	Eskom ITO-Schedule Q	**Document Identifier**	**240-IT002**	**Rev**	**0**
		Effective Date	**30 June 2021**		
		Review Date	**30 June 2025**		

SCHEDULE Q – SUPPLEMENTARY TERMS FOR CLOUD COMPUTING

[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 CLOUD 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 AS LEGALLY BINDING COMMITMENTS]

TABLE OF CONTENTS

Clause number and description	Page

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
1. **AGREEMENT**		
1.1. Please clearly state the envisaged start date of the agreement (i.e. commencement of services and service levels).	Any gap between service implementation and “go-live” must be clearly identified and payment obligations should be adjusted accordingly. (Note: As per your RFP if applicable)	
1.2. 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.	
1.3. Please provide an explanation of circumstances in which the services could be terminated.		

QUESTION / STATEMENT		ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
1.4.	Please provide an explanation of notification, or an option to subscribe to a notification service, in the event of changes made to the terms governing the service.	This only applies to a standard public cloud offering where ESKOM agrees to Supplier's standard terms on an as is basis.	
2.	**DATA OWNERSHIP AND USE**		
2.1.	Please confirm that ESKOM retains ownership of the data that ESKOM stores, transmits, and/or creates with the cloud service.		
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 anonymized open data (through standard APIs)?	ESKOM prohibits this unless otherwise agreed in writing with ESKOM and then under specific 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?		

QUESTION / STATEMENT		ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
2.6.	Do the Supplier's terms apply to metadata?	ESKOM requires no exception for metadata.	
2.7.	Does ESKOM gain ownership of metadata generated by the cloud service system during procedures of upload, management, download, and migration?		
2.8.	Does ESKOM have the right to access these metadata during the contractual relationship? Please see Section 8.		
3.	**AVAILABILITY, RETRIEVAL AND USE**		
3.1.	Are precise indicators provided regarding the availability of the service?	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?		
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?		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
3.5. Does the degree of availability of the data allow ESKOM to comply with the right of authorities to legally access ESKOM data for investigation, audit, control or judicial purposes?		
3.6. Are the procedures, time and cost for restoring ESKOM data following a service outage clearly stated?		
4. **DATA STORAGE AND PRESERVATION**		
4.1. Data Storage		
4.1.1. Does the Supplier create backups of ESKOM's data?		
4.1.2. If ESKOM organization manages external records (e.g. customer data), does the Supplier create backups of ESKOM customer's data?		
4.1.3. Do the Supplier's terms/offering apply to any backup created?		
4.1.4. Are there specific service levels around back up?		
4.1.5. Does ESKOM have audit rights to verify that back-ups have been done as contracted?		

QUESTION / STATEMENT		ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
4.1.6.	In the event of accidental data deletion, does the Supplier bear responsibility for data recovery?	No exception or exclusion of liability shall apply.	
4.2.	Data Preservation		
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?		
4.2.2.	Are there procedures to ensure file integrity during transfer of ESKOM data into and out of the system (e.g. checksums)?		
4.2.3.	Is there an explanation provided 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.	

QUESTION / STATEMENT		ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
4.2.5.	Will ESKOM be notified by the Supplier of changes made to ESKOM data due to evolution of the service?	ESKOM requires both 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 back-up) in the event of data loss or corruption.	
4.2.7.	Can ESKOM request notification of impending changes to the system related to evolution of the service that could impact ESKOM data?		
5.	**DATA RETENTION AND DISPOSITION**		
5.1.	Is ESKOM clearly informed about the procedure and conditions for the destruction of ESKOM data?		
5.2.	Will ESKOM data (and all their copies, including backups) be destroyed in compliance with ESKOM data retention and disposition polices?		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
5.3. If so, will they be immediately and permanently destroyed 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?		
5.5. Will the Supplier destroy associated metadata upon disposition of ESKOM data?		
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)?		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
6. **SECURITY, CONFIDENTIALITY AND PRIVACY**		
6.1. Security		
6.1.1. Does the system prevent unauthorized 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?		
6.1.4. Will ESKOM be notified in the case of a security breach or system malfunction?	This is a strict requirement.	
6.1.5. Does the Supplier use the services of a sub-contractor?		
6.1.6. Does the Supplier offer information about the identity of the sub-contractor and its tasks?		
6.1.7. Are subcontractors held to the same level of legal obligations as the Supplier of the cloud service?	.	

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
6.1.8. Is a disaster recovery plan available or does the contract consider what happens in the event of a disaster?		
6.1.9. Does the Supplier offer any information regarding past performance with disaster recovery procedures?		
6.1.10. Please specify the location where all systems are located and advise re ESKOM's access rights to such location and facilities.		
6.2. Confidentiality		
6.2.1. Does the Supplier have a confidentiality policy with regards to its employees, partners and subcontractors?	.	

QUESTION / STATEMENT		ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
6.3.	Privacy		
6.3.1.	Does the Supplier's terms include privacy, confidentiality, or security policies for sensitive, confidential, personal or other special kinds 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, organizations, or individuals without ESKOM's consent?		
6.3.4.	Does the Supplier state the legal reasons for which they would share this information with other companies, organizations, or individuals?		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
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?		
6.4. Accreditation and Auditing		
6.4.1. Is the Supplier accredited with a third-party certification program?		
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?		
6.4.4. Does ESKOM have access to information such as the certifying or audit body and the expiration date of the certification?		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
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?		
7.1.2. Does Supplier comply with the location requirements that might be imposed on ESKOM organization'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?	Yes Local	
7.1.4. Will ESKOM be notified where metadata are stored and whether they are stored in the same location as ESKOM data?		

QUESTION / STATEMENT		ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
7.2.	Cross-border Data Flows		
7.2.1.	Will ESKOM data be sent out of the borders of the Republic of South Africa?	ESKOM will not permit any offshoring of data unless as a mere conduit.	
7.2.2.	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.	
7.2.3.	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.	
7.2.4.	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.	
7.2.5.	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.	

QUESTION / STATEMENT		ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
8.	**END OF SERVICE – CONTRACT TERMINATION**		
8.1.	In the event that the Supplier terminates the service, will ESKOM be provided with sufficient lead time to migrate the service without service interruption?		
8.2.	Is there an established procedure for contacting the Supplier if ESKOM wishes to terminate the contract?		
8.3.	If the contract is terminated, will 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.	
8.4.	Supplier must stipulate the procedure, cost (or cost estimate or costing basis), and time period for returning/transferring ESKOM data at the end of the contract.		
8.5.	At the end of the contract, do ESKOM have the right to access the metadata generated by the cloud service system?		
8.6.	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?		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
8.7. Is there an option for confirmation of deletion of records and metadata by the organization prior to termination of services with the Supplier?		
8.8. Is there an option for ESKOM to terminate the service agreement without penalty in the event that the Supplier of the cloud service changes?	ESKOM reserves the right to request this.	
9. **SERVICE AVAILABILITY**		
9.1. Please provide details of your standard offering related to service availability.		
9.2. Please advise how soon ESKOM will access its data and the services in the event of downtime which may be caused due to, *inter alia*: 9.2.1. a server being down; 9.2.2. data loss or corruption; 9.2.3. the failure of a telecommunications link; 9.2.4. a natural disaster causing damage to Supplier's data centre; or	Even in such instance, ESKOM still requires access to its data.	

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
9.2.5. the provider closing its business because of financial difficulties.		
9.3. Please advise what remedies are available to ESKOM in the event of downtime.		
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.		
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		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
diligence, and training, shall apply to the Provider disaster recovery site.		
10.4. Withholding of services		
10.4.1. Under Supplier's standard offering, to what extent would Supplier withhold services?	Supplier is not allowed to withhold services under any circumstances.	
10.4.2. Suppler 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 authorized herein.		
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.		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
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.		
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.		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
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.	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.	

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
12. **DATA SECURITY**		
12.1. Supplier to make available all of its data security policies, procedures and protocols for review by ESKOM	• **Proof for compliance to security best 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**	

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
	with very sensitive or special personal information. • **Results of DR tests** • **Any other form of further evidence that proves reasonable measures are applied.**	
12.2. 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 provider’s security practices.	
12.3. Supplier shall be required to make available its data protection controls in place, for review and consideration by ESKOM.		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
12.4. 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.		
12.5. Location of Data Centre		
12.5.1. Supplier to advise the extent to which it intends to use offshore data centres to provide services.		
12.5.2. 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 in South Africa, and that no data be made available to those located outside South Africa.	Data centres located in foreign countries may: • 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	

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
	from a foreign country with limited security and privacy laws. Please check the RFP for specific requirements/prohibitions in this regard.	
12.5.3. Where ESKOM does provide permission for use of offshore documents, ESKOM reserves the right to preclude the Supplier from transferring data to certain jurisdictions.		
12.6. Operator of the Data Centre		
12.6.1. 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: 12.6.1.1. ensure that the third-party host complies with the terms of the	ESKOM reserves the right to object,	

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
agreement (including the data security requirements); 12.6.1.2. accept responsibility for all acts of the third party host; and 12.6.1.3. be jointly and severally liable with the third party host for any breach by the third party host of the agreement.		
12.6.1.4. ESKOM reserves the right to enter into separate direct agreements including 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		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
host. ESKOM reserves the right to reject any proposed host.		
12.7. Provider's Security Practices		
12.7.1. 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.		
12.7.2. To the extent that Supplier is unable to distribute copies of its security policies, ESKOM requires the right to inspect such policies on site. Such policy inspection should be done, if the customer information at issue is very sensitive or mission-critical.		
12.7.3. Supplier will maintain and enforce safety and physical security procedures with respect to its access and maintenance of ESKOM Data that are:		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
(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 organizational safeguards against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access of ESKOM data and all other data and information provided by ESKOM and accessible by Supplier under this Agreement. 12.7.4. Storage of Customer Information. All ESKOM Data must be stored in a physically and logically secure environment that protects it from unauthorized 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. 12.7.5. 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		

QUESTION / STATEMENT		ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
	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.		
12.7.6.	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.		
12.7.7.	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.		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
13. **INSURANCE**		
13.1. 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.	
13.2. At a minimum, such cyber insurance policy must cover damages arising from unauthorized 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.		
13.3. In addition, Supplier is required to take out insurance which includes: 13.3.1. technology errors and omissions liability insurance; and 13.3.2. a commercial blanket bond, including electronic and computer crime or unauthorized computer access insurance.		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
13.4. 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 provider's employees, hackers, etc.).		
13.5. ESKOM also requires the provider to list ESKOM as an additional insured party on its policies; so as to allow ESKOM to claim directly from the insurance company.		
14. **INDEMNIFICATION AND LIABILITY**		
14.1. 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 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 or other obligations required by data privacy laws.	Eskom requires this from the Supplier.	
14.2. Supplier must agree to defend, indemnify, and hold harmless ESKOM and its affiliates and agents from any claim that the services infringe the intellectual property rights of any third party.		

QUESTION / STATEMENT	ESKOM MINIMUM CRITERIA (TO THE EXTENT THAT THIS IS NOT CLEAR FROM COLUMN 1)	SUPPLIER RESPONSE
14.3. Under no circumstances will Supplier include any exclusion of liability clauses under the Agreement.	This is critical and any such exclusions may disqualify Supplier.	
15. **FINAL RISK ASSESSMENT**		
15.1. 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.		