Corrigendum I

Tender Reference No: AIR/IT-001/2017 **Dated: 08.09.2017**	**Supply, Installation, Commissioning, Implementation of IT Security Solutions for Air India Ltd.**

Following changes have been made to the Request for Proposal (RFP) for Supply, Installation, Commissioning, Implementation of IT Security Solutions for Air India Ltd.

Sl. No.	Reference in RFP	As Appearing in the Original Published RFP	Changes/ Modifications
1	Individual Solution's Technical Requirements-Solution 'B' Secure Web Gateway and Content Filtering Solution, 2(B), Clause 5.4.2 , page 55 (Point 4) & Page 38 Point 4	Should Support external Load balancer as High Availability option and HA in Transparent Bridge Mode	Please read clause as: Solution should Support external Load balancer as High Availability option if required in future.
2	General Requirments Broad General Requirements for Security Architecture Project, Clause 5.4.1, Point 1, Page 48 & Page 26, Point 3.1	OEM should attain ISO 27001 Certification as well as should attain ISO for its Support Services	This Clause is deleted.
3	Individual Solution's Technical Requirements-Solution 'A' Next Generation Security Architecture-UTM (Firewall with IPS), Clause 5.4.2, Basic Criteria- 1a, Page 49 & Page 32 Point 1 a)	OEM should attain ISO 27001 certification as well as should attain ISO for its Support Services	This Clause is deleted.
4	Individual Solution's Technical Requirements-Solution 'A' Next Generation Security Architecture-UTM (Firewall with IPS), Clause 5.4.2, Basic Criteria - 1f, page 50 & Page 32 point 1 f)	Firewall throughput of 100,000 Gbps	Please read clause as: Firewall throughput of 100 Gbps
5	Individual Solution's Technical Requirements-Solution 'A' Next Generation Security Architecture-UTM (Firewall with IPS), Clause 5.4.2, General Features- 2n, page 50 & Page 33 point 2 n)	4 Eye Authentication feature for data integrity.	This Clause is deleted.
6	Gateway Antivirus, Anti-Spyware and Anti-Spam, Point 3, Page 50 & Page 33 point 3	Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email	Please read clause as: Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time

Sl. No.	Reference in RFP	As Appearing in the Original Published RFP	Changes/ Modifications
		address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Recurrent pattern Detection Technology for AS. Self Service Quarantine area. Should have dual AV engine, Email Encryption, Recipient self-registration SPX password management, DLP engine with automatic scanning of emails and attachments for sensitive data	blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Should have dual AV engine, Email Encryption, Recipient self-registration, SPX password management, data protection engine with automatic scanning of emails and attachments for sensitive data.
7	Section 1: Instructions to Bidder , Page 5, Point 3 – Eligibility of Bidders	A bidder should be a Company, registered under the Indian Companies Act, 1956/ Revised Companies Act, 2013 with a minimum of 05 years into Operation having experience in providing complete IT security solutions architecture in any large company with Pan India infrastructure setup.	Please read clause as: Bidder should be a Company, registered under the Indian Companies Act, 1956/ Revised Companies Act, 2013 with a minimum of 05 years into Operation having experience in providing complete IT security/ IT Infrastructure solutions.
8	Section 2: Data Sheet Page 16, Point 8- Pre-Qualification Critieria	(a) The bidder (Company) must be an OEM or its Authorized Vendor and should be a Company registered under the Indian Companies Act, 1956/ Revised Companies Act, 2013. with a minimum of five (05) years into Operation, having relevant experience in providing IT security solutions. (Incorporation/ Registration Certificate required).	Please read clause as: (a) The bidder (Company) must be an OEM or its Authorized Vendor and should be a Company registered under the Indian Companies Act, 1956/ Revised Companies Act, 2013. with a minimum of five (05) years into Operation, having experience in providing complete IT security / IT Infrastructure solutions. (Incorporation/ Registration Certificate required).
9	Individual Solution's Technical Requirements- Solution 'B' On-Premise Anti – APT Solution Page 53, Point 35 , Page 87, Point 35 & Page 36 point 35	The proposed solution should have an endpoint security component and should have following functionalities (Antivirus, antimalware, Ransomeware protection, C&C detection, and ability to quarantine and clean the infected files, ability to integrate with Anti APT components and automatically block/Quarantine zero day malwares by sharing Indicators of Compromise.	Please read clause as: The proposed solution should have an endpoint security component and should have following functionalities (Antivirus, antimalware, ransom ware protection, Vulnerability Protection in endpoint, integrated DLP and C&C detection, ability to quarantine and clean the infected files, ability to integrate with Anti APT components

Sl. No.	Reference in RFP	As Appearing in the Original Published RFP	Changes/ Modifications
			and automatically block/Quarantine zero day malwares by sharing Indicators of Compromise.
10	Technical Requirements, Clause 5.4.2 Point 6 -, page 51 Security Features & Page 33 point 6	Intrusion Prevention System (IPS): For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures: Default (5000+), Custom , IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates from CR Protect networks, Protocol Anomaly Detection	Please read clause as: Intrusion Prevention System (IPS): For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures: Default (5000+), Custom , IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates, Protocol Anomaly Detection
11	Technical Requirements, Clause 5.4.2 Point 12 d) -, page 51 & Page 34 point 12 d) Monitoring and Reporting System	b) · Should provide User Threat Quotient (UTQ) report for actionable security intelligence, helping Administrators identify risky users with ease within the organization's network.	This Clause is deleted.

Except for the changes mentioned above, all other terms and conditions of the original RFP document remains unchanged.