Modified Annexures w.r.t Corrigendum to RFP -3

Request for Proposal for Implementation & Maintenance of Enterprise Mail Messaging Solution Ref: LIC/CO/IT-BPR/EMS/RFP/2017-18 Dated: 14/03/2018

Annexure XI - Functional Requirements

Bidder has to conform to all Mandatory points and provide satisfactory responses to all questions

Feature	Requirement	Bidder's Response		
	1.Primary Objectives of the Mailing Solution		Whether Complies (Yes/No)	Details /page no.
1.1	Whether Architecture Proposed is Centralized and the delivery method –whether On-premises or Cloud Computing on public Cloud or Hybrid ?	Mandatory		
1.2	If the Delivery method is Public Cloud Computing based , the location of hardware, software ,data at rest ,all data centres including DR sites should be within India. Whether Complies?	Mandatory and give locations of Data Centres		
1.2	Whether the solution proposed is "high performing?"	Justify		
1.3	Whether the solution proposed is "highly available?"	Justify		
1.4	Whether the solution proposed is "Scalable" (upto **157500** users) Mail DB size of 65 TB in first year to 75 TB in sixth year	Mandatory		
1.5	Whether the solution proposed is having redundancies	Mandatory		
1.6	Whether the solution proposed has "no single point of failure?"	Mandatory		
1.7	Comment on the Bandwidth utilization by the proposed solution per user as well as aggregate of all users at central point for on-premises as well as for Public cloud	Indicate the bandwidth required		
1.8	Whether easier back up and retrieval mechanisms are built in to the solution proposed?	Describe		
1.9	BCP Features	Describe		
1.10	Whether the proposed solution is all set for DR Replication	Mandatory		
1.11	Whether the bidder is willing to provide Annual Maintenance Contract after the expiry of Warranty	Mandatory		

1.12	Whether the bidder will follow Information Security Best Practices as given in point	Mandatory		
1.13	Whether The Bidder would be able to meet all statutory or regulatory requirements as mandated by authorities from time to time like IRDAI Cyber security guidelines	Mandatory		
1.14	Whether Unpriced Bill of Materials for Hardware and Software enclosed	Mandatory		
1.15	Whether Directory services of the mail messaging solution or additional Directory services proposed is able to deploy policies and configurations on Windows desktops and join them to the domain	Mandatory		
1.16	If Additional Directory services proposed for deployment of policies and domain join on Windows desktops ,whether bridging Software also proposed	Mandatory		
2.Components of the mailing solution required				
2.1	Mail Transfer Agent	Mandatory		
2.2	Secured webmail service	Mandatory		
2.3	Mail DB	Mandatory		
2.4	Integration with LIC existing Anti-Relay, Anti-SPAM Global filtering and content scanning & Anti-Virus Service for on-premises solution	Mandatory		
2.5	Mobile access and synchronization with mailbox	Mandatory		
2.6	Backup solution	Mandatory		
2.7	Support for Indian Languages	Desired		
2.8	Authentication/Encryption Enabled	Mandatory		
2.9	Support for use of Digital Certification	Mandatory		
2.10	Support for Multiple Domains	Mandatory		
2.11	Support for SMTP relay services to Email Gateway Security and Automated Transactional Bulk Mails relayed from Application SMTP servers to within and without domain users	Mandatory		
2.12	Support for Public/Private Folders, Personal/Global Address Books	Mandatory		
2.13	Querying and Report Mechanism	Mandatory		
2.14	Inactive Time Out	Mandatory		
2.15	Whether Facility Management and Onsite resources offered?	Mandatory		
2.16	Support Desktop Client having POP3,MAPI over http/s, any third party client versions used in LIC, OWA ,Windows Mail, etc.	Mandatory		
3.Protocols Supported				
Feature	Requirement	Bidders Response		
3.1	Specify the standards/ protocols supported/used between different components/modules in the total solution. The Solution should support IMAP,	Mandatory		

	POP3,SMTP and ESMTP ,MAPI over http/s			
4.Interoperability				
4.1	Support for different clients across LIC like MS outlook ,Thunderbird , Wndows Mail ,OWA on browsers like IE,Chrome ,Mozilla etc. Comment on the interoperability of the solution proposed across Applications/platforms	Mandatory		
4.2	Whether the bidder will implement Configuration required to connect to Cloud Computing based solution for above given clients ? Provide Details.	Mandatory		
5.Bandwidth and Other Details				
5.1	The bidder should indicate the type/bandwidth for each type of connectivity in the present network architecture at each level. (In general, light users work from branch Offices, and medium users work at Divisional Offices ,Heavy users at Zonal Offices and Central office	Indicate		
5.2	Is a detailed architecture diagram attached?	Mandatory		
5.3	Is a detailed mail flow diagram for the proposed messaging solution attached	Mandatory		
5.4	Infrastructure Design Documents to be submitted: for Mail Messaging Solution a.Architecture: i) Physical design ii) Logical design Including Layers implementation as per OEM's implementation recommendation. b. SMTP Relay methodology c. Servers & their roles as per OEMs recommendation e. High Availability, Redundancy, Expandability f. D R Implementation Strategy g. Storage organization and utilization as per OEMs recommendations h. Antivirus, Antispam & security implementation methodology i. Backup , Recovery, j. Implementation and project plan up to the stage of Go-Live k. Data/ mail boxes migration strategy from existing Mail Solution l. Any other as per the design suggested.	Mandatory		

6. List of Hardware Proposed: (Mandatory)(only for on –premises)

for 150500 email accounts and the proposed H/W should scalable to 157500 email accounts Growth and for Growth of 4 cr mails per year reaching 40.66 crore total number of mail processed by sixth year by Solution. Mail DB size 65 TB in first year to 75 TB in sixth year

S.No	Hardware Details	Qty	Use
1			

2				
3				
5				
6				
7				
8				
List of Software Proposed by the Bidder : (Mandatory))(only for on –premises)				
S.No	Software Details	Qty	Version & No. of Licenses	
1				
2				
8.Sizing Details				
Feature	**Requirement**	**Bidders Response**		
8.1	Number of Users Supported by the solution given by the Bidder	Minimum is as given in Bid. **(Work Sheet on sizing Hardware for each of the service shall be enclosed).**		
8.2	Scalability	Indicate the details of scalability supported by your design		
8.3	Upgradability	Indicate the details of upgradability supported by your design		
9.Performance				
9.1	Does the Bidder recommend a separate Load Balancer (if a native solution is not available)? If yes, cost of load balancer to be included in Commercial Bid Form	Indicate whether a separate load balancer is proposed. The software /hardware for load balancer proposed should be mentioned in the relevant table along with the details of configuration, software and no of licenses required.		
9.2	Mention the components of messaging solution, which can be available through high availability mode.	Mention		
9.3	All the messaging services in the total mail Messaging solution should have a single source of authentication and authorization.	Mandatory		
9.4	Clustering of Servers	Mandatory		
9.5	The Servers proposed have to provide for (a) clustering in Active- Active or Active-Passive mode (b) Fail Over (c) High	Mandatory		

	Availability (d) Expandability of CPU/RAM/ HDD (e) Implementation of DR			
9.6	Shall Support for application level automatic fail-over for high availability. In case of failover of services, the performance and functionality of Messaging solution should remain same as of previous state and transparent to the end user.	Mandatory		
9.7	The proposed Operating System shall support for 32 and 64bit applications and architecture for client side and 64bit applications and architecture for server side.	Mandatory		
9.8	The proposed Operating System has to support both hardware and software level clustering and clustered file system.	Mandatory		
9.9	The Operating system has to provide/ support implement Multi level security features.	Specify		
9.10	Performance parameters : Hardware & Software should support for a Minimum Requirement of Mail Messaging System per mail box: Received: 50 Sent: 50	Mandatory		
9.11	Response Time: Maximum mail delivery time within domain should be 2 minutes	Mandatory		
10.Proposed Servers, Storage & their configuration (Provide information in separate tables for each type of server proposed) for on -premise				
Features	**Requirement**	**Bidders Response**		
10.1	Server Details : Whether Servers are present in the leaders or challengers quadrant of Gartner's Magic quadrant for Modular Servers in the year 2016 and 2017	Mandatory and specify details		
10.2	Server Details: Whether servers comply with specifications given in 5.3.2 Supply and Installation of Hardware required – Pt 18 –Server specifications	Mandatory and specify details		
10.3	Volume of Mail Traffic that can be handled per day/ month	Specify		
10.4	Thick/Desktop mail client Concurrent connections supported	Specify		
10.5	Software Requirements	Specify		
10.6	Backup Devices	Specify		
10.7	Storage Details – Whether the Storage is present in the leaders or challengers quadrant of Gartner's Magic Quadrant for General Purpose Disk Arrays in the	Mandatory and Specify		

	year 2016 and latest year			
10.7	Whether Hardware provides for Expandability of disk space, Clustering, High Availability and support Hot Re-placement Feature	Specify		
10.8	Whether OEM has certified Design, Hardware and Software of Mail Messaging Solution and OEM Certification Of Design, Hardware and Software of Mail Messaging Solution is submitted	Mandatory		
11.External Backup Software Solution (for on-premise solution)				
Features	**Requirement**	**Bidders Response**		
11.1	Backup Solution : Backup Solution should be present in the leaders or challengers quadrant of Gartner's Magic Quadrant for Data Center backup and Recovery solutions	Mandatory		
11.2	External Backup system proposed shall provide for speed backup.	Give specifications of all the components of external backup system proposed (make, model, configuration, backup speed, bench mark details with the proposed server/ storage, if any,		
12. Any Other Equipment Proposed by the Bidder and not Covered Above (to make the solution fully functional as per the architecture proposed by the bidder):				
Features	**Requirement**	**Bidders Response**		
12.1				
12.2				
12.3				
12.4				
12.5				
13.Security Features				
Features	**Requirement**	**Bidders Response**		
13.1	The proposed solution shall provide a secure means of accessing the mails from LAN/ WAN/ as well as the Mobile/ Internet with respect to the security standards.	Specify		

13.2	The proposed solution shall integrate with LIC existing Trend Micro Anti-Spam, anti-phishing Email Gateway Security ,Anti-Virus solution for server and mails	Mandatory		
13.3	The Messaging Solution should use multiple layers of defenses against intruders, unauthenticated users against being an Open Relay , and Denial of Service attacks (DoS). It should prevent any unauthorized usage and should facilitate features included, but not limited to authentication before relaying, TLS/SSL, and HTTPS.	Mandatory;		
14. Other Features (Please List Out)				
1				
2				
3				
15.End-to-End Facility Management and AMC for hardware and Software				
15.1	Onsite and remote support for Management and Maintenance of all Software components (software of mail servers, security devices, storage devices, backup devices etc) whether supplied by the bidder or LIC for the purpose of end-to-end Mail Messaging Solution including Patch management, Updates ,Service packs ,Rollups and applications, OS Hardening etc	Mandatory		
15.2	No of dedicated Resource Persons Proposed.	Indicate (4 in number Mandatory)		
15.3	Certification and experience proposed of Resource Persons.			
15.4	Contract Period	Minimum 6 Years and further extension		
15.6	Whether bidder has back to back support or ATS with all OEM .Whether certificate attached regarding this	Mandatory		
15.5	Whether bidder agrees to perform AMC during warranty and 1 years after warranty and further extension period as per Terms and conditions specified in Annexure XII and has submitted undertaking as given in Annexure xiv	Mandatory		
16.Training				
16.1	Training Schedule	Mandatory :Indicate no of days and total number of hours		
16.2	No of persons to be trained	Mandatory :Minimum of 10 persons		
16.3	Content (Minimum as given in cl 5.5.2-Training)	Mandatory: Indicate broad areas of proposed		

		training		
16.4	Whether training will be provided at Mumbai	Mandatory :		
16.5	Training material	Mandatory : To be prepared and given by the bidder – Indicate willingness		
16.6	Equipment required for training	Mandatory : To be brought in by the bidder		
17.Delivery Schedule				
Sr. No.	Activity-Delivery schedule			
17.1	Whether Delivery of software , hardware etc.would be done within 6 weeks from the date of Purchase Order or Contract	Mandatory :Delivery Schedule proposed		
17.2	Whether Implementation, Migration , Project completion period would be 30 weeks from the date of Purchase Order or Contract	Mandatory: Project completion period proposed		
17.3	Whether Deployment of On-site Engineer in Mumbai after receipt of the purchase order would be beginning at Go-live	Mandatory		
17.4	Training - Immediately on Go - Live	Mandatory		
17.5	Commencement of Facility Management at Go-Live	Mandatory		
18	**Cloud Computing delivery method requirements**			
18	**Compliance with Information Security Policy for Public Cloud Computing delivery Method**			
18.1	The bidder /cloud service provider/OEM shall have to comply with LIC's IT & IS Security policy in key concern areas relevant to the RFP, details of which will be shared with the finally selected Bidder. Some of the key areas are as under: Cloud Computing Policy Data Life Cycle Protection Policy Access Management Policy User Life Cycle Management Policy Cryptographic Control Policy Third Party Risk Management	Mandatory		

	Policy Data Life Cycle Protection Procedure Access Management Procedure User Life Cycle Management Procedure Cryptographic Control Procedure Incident Management procedure			
18.2	A pre-selection risk assessment & technical assessment shall be carried out for cloud infrastructure and cloud service provider/OEM providing cloud computing services to LIC and its users. Whether bidder/cloud service provider is agreeable to this	Mandatory		
18.3	Systems or applications shall be assessed from compatibility, performance and security requirements before hosting on cloud infrastructure. Whether bidder/cloud service provider is agreeable to this	Mandatory		
18.4	Service level agreements shall be signed with the bidder/cloud service provider/OEM detailing the responsibilities of the bidder/cloud service provider/OEM and LIC.	Mandatory and provide a list of the agreements and attach draft copies of all agreements ,if required to be agreed to by LIC		
18.5	Non-disclosure agreement shall be signed between the bidder/cloud service provider/OEM and LIC. Whether bidder/cloud service provider /OEM is agreeable to this	Mandatory		
18.6	LIC shall Conduct periodic risk Assessment & technical assessment and audit of cloud infrastructure.This includes audit for IRDAI/Law enforcement agencies/CERT-In to access information/log. Whether bidder/cloud service provider/OEM is agreeable to this	Mandatory		

18.7	Bidder shall Establish a dedicated encrypted data link between LIC and cloud service provider network.	Mandatory		
18.8	Bidder/Cloud service Provider/OEM to Implement adequate data retention controls for cloud computing services. Whether complies	Mandatory and specify details		
18.9	Bidder/Cloud service Provide/OEM r to Ensure adequate data encryption solutions are implemented on the data at rest ,data in transit and data in use stored in the cloud infrastructure.	Mandatory and specify details		
18.10	Bidder/Cloud service Provider/OEM Ensure that the authentication mechanism for the cloud infrastructure shall be in line with the User Life cycle and Access Management policy of LIC	Mandatory and specify details		
18.11	Bidder/Cloud service Provider/OEM to ensure to Restrict access to cloud infrastructure to authorized users only.	Mandatory and specify details		
18.12	Bidder/Cloud service Provider/OEM to Ensure that remote access to the console to cloud computing infrastructure is restricted to authorized users only and be configured on a separate network segment.	Mandatory and specify details		
18.13	Bidder/Cloud service Provider/OEM to Ensure that the bidder/cloud computing service provider does not have access to stored data /mail boxes , and its access is limited to server/host administration activities	Mandatory and specify details		
18.14	Bidder/Cloud service Provider/OEM to Ensure that the cloud infrastructure shall be treated identical to the physical hardware which shall be configured per the Secure Configuration Document maintained by LIC.	Mandatory and specify details		
18.15	Bidder/Cloud service Provider/OEM to Ensure that the unauthorized file sharing, clipboard sharing and network shared storage between LIC and cloud	Mandatory and specify details		

	infrastructure shall be disabled.			
18.16	Bidder/Cloud service Provider/OEM to Ensure that the unused physical hardware from the host system is disabled.	Mandatory and specify details		
18.17	Bidder/Cloud service Provider/OEM to Ensure that unwanted services in cloud servers such as file sharing between the guest and host operating systems shall be disabled	Mandatory and specify details		
18.18	Bidder/Cloud service Provider/OEM to Ensure that auditing and logging feature on cloud infrastructure is enabled and the logs are accessible to LIC to be reviewed periodically or provide log review report to LIC	Mandatory and specify details		
18.19	Bidder/Cloud service Provider/OEM to Ensure that cloud infrastructure is updated with latest patches and anti-virus signatures periodically.	Mandatory and specify details		
18.20	Bidder/Cloud service Provider/OEM to Ensure that the cloud infrastructure is synchronized with LIC's time server or International time server	Mandatory and specify details		
18.21	Bidder/Cloud service Provider/OEM to Ensure that adequate storage space is maintained in the cloud infrastructure	Mandatory and specify details		
18.22	Bidder/Cloud service Provider/OEM to Ensure that the virtual systems are regularly backed-up for error recovery. The data stream of a backup / or any other data transfer activity shall be encrypted to prevent the "theft" of a server image /data by capturing the packets in the backup /data transfer .	Mandatory and specify details		
18.23	Bidder/Cloud service Provider/OEM to Ensure that the DR Plan strategies address the availability of cloud computing services in case of disaster.	Mandatory and specify details		

18.24	Bidder/Cloud service Provider/OEM to Ensure all the incidents occurring at cloud computing services provider premises, which directly or indirectly impacts LIC's services are reported immediately to LIC by the bidder.	Mandatory and specify details		
18.25	Bidder/Cloud service Provider//OEM to Ensure service provider implements DDOS prevention techniques and to ensure the data being not accessed by attackers.	Mandatory and specify details		
18.26	Bidder/Cloud service provider//OEM must comply with Information Technology Act, 2000 and Rules made there under , and the later amended Information Technology (Amendment) Act 2008 , and Data Protection Laws to be enacted in India in future with respect to all LIC data hosted on the cloud and to LIC data which falls under category of health information and personally identifiable information(PII) or sensitive personal data hosted on the cloud and to Cloud service provided to LIC	Mandatory and specify details		
18.27	**LIC data** : Bidder/cloud service provider/OEM will not use LIC Data or derive information from it for any advertising or similar commercial purposes and will use it only for providing services covered in the RFP. LIC retains all right, title and interest in and to LIC Data.	Mandatory and specify details		
18.28	**Disclosure of LIC Data:** Bidder/Cloud service provider**/OEM** will not disclose LIC Data outside of Cloud Service provider except (1) as LIC directs or (2) as required by law. Bidder/Cloud service will not disclose LIC Data or encryption keys used to secure the data or give access to LIC data to law enforcement unless required by law or to any third party . If law enforcement or any other third party contacts Bidder/Cloud Service Provider with a demand for LIC Data, Bidder/Cloud Service Provider /OEM	Mandatory and specify details		

	will redirect the law enforcement agency or the third party to request that data directly from LIC			
18.29	**Security** :Bidder/Cloud Service provider**/OEM** must ensure implementation , maintenance and following of appropriate technical and organizational measures that are intended to protect LIC Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.	Mandatory and specify details		
18.30	**Security Incident Notification** :On becoming aware of any unlawful access to any LIC Data stored on bidder/cloud service provider's**/OEM** equipment or in bidder/cloud service providers facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of LIC Data (each a "Security Incident"), the bidder/cloud service provider **/OEM** will promptly (1) notify LIC of the Security Incident; (2) investigate the Security Incident and provide LIC with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.	Mandatory and specify details		
18.31	The location of the physical servers and LIC data at rest should be in India to ensure conformance with specific regional privacy and security regulations of IRDAI	Mandatory and specify details		
18.32	**Bidder/Cloud service provider Personnel. 1.**Bidder/Cloud service provider/OEM personnel will not process LIC Data without authorization from LIC . **2.**Bidder/Cloud Service provider/OEM personnel are obligated to maintain the security and secrecy of any LIC Data and this obligation continues even after their engagements end.	Mandatory and specify details		

18.33	Bidder /Cloud Service provider**/OEM** will maintain the following security practices with ref to LIC data **Organization of Information Security-** **1**.**Security Ownership**. Specific personnel are required to be posted who are responsible for coordinating and monitoring the security rules and procedures. **2.Security Roles and Responsibilities**. Bidder /Cloud service provider/OEM personnel with access to LIC Data should be subject to confidentiality obligations. **3.Risk Management Program**: Bidder/Cloud Service provider /OEM should have a risk assessment program for the services	Mandatory and specify details		
18.34	**Asset Management-** **1. Asset Inventory-** Bidder/Cloud service provider/OEM should maintain an inventory of all media on which LIC Data is stored. Access to the inventories of such media is restricted to authorized Bidder/Cloud service provider/OEM in writing to have such access. **2.Asset Handling** - Bidder /Cloud service provider/OEM should classify LIC Data to help identify it and to allow for access to it to be appropriately restricted. - Bidder /Cloud service provider /OEM should impose restrictions on printing LIC Data and has procedures for disposing of printed materials that contain LIC Data. -Bidder/Cloud Service provider /OEM personnel must obtain Bidder/Cloud Service provider/OEM authorization prior to storing LIC Data on portable devices, remotely accessing LIC Data, or processing LIC Data outside Bidder/Cloud service provider 's facilities.	Mandatory and specify details		

18.35	**Human Resources Security- 1.Security Training-** Bidder/Cloud service Provider/OEM is required to inform its personnel about relevant security procedures and their respective roles. **2.**Bidder/Cloud service Provider/OEM should also inform its personnel of possible consequences of breaching the security rules and procedures **3.Bidder/Cloud service Provider** /OEM will only use anonymous data in training.	Mandatory and specify details		
18.36	**Physical and Environmental Security**- **1.Physical Access to Facilities.** Bidder/Cloud service provider /OEM should limit access to facilities where information systems that process LIC Data are located to identified authorized individuals. **2.Physical Access to Components**. Bidder/Cloud service provider /OEM maintains records of the incoming and outgoing media containing LIC Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of LIC Data they contain. **3.Protection from Disruptions**. Bidder/Cloud Service provider /OEM should use a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **4.Component Disposal**. Bidder /Cloud Service provider/OEM should use industry standard processes to delete LIC Data when it is no longer needed.	Mandatory and specify details		
18.37	**Operations Management –** **1.Operational Policy.** Bidder/Cloud Service Provider /OEM should maintain security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to LIC Data. **2.Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no LIC Data has been	Mandatory and specify details		

	updated during that period), Bidder/Cloud Service Provider/OEM should maintain multiple copies of LIC Data from which LIC Data can be recovered. - Bidder/Cloud Service Provider /OEM should store copies of LIC Data and data recovery procedures in a different place from where the primary computer equipment processing the LIC Data is located. - Bidder/Cloud Service Provider /OEM should have specific procedures in place governing access to copies of LIC Data. - Bidder/Cloud Service Provider/OEM should review data recovery procedures at least every six months - Bidder/Cloud Service Provider /OEM should log data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **3.Malicious Software.** Bidder/Cloud service provider should have anti-malware controls to help avoid malicious software gaining unauthorized access to LIC Data, including malicious software originating from public networks. **4.Data Beyond Boundaries** - Bidder/Cloud Service Provider /OEM should encrypt, or enable LIC to encrypt, LIC Data that is transmitted over public networks. - Bidder/Cloud Service Provider /OEM should restrict access to LIC Data in media leaving its facilities. **5.Event Logging.** Bidder/Cloud Service Provider /OEM should log, or enables LIC to log, access and use of information systems containing LIC Data, registering the access ID, time, authorization granted or denied, and relevant activity.			

18.38	**Access Control**- **1. Access Policy**. Bidder/Cloud Service Provider /OEM should maintain a record of security privileges of individuals having access to LIC Data. **2.Access Authorization** - Bidder/Cloud Service Provider/OEM should maintain and update a record of personnel authorized to access its systems that contain LIC Data. - Bidder/Cloud Service Provider/OEM should deactivate authentication credentials that have not been used for a period of time not to exceed six months. - Bidder/Cloud Service Provider/OEM should identify those personnel who may grant, alter or cancel authorized access to data and resources. - Bidder/Cloud Service Provider/OEM should ensure that where more than one individual has access to systems containing LIC Data, the individuals have separate identifiers/log-ins. **3.Least Privilege** - Technical support personnel should only be permitted to have access to LIC Data when needed. - Bidder/Cloud Service Provider/OEM should restrict access to LIC Data to only those individuals who require such access to perform their job function. **4.Integrity and Confidentiality** - Bidder/Cloud Service Provider/OEM should instruct its personnel to disable administrative sessions when leaving premises it controls or when computers are otherwise left unattended. - Bidder/Cloud Service Provider/OEM stores passwords in a way that makes them unintelligible while they are in force. **5.Authentication** - Bidder/Cloud Service Provider/OEM should use industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms	Mandatory and specify details 1 2 3 4 5 6		

	are based on passwords Bidder/Cloud Service Provider/OEM requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Bidder/Cloud Service Provider/OEM requires the password to be at least eight characters long. - Bidder/Cloud Service Provider/OEM should ensure that de-activated or expired identifiers are not granted to other individuals. - Bidder/Cloud Service Provider/OEM should monitor, or enable LIC to monitor, repeated attempts to gain access to the information system using an invalid password. - Bidder/Cloud Service Provider/OEM should maintain industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Bidder/Cloud Service Provider/OEM should use industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **6.Network Design.** Bidder/Cloud service provider /OEM should have controls to avoid individuals assuming access rights they have not been assigned to gain access to LIC Data they are not authorized to access.			
18.39	**Information Security Incident Management** **1.Incident Response Process** - Bidder/Cloud service provider /OEM should maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a	Mandatory and specify details 1 2		

	Security Incident, notification by Bidder/Cloud service provider /OEM will have to be made without unreasonable delay and, in any event, within 30 calendar days. - Bidder/Cloud service provider /OEM should track, or enable LIC to track, disclosures of LIC Data, including what data has been disclosed, to whom, and at what time. **2.Service Monitoring.** Bidder/Cloud service provider /OEM security personnel should verify logs at least every six months to propose remediation efforts if necessary.			
18.40	**Business Continuity Management—** **1.**Bidder/Cloud service provider /OEM should maintain emergency and contingency plans for the facilities in which Bidder/Cloud service provider /OEM information systems that process LIC Data are located. **2**.Bidder/Cloud service provider /OEM redundant storage and its procedures for recovering data should be designed to attempt to reconstruct LIC Data in its original or last-replicated state from before the time it was lost or destroyed	Mandatory and specify details 1 2		
19	**Data Control requirements for Cloud Architecture**			
19.1	The following details are required to be provided by the bidder/Cloud Service Provider/OEM **a**.Data Retrieval Period (length of time in which the customer can retrieve a copy of their cloud service customer data from the cloud service): **90 days**	Mandatory and specify details		
	b.Data retention period (length of time which the cloud service provider will retain backup copies of the cloud service customer data during the termination process (in case of problems with the retrieval process or for legal purposes). :**90 days**	Mandatory and specify details		

	c. Residual data retention (refers to a description of any data relating to the cloud service customer which is retained after the end of the termination process – typically this will be cloud service derived data, which could be subject to regulatory controls): **90**	Mandatory and specify details		
	d. Log Access Availability (what log file entries the cloud service customer has access to)	Mandatory and specify details		
	e. Logs retention period (the period of time during which logs are available for analysis) **:90**	Mandatory and specify details		
	f. Backup Requirements :The bidder to provide details			
	i. Data Mirroring Latency (the difference between the time data is placed on primary storage and the time the same data is placed on mirrored storage) ii. Data Backup Method (list of method(s) used to backup cloud service customer data): iii. Data Backup Frequency (the period of time between complete backups of data) iv. Backup Retention Time (the period of time a given backup is available for use in data restoration) v. Backup Generations (the number of backup generations available for use in data restoration) vi. Maximum Data Restoration time (the committed time taken to restore cloud service customer data from a backup)	Mandatory and specify details I Ii Iii Iv V Vi		
	g. Provide support for automation tools for data portability	Mandatory and specify details		

	h. Data portability format (the electronic format(s) in which cloud service customer data can be transferred to/accessed from the cloud service)	Mandatory and specify details		
	i. Data portability interface (the mechanisms which can be used to transfer cloud service customer data to and from the cloud service. This specification potentially includes the specification of transport protocols and the specification of APIs or of any other mechanism that is supported)	Mandatory and specify details		
	j. Data transfer rate (refers to the minimum rate at which cloud service customer data can be transferred to/from the cloud service using the mechanism(s) stated in the data interface)	Mandatory and specify details		
20	**Exit Management /Transition out services from Cloud Service Provider/OEM**	Mandatory and specify details		
20.1	The responsibilities of the bidder/cloud service provider /OEM upon exit or transitioning out the services from Cloud service provider include: Migration of the VMs, data, content and any other assets to the new environment or on alternate cloud service provider's offerings and ensuring successful deployment and running of the LIC solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to LIC supplied industry standard media.	Mandatory and specify details		
20.2	The format of the data transmitted from the cloud service provider to the LIC should leverage standard data formats (e.g., OVF, VHD…) whenever possible to ease and enhance portability.	Mandatory and specify details		
20.3	The ownership of the data generated upon usage of the system, at any point	Mandatory and specify details		

	of time during the contract or expiry or termination of the contract, shall rest absolutely with LIC.			
20.4	Bidder/Cloud service provider/OEM should ensure that all the documentation required for smooth transition including configuration documents are kept up to date	Mandatory and specify details		
20.5	Bidder/Cloud service provider /OEM should ensure that the CSP does not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement) without the express approval of LIC .	Mandatory and specify details		
20.6	Bidder/Cloud service Provider/OEM should ensure that once the exit process is completed, data, content and other assets are removed from the cloud environment and Content and data of LIC are destroyed as per stipulations and shall ensure that the data cannot be forensically recovered.	Mandatory and specify details		
21	**Migration Plan**			
	The migration plan to be submitted by bidder should detail out: i. The configuration proposed to fulfill day-1 requirements with the explicit understanding that during the duration of the contract these nominal profile requirements will change ii. Procedures and documentation to be developed and implemented for migration of applications and data & content ,client ie MS outlook ,OWA ,Thunderbird configuration at desktops including redevelopment/additional development that may be required iii. Plans for co-existence of non-cloud and cloud architectures during and after migration iv. Communication, change management, and training needs v. Cloud governance for post-	Mandatory and specify details I Ii Iii Iv V Vi Vii viii		

	implementation vi. Test Plans for verifying successful migration vii. Detailed Risk Management Plan that will identify potential risks, set out possible mitigation approaches, and identifies specific tasks the Service Provider will undertake to help avoid identified risks connected with the Migration			
21.1	**Hardware for Cloud Computing Architecture** 1.Bidder/Cloud Service/Provider/OEM should deploy high availability hardware for cloud infrastructure. *2*.Bidder/Cloud service provider/OEM should regularly back-up the cloud systems for error recovery and the data stream of a backup should be encrypted. 3. LIC should be provided interface to monitor the backup process followed by the bidder/cloud service provider/OEM and LIC should be able keep track of the backups done on the media and the safe custody of the media backup tapes. 4. LIC should be provided interface to monitor the backup restoration test done by the bidder /cloud service provider and ensure that the backup restoration testing is done once in a quarter. 5. The DR plan should cover the recovery strategies for systems in cloud environment. The Geographical Location of the Disaster Recovery Environment should be different seismic zone from the production environment or at a different place other than the Primary DC 6. The location of the physical servers and LIC data at rest should be in India to ensure conformance with specific	Manadatory and give details i. ii. iii iv v vi vii viii ix x		

	regional privacy and security regulations of IRDAI 7. The bidder/Cloud service provider/OEM should report major information security and physical security incident and ensure that the incident reporting occurs without fail. 8. The bidder/Cloud service provider/OEM will be owner and responsible for the maintenance of the assets and the licensing must be done by the bidder/cloud service provider/OEM . 9. Bidder/Cloud Service provider/OEM should ensure that cloud infrastructure has similar data sensitivity and recovery requirements as that are hosted in LIC network. 10.Cloud service provider/Bidder/OEM should share details about the recent vulnerability assessment conducted, patch and configuration management processes done to ensure a timely maintenance of assets.			