

Appendix 1

RFP UJ 37/2023: Provision and Implementation of a Domain Based Message

Authentication, Reporting and Conformance Tool

#	Requirement	Maximum attainable Points	Compliance		Explanation of Compliance
	Key Requirements		Yes	No	
1.	The Contractor shall implement DMARC Protection, Monitoring and Reporting at UJ ICS, insuring integration with the existing UJ ICS hybrid IT Infrastructure (on premise and in the cloud). This work can be done remotely or on-site with at least 3 days prior arrangement.				
2.	The Contractor shall provide minimum two (2) days of vendor authorised training (presented in English) for up to five (5) staff of the UJ ICS department, in the operation and maintenance of the System immediately after the installation of the System. The training should be delivered remotely.				
3.	The Contractor shall: - Complete and hand over to UJ ICS Team a set of technical design documents, operation and servicing manuals and technical architecture documents; - Deployment documents and technical architecture documents; - Testing and acceptance document;				
4.	The Contractor will create a Testing and Acceptance document. This document shall record the results of System testing and shall demonstrate System's compliance to product performance specifications. The Contractor shall recommend, based on Contractor's technical expertise, a DMARC Compliance Score scheme.				

Appendix 1
RFP UJ 37/2023: Provision and Implementation of a Domain Based Message
Authentication, Reporting and Conformance Tool

	This scheme will have measurable Key Performance Indicators (KPI's) to assess effectiveness of the DMARC performance (e.g, "Good," "Moderate," etc.) in order to set a clear benchmark for improvement.				
5.	The Contractor shall: <ul style="list-style-type: none"> - Provide resolution within 4 hours of designation of an incident at the highest severity level; - Actively participate in resolution of identified problems and root cause analysis in which Contractor provided components are involved; - Acknowledge all reported tickets / incidents by either email or phone call within one hour of being reported by the UJ ICS team; - Ensure Service availability at least 99.9%; 				
Technical Requirements					
1.	The System shall be capable to analyse and interpret UJ ICS Email reports (configured domains – uj.ac.za; jbs.ac.za) to identify authorized and unauthorized traffic	10			
2.	The System shall be capable to monitor and report all security and/ or configuration issues through user friendly dashboards	10			
3.	The System shall be capable to create dashboard-s that display all sources of traffic (authorized and unauthorised)	5			
4.	The System shall be capable to visualize reports with reading friendly display, providing instant overview of DMARC compliance and Email traffic	10			

Appendix 1

RFP UJ 37/2023: Provision and Implementation of a Domain Based Message Authentication, Reporting and Conformance Tool

5.	The System shall be capable to provide Multi-Factor Authentication (MFA) for authorised users	5			
6.	The System shall be capable to provide API to integrate into existing security dashboards, as well as, to common SIEM solutions.	5			
7.	The System shall be capable to provide and maintain DNS record database that contains data sets on mail servers from a large DNS domain base, while being updated regularly on timely manner, at the same time, tracks changes to ensure that UJ ICS is provided with most current and comprehensive database of known Email senders	10			
Maintenance, Support and Personnel Requirements					
1.	The Contractor shall provide regular system updates and schedule annual maintenance in coordination with UJ ICS department	5			
2.	The Contractor shall provide a 24/7 online technical support. This includes a mechanism available to log service requests and categorize them by severity levels and response times accordingly as follows: <ul style="list-style-type: none"> • Level 1 (High) – response time within 1 hour • Level 2 (Medium) – response time within 2 hours • Level 3 (Low) – response time within 6 hours 	10			
3.	The Contractor shall provide a telephone number that assures a human response within one-hundred eighty (180) seconds, and an up-to-date e-mail address	5			
Additional Functionality					

Appendix 1
RFP UJ 37/2023: Provision and Implementation of a Domain Based Message
Authentication, Reporting and Conformance Tool

1.	The System shall be capable to provide administrators with action items that are required in order to configure Email services for full DMARC protection	7			
2.	The System shall be capable to provide forensic reports enabling security analysts with detailed insight into Email exploitation methods used by attackers	3			
3.	The System shall be capable to provide capability to classify Email sources as “authorized and non authorized”	10			
4.	The System shall be capable to include SAML SSO integration, with Identity and Access Management (IAM) solutions (i.e. Azure, etc)	3			
5.	The Contractor shall propose any additional features and costs associated with these additional features	2			
Total Points		100			

Company

Authorized representative

Date and Signature