Integration Services etc.		

19.6. Which character sets, languages, text orientations and units of measure do you support?		
19.7. If, for whatever reason, the cloud service should be terminated, how and who will perform data migration back to Eskom, and in what format?		
20. Electronic Discovery (e-Discovery)	YES/NO/N/A	SUPPLIER EXPLANATION
20.1. Do you offer e-Discovery capability?		