Corrigendum-5

Name of Work: **RFP for Selection of System Integrator (SI) for Monitoring Infrastructure Projects using IDDP for MMRDA (RFP CA NO.03/MMRDA/IT CELL/SM/2024-25).**

RFP/ Corrigendum 2 Reference (Section and Page Number)	Published as	To be read as
Section 24.2 Annexure A Bid Price (Financial): Summary (Page No.56)	**Implementation & Support Cost:** GIS based web application Common Data Environment Helpdesk & Facility Management Any Other Item.	**Implementation & Support Cost:** GIS based web application Common Data Environment 5D BIM Software Helpdesk Any Other Item
RFP Clause No.12.1 Cloud Requirement & Hosting Services, (Page No.101)	Reliability: The Cloud shall be reliable to comply with the SLA requirements provided in Chapter 14 and there shall not be any outages. Cloud platform shall always run in redundancy/High Availability so that in case of any outage system shall automatically switch to the available servers h) The specification of the servers shall be designed to ensure high availability of servers. All the major servers shall be configured in such a way that there is no single point of failure. In case there is any requirement of application specific server at any point of	Points related to Redundancy/High Availability mentioned in RFP 12.1 Cloud Requirement & Hosting Services, Reliability Clause No. 12.1, sub clause no. (a), ii, page no.100 & RFP clause No. 12, sub-clause No.12.1, sub-clause no.(h), page no.101 is **omitted.** **Bidder has to maintain required SLA as per RFP .**

RFP/ Corrigendum 2 Reference (Section and Page Number)	Published as	To be read as
	time, the SI shall be required to provide the same also without any additional cost to MMRDA.	
RFP Clause No. 12.1 Cloud Requirement & Hosting Services, (Page No. 101)	e) At Disaster Recovery site 50% of total environment (100% of Production environment) is required. The application environment shall be installed and ready for use without any additional software and Database license cost implication on MMRDA	Bidder can provide DR solution on PAYG model instead of 50% of total environment, but it is mandatory for bidder to meet RPO mentioned in RFP
RFP Clause No.27.4.8 Backup Solution - Clause No. 27.4.8 sub-clause no. 1 to 32, (page no. 339)		Point mentioned in RFP clause no. 27.4.8 Backup Solution, sub-clause no. 1 to 32, RFP page no. 339 is **omitted.** Bidder can offer Cloud Native or 3rd Party Backup Solution to meet backup requirement as per RFP. Bidder will be responsible to manage backup and maintain data redundancy. Bidder need to provide backup of data to MMRDA as and when requested. Bidder should also person periodic backup restoration drill and confirm to MMRDA
RFP Clause NO. 27.4.4 Web Application Firewall -(Page No. 322) 27.4.5 Vulnerability Assessment and Monitoring Service (Page No. 326). 27.4.6 Application Performance Monitoring – (Page No 330) 27.4.7 SIEM Service – (Page No.32) and Corrigendum-2, clause no.27.4.7 , Point no. 1 to 75 (page no.80)		RFP Clause No. 27.4.4 Web Application Firewall - RFP Page No. 322 is **omitted.** RFP Clause No. 27.4.5 Vulnerability Assessment and Monitoring Service - RFP Page No. 326 is **omitted.** RFP Clause No.27.4.6 Application Performance Monitoring - RFP Page no. 330 is **omitted** RFP Clause No. 27.4.7 SIEM Service - Page No.32 and Corrigendum-2, clause no.27.4.7, Point no. 1 to 75-page no.80 is **omitted.** New Clause: Bidder should offer Cloud Native WAF, Vulnerability Assessment and SIEM. Solution should be cloud-native from the same proposed CSP. Cloud Native SIEM should support SIEM, SOAR , UEBA , Threat hunting out of the Box AI/ML

RFP/ Corrigendum 2 Reference (Section and Page Number)	Published as	To be read as
		detection rules and Threat Intelligence capabilities as a single product. Technical Compliance should be as per industry best practice and product features should be available on CSP website with active public link. For monitoring services Cloud Native or 3rd party Monitoring services can be offered to monitor VM Resource Monitoring (CPU, RAM, DIsk, IOPS,etc.), Application Insights/ Monitoring
RFP Clause No. 27.4.3 General Cloud Requirements; (Page No.80)	Object storage should be replicated across multiple DC's for better resiliency and should be designed for 99.99999999999999% (16 9's) durability.	Object storage should be replicated across multiple DC's for better resiliency and should be designed for 99.99% durability.
RFP Sub-clause ii. (Page No 102)	Network Service; DNS as Service: Highly available and scalable Cloud Domain Name System (DNS) web service with features like DNS Failover, DDOS Mitigation, Geo DNS, Latency Based Routing, Weighted Round Robin (WRR) functionality Private DNS for Cloud-based servers, access to management console. The service shall support internal domain names for intranet portals	It is Omitted
RFP Clause No. 12.1 (Page No. 103)	Cloud Advisor: System shall analyze the Cloud environment and provides best practice recommendations (or checks) in five categories: cost optimization, security, fault tolerance, performance, and service limits.	To Be read as: Performance Advisor: System shall analyze the Cloud environment and provides best practice recommendations (or checks) in five categories: cost optimization, security, fault tolerance, performance, and service limits.
RFP Clause no. 12.3 (Page No 103)	a) Network Requirements Independent WAN and last mile Connectivity devices to be commissioned at MMRDA with redundancy	Lease Line to be commissioned at MMRDA with redundancy.
RFP Clause 12.1; (Page no.100)	Cloud Requirement & Hosting Services	iii. Security: The Cloud shall have highest level of security features against both physical as well as cyber threats. It is

RFP/ Corrigendum 2 Reference (Section and Page Number)	Published as	To be read as
	Sub-clause no. iii. Security: The Cloud shall have highest level of security features against both physical as well as cyber threats. It is critical to have a set of IT security management processes and tools to ensure complete cyber security of all applications. An IT security policy, framework and operational guidelines as per ISO 27001 be maintained by the SI and Cloud service provider (CSP) as an overall guideline to all forms of IT security – Physical, application, data, network and cloud.	critical to have a set of IT security management processes and tools to ensure complete cyber security of all applications. An IT security policy, framework and operational guidelines as per ISO 27001 be maintained by the SI and Cloud service provider (CSP) as an overall guideline to all forms of IT security – Physical, application, data, network and cloud.
RFP clause no.27.4.3 (Page No.321)	General Cloud Requirement 6. The IT infrastructure should be hosted on Government Community Cloud.	As Per the RFP, GCC or VPC (MEITY Empanelled) can participate.
RFP Clause 27.4.2; SL.No.36 (Page No.320)	Cloud System should have provision to live migration of virtual machine to another physical servers in case of any failure.	Cloud System should have provision to live migration of virtual machine to another virtual machine in DR in case of any failure.
Corrigendum-2 Point No.21 Section 26.1.12 (Page No.13)	**Response: Arbitration Act** The arbitration shall be governed by the provisions of the Indian Arbitration and Conciliation Act, 1966	The arbitration shall be governed by the provisions of the Indian Arbitration and Conciliation **Act, 1996**.

Date: 29.08.2024

Place: Mumbai

No.: IT Cell/2024

Sd/-

Additional Metropolitan Commissioner-II

MMRDA