

Annexure A

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



## **Annexure A**

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

## Table of Contents

Overview .....	3
Requirements .....	3
Project Management.....	6
Additional notes .....	6
Evaluation Criteria .....	6

## Specifications

### Overview

The University of Johannesburg (UJ)'s Information and Communications Systems department (ICS) is responsible to provide IT services to enable UJ to meet its strategic objectives of research, teaching and learning.

The ICS department currently makes use of a hybrid Email infrastructure on the staff tenant to ensure that the email accounts remain secure, ICS would like to implement a Domain-based Message Authentication, Reporting, and Conformance tool (DMARC) to enhance the email security, monitoring and reporting. Email accounts are assigned according to Microsoft terminology of information workers (4200) and non-information workers (17 048) for the Staff tenant and Johannesburg Business School (JBS) email accounts (75) (fully cloud based).

The ICS department is currently undertaking a project to implement a DMARC tool on the staff tenant and JBS tenant. ICS would like implementation, monitoring and reporting available to them once the DMARC tool tender has been allocated. We request that suppliers submit proposals as per the specifications and requirements stated below.

### Requirements

The successful supplier **must** meet the following requirements and list any value added or extra features not listed below:

#### 1.1 Introduction

UJ ICS requires the successful bidder, the Contractor, to provide the delivery, installation, testing, commissioning, maintenance and knowledge transfer of DMARC Protection, Monitoring and Reporting Tool Set.

##### 1.1.1 Accreditations

An accreditation (from the International Organisation for Standardisation (ISO 27001)) or an on-going accreditation process by a certified accreditation body will be an asset (desirable).

#### 1.2 Work to be performed

Implement a system able to provide adequate DMARC Protection, Monitoring and Reporting capabilities for UJ ICS

##### 1.2.1 Key requirements

Refer to Appendix 1

### **1.2.2 Technical Requirements**

The System shall be capable to:

- Analyse and interpret UJ ICS email reports (configured domains) to identify authorized and unauthorized traffic;
- Monitor and report all security and / or configuration issues through user friendly dashboards;
- Create dashboard-s that display all sources of traffic (authorised and unauthorised);
- Visualise reports with reading friendly display, providing instant overview of DMARC compliance and email traffic;
- Provide Multi-Factor Authentication (MFA) for authorised users;
- Provide integration to common SIEM solutions;
- 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.

### **1.2.3 Maintenance, Support and Personnel Requirements**

- a) Provide regular system updates and schedule annual maintenance in coordination with UJ ICS;
- b) Provide a 24/7 online technical support. This includes a mechanism available to log service requests and categorise them by severity levels and response times accordingly as follows:
  - o Level 1 (High) – response time within 1 hour
  - o Level 2 (Medium) – response time within 2 hours
  - o Level 3 (Low) – response time within 6 hours
- c) Provide a telephone number that assures a human response within one - hundred eighty (180) seconds, and an up-to-date email address.

### **1.2.4 Additional Functionality**

The System shall be capable to:

- Provide administrators with action items that are required in order to configure email services for full DMARC protection;
- Provide forensic reports enabling security analysts with detailed insight into email exploitation methods used by attackers;
- Provide capability to classify email sources as “authorised and non authorised”;
- Include SAML SSO integration, with Identity and Access Management (IAM) solutions (i.e. Azure etc.);
- A Contractor shall propose any additional features and costs associated with these additional features;

**\*\* Please note, in response to section 1.2.1 Appendix 1 (Format responding to requirements) need to be completed and submitted with the technical proposal.**

### **1.2.5 Place of Performance**

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.

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.

The Contractor shall:

- Complete and hand over to UJ ICS Team a set of technical design documents, operation and servicing manuals and technical drawings;
- Deployment documents and technical drawings;
- Testing and acceptance document;

### **1.2.6 Timelines**

System implementation should be completed and operational one (1) month after UJ Tender has been awarded. Should extra time be required this needs to be communicated with the UJ ICS team via the UJ Tender office.

### **1.2.7 Reporting requirements**

Once installation is completed, the system shall be tested by the Contractor together with the UJ ICS team, to demonstrate that performance meets the manufacturer's performance specifications and the requirements specified in the Specifications and Requirements document.

As specified in section 2.2.5 of the Specifications and Requirements document, UJ ICS team and 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. 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.

### **1.2.8 Performance monitoring**

The Contractor shall:

- 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%;

### **Project Management**

Project management methodology must be included indicating approach that will be used for the UJ project

The project duration from site handover will be 1 month (from site handover). The service provider to ensure that the programme/methodology to demonstrate the following:

- The programme to be sequenced properly
- The activities need to be linked
- Indicate a critical path

1.2.9 High level project plan to be included as part of the submission.

1.2.10 Detailed project plan will be required by the successful service provider after awarding.

### **Additional notes**

- The response must adhere to the requirements strictly. Deviations must be clearly mentioned and explained. However, it will be at the sole discretion of UJ to accept or reject such deviations.
- Health and Safety file to be submitted after the award and compliance to COVID protocols to be strictly adhered to.
- Contract to be signed between the two parties for the duration of the implementation of the project before implementation of DMARC tool is done.

### **Evaluation Criteria**

The RFP will be evaluated in three (3) stages,

Stage 1 – Tender Compliance requirements

Stage 2 – Functionality / Technical

Stage 3 – Financial and B-BBEE

#### **1.2.11 Key Requirements**

<b>Requirement</b>	<b>Maximum attainable Points</b>
Key requirements (Appendix 1)	Bidder needs to comply to move on to Stage 2

**1.2.12 Functionality**

Requirement	Maximum attainable Points
Technical Requirements (1.2.2 and Appendix 1)	55
Maintenance, Support and Personnel Requirements (1.2.3 and Appendix 1)	20
Additional Functionality (1.2.4 and Appendix 1)	25
<b>Total points awarded</b>	<b>100</b>

A minimum of 70 points is required by any tenderer before further evaluation. All tenders who achieve 70 points or more will be evaluated equally in terms of stage 3.

**1.2.13 Financial and B-BBEE**

- Price (80 points)
- BBEE (20 points)

**Other Information**

Please supply any other information that you think is useful for the submission that needs to be completed.