CSIR-INDIAN INSTITUTE OF INTEGRATIVE MEDICINE

Council of Scientific & Industrial Research
CANAL ROAD, JAMMU
Phones: 0191-2585000, 2585006 to 13, 15, 18 (11 Lines) Tele fax: 2585032, 2585019

File No. 06(278)/19-P **Dated: 04-12-2020**

CORRIGENDUM

Reference to Tender_id: **2020_CSIR_63368_1** for "**Third party Mobile Application (Android) Security Audit, Report Generation including recommendations",** the **Technical Specification** is enclosed below as **Annexure-I**. All other terms and conditions will be remained same.

Sd/-
Stores & Purchase Officer

Annexure-I

Third party Mobile Applications (android) Security Audit, report generation including recommendations and issue of Clearance certificate

1. **Background**

Third party security/privacy/protection validation audit for a mobile application named " COVID KAVACH APP" for elective data management of health/clinical data of participants involved the clinical trials is required .
COVID KAVACH APP made by third party for effective data management and alerts of participants of the clinical trials. This App is expected to provide real-me data on the clinical status of participants.
This App is expected to track the participant's symptoms and manage participants at admin level with the help of web based admin panel. Admin panel includes Super admin, Invigilator, Site coordinator modules. Each module have different role as per the requirement. Goal for the app is to develop user friendly app which can be easily usable to common man and also able to track the data of the participants digitally.

Mobile Application Security Audit Testing	
Parameters	Description
Mobile Application Name	**COVID Kavach**
Development platform Details (E.g. Android, iphone, Windows etc.)	Android
Authorization No. of roles & types of privileges for the different roles	Participant's role. Participant can add daily symptoms
Total No. (Approximate) of Input Screens	Login screen, profile screen, submit symptoms =Total no of screens 3
Total No. of input fields	11 to 12
Number of Web Services, if any	7
Number of methods in all web services	2 methods get and post

Scope of Mobile Application Security Testing

Vulnerability assessment and penetration and Gray box assessment with the Vulnerabilities testing.

The vendor should follow frameworks such as OWASP. The target areas for carrying out VAPT are: Android Mobile App

Any other activity concerning security audit related aspects, not essentially covered by work areas outlined as above.

Cont…

Deliverables

- Mobile Application Security Audit Report based upon vulnerability assessment and penetration testing (VAPT) observations, Gray box assessment with the Vulnerabilities and Flaws highlighted along with recommendations
- Executive summary of observations

Observations covering the following:

- Observation (in case of VA PT observations details of CVE, technical vulnerability)
- Clearance certificate for Android Mobile application

The bidder will be responsible for using their own tools for conducting VAPT and no cost/compliances shall be borne by IIIM.

C. Eligibility criteria:

The company participating in this as a bidder must have the following:

- ➔ The agency /bidder must be in the current empanelment of CERT-IN for IT Security Audit.
- ➔ Must have at least 2 CISA qualified/2 CEH qualified /1 OSCP qualified permanent employees in the organization at least for 6 months
- ➔ Must have conducted at least 6 assignments of covering similar scope area(s) in the past 2 years