BOSNIA AND HERZEGOVINA

FEDERATION OF BOSNIA AND HERZEGOVINA

FEDERAL ADMINISTRATION FOR GEODETIC AND REAL PROPERTY AFFAIRS

REAL ESTATE REGISTRATION PROJECT IMPLEMENTATION UNIT

TERMS OF REFERENCE

FOR A PROJECT OF VULNERABILITY SCANNING AND PENETRATION TESTING OF THE LOCAL NETWORK AND KEY INFORMATION SYSTEMS OF THE LR AND C INSTITUTIONS (katastar.ba and E-GRUNT)

Bosnia and Herzegovina, October 2023

Contents

1. Introduction

The purpose of the project of vulnerability **scanning and penetration testing of the local networks and key information systems of the LR and C institutions (katastar.ba and E-GRUNT)** (hereinafter: testing project) is to find system security weaknesses in the form of unauthorized access to network, data, applications and other information assets with the ultimate goal of improving system protection measures based on established test results. As a common name for the Federal Administration for Geodetic and Real Property Affairs, Federal Ministry of Justice, Cadastral offices and Land Registry offices in the subsequent text of this document, the term LR and C institutions shall be used whenever all four institutions are referenced.

The scope of the project includes vulnerability testing and penetration testing of internal and external network infrastructure as well as critical applications, using a standard methodology that includes the use of manual and automated testing techniques and identification of vulnerabilities and weaknesses.

2. Background information

Real Estate Registration Project, Additional Financing (hereinafter: "Project") is implemented on the basis of the Loan Agreement - Real Estate Registration Project, Additional Financing - between Bosnia and Herzegovina and the International Bank for Reconstruction and Development - IBRD (hereinafter: "Bank ") Signed on July 2, 2020, and the Decision on Ratification of the Loan Agreement (" Official Gazette of BiH ", International Agreements No. 19/20 of December 19, 2020).

The objective of the Project is to support development of a sustainable real estate registration system with harmonized land register and cadastre records in urban areas of both the Federation of Bosnia and Herzegovina and the Republika Srpska. Real estate registers, land registers and cadastres, provide base information layers for land administration and for the establishment of a National Spatial Data Infrastructure. They are considered harmonized when their contents are aligned, interlinked and verified. Sustainability is measured by the degree an institution generates revenue to match its costs, charges affordable fees, delivers quality services without discrimination and within a reasonable time. A key driving force for the real estate registration system will be the registration of real estate rights and mortgages, and the availability of reliable information to facilitate investments, real estate taxation and spatial planning, and to enable social monitoring of real estate transactions.

The Project in the FBH is managed by the Federal Administration for Geodetic and Real Property Affairs. The Project Implementation Unit established in the Federal Administration for Geodetic and Real Property Affairs is the operative and executive body of the Project consisting of civil servants and contracted specialists with professional background necessary for successful implementation of the Project activities.

Cyber Security Policy and Action Plan for real estate/land cadaster and land register were prepared under Project activity. The Cyber Security Policy is an umbrella, strategic document that defines the requirements, standards and goals of cyber security, while the Cyber Security Action Plan is a document that defines how to achieve the set goals and fulfill the requirements through the implementation of security improvements, i.e., projects as well as project activities, and identification of resources necessary for the implementation of these activities.

LR and C institutions established a Working Group to monitor the implementation of the Cyber Security Action Plan. One of the main tasks of the working group is to supervise the realization of the contract for the Testing project.

2.1 Institutional Framework for the Land Administration Sector in the Federation of BiH

The institutional framework for the land administration sector is defined by the Law on Ministries and Other Bodies of Administration of the Federation of BiH , the Law on Courts in the Federation of Bosnia and Herzegovina and cantonal laws on cantonal ministries and other administrative bodies, while the operation of the administrative bodies in the Federation of BiH is stipulated by the Law on Organization of Administrative Bodies in the Federation of Bosnia and Herzegovina .

The Federal Administration for Geodetic and Real Property Affairs (hereinafter: the FGA) is responsible for all geodetic affairs, including the cadaster. The FGA performs administrative and other technical tasks which fall under the competence of the Federation of BiH, relating to survey, establishment and updating of real estate cadaster and utility cadaster, apart from the tasks that have been made the competence of the cantons and the municipalities under the law, mapping of the territory of the Federation of BiH, geodetic and cartographic affairs that are of relevance to defense, management of technical archives of original plans and maps of basic geodetic works and other records obtained through performance of geodetic works, land consolidation and special purpose land survey, real property records, submitting proposals for re-privatization of property and inspection control of activities involving survey, real estate cadaster, land cadaster and utility cadaster. The FGA, among other responsibilities, carries out professional and inspection supervision of works related to survey and real estate cadaster in the Federation of BiH. Furthermore, there are four cantonal administrations for geodetic and real property affairs, which are established as independent administrative bodies in the Herzegovina-Neretva Canton, the Central Bosnia Canton, the West-Herzegovina Canton and the Canton 10.

Cadastral offices in the Federation of BiH are part of the municipal administration, with responsibility to maintain the survey and real estate cadaster, including monitoring, identification and surveying of technical changes on land, buildings and other objects that impact survey and real estate cadaster records, registering identified changes in geodetic plans, maps, the survey elaborate and the cadastral operate, as well as registering changes pertaining to registered real property rights in relevant registration sheets. In the Federation of BiH, there are overall 79 municipal cadastral offices as part of the municipal administration, under supervision of the FGA.

The cadastral information system of the Federation BiH (hereinafter: the CIS) was established in 2012 with a distributed architecture, i.e. local servers with clients have been established in all 79 cadastral offices, while the central server that consolidates cadastral data from all over Federation of BiH is located in the FGA. The key element of CIS is the cadastral software in FBiH – katastar.ba, supporting all processes regarding the real estate cadaster database. Access to the data has been provided via two groups of services: public and user services. The first group of services, public services, is available at the address www.katastar.ba and it allows an insight in alpha-numerical and graphic data of the real estate data base, and provides seven services. The second group of services, user services, that is accessible through the OGC standardized web services, which allows viewing, taking over and making inquiries.

Federal Ministry of Justice has jurisdiction to perform administrative, technical and other tasks provided for by the law pertinent to, inter alia, exercising of the authority in the fields of judiciary and judicial administration, as well as administrative oversight of the operations of the judicial administration.

High Judicial and Prosecutorial Council BiH (hereinafter: the HJPC) is independent body of the BiH with its competencies defined in the Law on the HJPC. The competences of the HJPC of BiH are defined by the Law on the HJPC of BiH and refer, among other things, to appointment of holders of judicial functions at all levels in BiH, disciplinary responsibility of judges and prosecutors, proposing annual budgets for courts and prosecutor's offices, professional training of judges and prosecutors, judicial administration and supervision, coordination and supervision of the use of information technology in courts and prosecutor's offices, giving opinions on draft laws, regulations and important issues that may affect the judiciary, initiation of the procedure for the adoption of laws and other regulations in areas important for the judiciary.

Maintenance of the land registry in the Federation of BiH falls under the competence of the municipal courts, which provide services of real estate registration and registration of the rights over real estate. Pursuant to the Law on Land Registry , LR offices are part of municipal courts. The municipal court where a real estate is located has territorial jurisdiction over registration of the estate. The seat and territory of municipal courts and branches outside the court seat are defined by the Law on Courts in the Federation of Bosnia and Herzegovina and 33 (thirty-three) courts with five (5) branches outside the seat of municipal court are currently operational. Services that land registry offices provide to the interested parties are prescribed by the Law on Land Registry and primarily include appropriate registration in the land registry (entry, notation and pre-entry). The same Law also provides for services of issuing land registry extracts and allowing viewing of land books under certain conditions. E-Grunt software has been installed in all land registry offices and it covers main registration tasks of the LR office and it operates in a distributed model/environment (each court has its own server and a certain number of clients). The communication links (VPN) have been established between databases of LR offices and the central FBiH LR database located on the premises of the Federal Ministry of Justice in Sarajevo. As of 31 January 2017, internet presentation of FBiH LR data has been established (address: www.e-grunt.ba). It enables online insight into the legal status of properties in the Federation of BiH by accessing data on the basis of the parcel number or number of land registry folio.

The land administration services have considerably improved with the digitization of records, implementation of tailor-made software solutions and systematic harmonization of real estate data between the cadaster and the land registry under the parent Real Estate Registration Project and previously implemented the Land Registration Project. Reform of the land administration sector aims at harmonizing the data between the cadaster and the land registry with ultimate goal to establish the land registry data based on the Austro-Hungarian survey with the cadastral data from the new survey. According to the short term objectives of the ICT Strategy, existing cadastral and land registry IT systems were improved to be able for data exchange based on services. Nonetheless, given that there is no Law on Electronic Signature, official data exchange is in analogue (printed) form.

2.2 Existing Regulations on Information and System security

Based on the **ICT Strategy** for Land Registry and Real Estate/Land Cadastre in the Federation of BiH for the period of 2019.-2029, as well as good business practice based on ISO/IEC 27001 and ISO/IEC 27002 standards, a **Cyber security policy** has been defined and developed, containing strategic goals and standards related to a set of security measures to preserve the confidentiality, authenticity and availability of information. **Cyber security policy** is an umbrella document related to information security and data protection in the field of real estate/land cadastre and land registry of the Federation BiH. Based on the developed and adopted policy, an **Action plan for cyber security** was developed. Cyber security action plan represents document that defines how to realize the set goals and fulfil the required requirements, through the implementation of security enhancements, i.e. projects as well as project activities and determining the resources needed for the realization of those activities defined by phases as short-term, medium-term and long-term. In the existing laws in the Federation of BiH, there are no regulations on cyber security in the land registry administration. It's in the process amendment of the current regulations defining the rules for the security of information and the land registry administration system of the Federation of Bosnia and Herzegovina in accordance with the Cyber Security Policy and ISO/IEC 27001 and ISO/IEC 27002 standards.

3. Objectives of the project

According to the ISO/IEC 27000:2018 standard, which provides an overview of terms and definitions in the field of information security, information is an asset that is owned by the organization and needs to be protected. Information can be stored in many forms, including digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees. Information can be transmitted by various means, via electronic or verbal communication or devices and equipment such as a laptop or USB drive. Whatever form information takes, or the means by which it is transmitted, it always needs appropriate protection. In addition, information and communication technologies (ICT) are an important element in information protection because they are an integral part of the complete life cycle of information (from creation, through processing, storage, transmission, protection to destruction).

Information security ensures the confidentiality, availability and integrity of information. Information security implies the implementation of adequate measures that protect information from various threats with the aim of ensuring sustained business success and continuity and minimizing consequences of information security incidents.

Information security is achieved through implementation of a set of measures that are determined based on the results of risk assessment and includes policies, procedures, processes, organization, software, IT infrastructure and services to protect information and information assets that contain information. Information security measures need to be established, implemented, monitored, reviewed and improved, where necessary, in order to ensure information security and business objectives.

4. Scope of work

Functional requirements of the project are:

- Vulnerability scanning and penetration testing of external network infrastructure is performed by application of „Grey box“ type of testing, which includes the simulation of a malicious user, testing without detailed knowledge of the internal structure of the system and access from the public network (Internet). The testing scope includes up to 150 external addresses which will be chosen by customer. External infrastructure includes following services: DNS, firewall, VPN, routers, email and other devices and services that are located on the local network perimeter and directly connected to the Internet. The service provider will be assigned a VPN account in order to perform testing in the case of an established VPN connection;

- Vulnerability scanning and penetration testing of internal network infrastructure is performed by application of „Grey box“ type of testing, which includes the simulation of a malicious user from the internal local network, that includes 250 internal addresses which will be chosen by customer. Testing of the internal infrastructure is preferable to be tested from LAN and WAN customer network;

- Vulnerability scanning and penetration testing of key information systems of the LR and C institutions (katastar.ba and E-GRUNT) is performed by implementation of „Grey box“ type of testing, and the minimum necessary information will be delivered to the service provider by the customer side. Testing of mentioned information systems includes vulnerability testing in the application code, security protocols and security patches, possible vulnerabilities of the web service katastar.ba and E-GRUNT that are in use, as well as resistance testing of the existing security measures to various types of attacks (denial of service, backdoors, cookie poisoning, forceful browsing, etc.).

The service includes retesting which is performed in the event that in the first iteration of vulnerability scanning and penetration testing, there is a detection or exploitation of a vulnerability that affects the security of the system. These are critical and high-risk vulnerabilities. The functional requirements under which the retest is performed are the same as the functional requirements listed above for the initial testing.

Conducting retesting confirms the closure of only detected/exploited vulnerabilities, without re-conducting complete testing as in the first iteration.

In case of conducting retesting, a reasonable amount of time is necessary to be provided for the client to eliminate the detected risks, i.e. close vulnerabilities.

5. Methodology and work plan

Testing project requires a systematic and thorough methodology. The Service Provider shall develop and document Methodology and work plan in cooperation with the Work group. The Methodology and work plan shall contain description of proposed activities, timeframe and deadlines for all activities and deliverables under this Terms of Reference. A Gantt chart with a graphic presentation of the time schedule of all activities and deliverables shall be an integral part of the Methodology and work plan document.

The Service Provider shall submit the proposal of the Methodology and work plan document to the Work group within two weeks from the date of Contract signing. The Work plan will be final after acceptance by the Work group.

The service provider shall closely cooperate with the Work group on the side of the LR and C institutions, making contact through the contact person in the team.

6. Timeline and Expected deliverables

The Service Provider is requested to submit following deliverables under the conditions of this ToR:

a. Methodology and work plan
b. Detailed project plan
c. Critical or high-risk vulnerability that can lead to significant consequences for the security of the system (optional)
d. Report on testing results with recommendations for risk mitigation (Excel dokument)
e. Updated report on testing results with recommendations for risk mitigation (Excel dokument)
f. Report on testing results with recommendations updated with results of retesting

6.1 Information meeting

The inception meeting shall be held with representatives of the Contracting Authority at the occasion of contract signing, in order to jointly analyze and discuss the ToR.

6.2 Preparation of Methodology and work plan with Gantt chart

In cooperation with the Work group, the service provider shall develop the Methodology and work plan with description of activities, timeframe and deadlines for all activities and deliverables under this Terms of Reference. A Gantt chart with a graphic presentation of the time schedule of all activities and deliverables shall be an integral part of the work plan. The service provider shall submit the proposal of the Work Plan to the Work group within two weeks from the date of Contract signing. The Methodology and work plan will be final after acceptance by the Work group.

6.3 Determining the testing plan

The service provider should confirm understanding of functional project requirements through definition of testing steps and to prepare a detailed testing plan.

Generally, testing of the systems includes system analysis, automated testing with tools, manual testing, analysis of results and reporting on results with recommendations.

Network infrastructure testing has the following steps:

- Design that includes analysis of publicly available information on targeted systems, initial identification of network security vulnerabilities and threat analysis;

- Verification that involves automated system scanning along with network traffic analysis in order to identify weaknesses that allows attacks to be performed. Also, detailed analysis of results is included, in order to identify typical vulnerabilities and prepare detailed attack plans;

- The attack involves performing tests (manual and automated) with the aim to use the vulnerabilities identified in the previous phase and to access without authorization to the systems and to obtain evidence that confirms the existence of vulnerabilities. The expected result of this phase is a list of identified and verified vulnerabilities that allow unauthorized access or create other security risks;

- Risk analysis include a detailed analysis of results in order to identify the causes of identified gaps and definition of recommendations and reporting.

Application testing consists of the following steps:

- Analysis of the purpose of the application, which includes gathering information about the application and the systems that support it;

- Automated application scanning for recognized vulnerabilities using security tools;

- Manual testing in order to identify security risks and perform attacks on vulnerabilities detected during automated scanning. The attacks are ethical and the client is aware of the plan of attack (i.e. attack scenarios);

- Analysis of test results and reporting with recommendations.

Results of this project phase is detailed project plan that contains all necessary steps of internal and external infrastructure testing as well as information systems (katastar.ba and E-GRUNT) including connected applications.

The Service provider shall submit a detailed project plan containing all elements not later than eight weeks from the Contract signing. The Service provider shall present this outcome in the form of the Power Point Presentation to the Work group. The Work group shall submit their comments within 7 calendar days. The updated detailed project plan shall be delivered within 7 calendar days from the date of receiving the comments of the Work group.

6.4 Performing testing according to the adopted project plan

This phase involves testing of the network infrastructure and applications using standard methodology and according to the steps defined in the previous phase.

If, during testing, the service provider detects or exploits a critical or high-risk vulnerability that can lead to significant consequences for the security of the system, the client have to be urgently notified of the issue and recommend immediate measures to address the identified vulnerability and reduce the risk. The client will close the vulnerability as soon as possible. In the meantime, the service provider can continue testing.

The service provider informs the client in written form (through Excel document) on the identified vulnerabilities, provides a brief description of the vulnerability, protentional consequences and risks, and recommends an urgent measures that should be implemented. Every time when vulnerability is identified during the testing, the mentioned Excel document is updated.

Results of this phase is report on testing results with recommendations for risk mitigation. Report contains summary of results with ranked vulnerabilities and protentional risks, as well as the severity of the consequences for the system security. In addition, the result must have a detailed description of project scope, used methodology, testing scenarios, details of identified vulnerabilities and weaknesses as well as instructions for closing identified security gaps.

The Service provider shall submit a Report on testing results with recommendations for risk mitigation containing all elements not later than eighteen weeks from the Contract signing. The Service provider shall present this outcome in the form of the Power Point Presentation to the Work group. The Work group shall submit their comments within 10 calendar days. The updated detailed Report shall be delivered within 10 calendar days from the date of receiving the comments of the Work group.

6.5 Closure of critical and high risk vulnerabilities, if they are identified

If critical or high-risk vulnerabilities have been identified in phase 2, the client will implement the closure of those vulnerabilities based on recommendations received from the service provider, then knowledge and experience of its own systems, as well as with the help of executors who maintain those systems.

After implementation of recommended measures and closing the identified vulnerabilities, the client updates Excel document and sends it to the service provider in order to have information about the applied measures.

6.6 Performing retesting including reporting

If, during testing, critical and high-risk vulnerabilities were identified and closed, the service provider should perform retesting in order to determine whether applied measures are effective. Retesting implies testing that only the measures that closed the critical and high-risk vulnerabilities detected during the initial testing are tested. Retesting does not imply repetition of the initial testing.

Results of the this project phase is report on testing results with recommendations updated with results of retesting. This report should contain all the parts that the report on initial testing also contains, with the fact that if the applied measures are effective, there should be no critical and high-risk vulnerabilities.

The Service provider shall submit a Report on testing results with recommendations updated with results of retesting containing all elements not later than 14 calendar days aftert implementation of recommended measures and closing the identified vulnerabilities. The Work group shall submit their comments within 10 calendar days. The updated detailed Report shall be delivered within 10 calendar days from the date of receiving the comments of the Work group.

7. Resources

The contractor is obliged to provide all the necessary technical, administrative and other resources to perform the tasks described in this ToR.

Key resources that the contracting authority will provide to the service provider:

1. Access to available Data and Information:

- Access to relevant reports, documents, policies, regulations and other documentation necessary for the Testing project.

2. Subject Matter Experts:

- Arrange access to key personnel who possess in-depth knowledge of the current status, policies, and practices.

3. Stakeholder Contact Information:

- Provide contact information for relevant stakeholders, including government officials, administrators, system users, and other parties.

4. Available Legal and Policy Documents:

- Copies of relevant policies, regulations, and legal documents that govern the organization's operations.

5. Access to Facilities and Systems:

- Provide access to facilities, network, data, applications and other information assets, to which the Testing project applies.

6. Support for Stakeholder Engagement:

- Assist in arranging interviews, focus groups, or surveys with stakeholders to gather insights and feedback.

- Provide contact information and help in scheduling interactions with relevant individuals.

7. Budget Allocation:

- Contractor fees, travel expenses, research tools, and any other costs associated with the Testing project are included in the Contract price.

8. Support for Ethical Considerations:

- Provide guidance on ethical considerations, such as obtaining informed consent from stakeholders and adhering to data protection regulations.

- Offer insights into the organization's ethical guidelines and expectations.

9. Access to Decision-Makers:

- Facilitate communication and coordination with decision-makers within the contracting authority to ensure alignment with the Testing project objectives and expectations.

10. Clear Scope and Objectives:

- Clearly communicate the scope, objectives, and expected outcomes of the Testing project to ensure that the contractor's work is aligned with the contracting authority's needs.

11. Regular Communication:

- Establish a communication channel via Working group for regular updates, progress reports, and any queries the Service provider may have during the study.

By providing these resources, the contracting authority will aim empower the Service provider to conduct a thorough and effective Testing project that produces valuable insights and recommendations.

8. Reporting and communication

Through the Working Group, the contracting authority will supervise and guide the services provided by the Service provider, and make final proposals to the contracting authority Director for adoption of documents produced through the Testing project.

The Service provider is obliged to Maintain regular communication with the Working Group, provide updates on milestones achieved, challenges faced, and progress made.

Both the Working Group and the Service provider will ensure that communication is timely, especially when unexpected developments or changes arise during the contract.

- Regular monthly reporting

The Service provider shall submit monthly reports on progress of activities that will, among other things and in addition to the summary, also include the administrative part of the implementation, technical part of the implementation by activity against the Terms of Reference the planned timeframe, possible difficulties and deviations, as well as description of the ways of overcoming the difficulties, deliverables during the observed period, and the Attachments.

- Final report

The Final Report shall contain the description of all activities carried out by the Service Provider during the agreement, and it shall be submitted to the Client within seven working days upon completion of all agreed activities. The Final Report shall be submitted in the form to be agreed with the Client and it shall contain, inter alia, the following:

- Report summary of maximum 4 pages;

- Short description of methodologies used for each phase of testing and scaning, potential difficulties encountered and the manner of overcoming them;

- The main body of the report, organized by type of Vulnerability scanning and penetration testing (external network infrastructure, internal network infrastructure and key information systems of the LR and C institutions). Containing the summary for each activity (type, scope, and dynamics) and recommendations for the future actions.

The Final report should have as annexes all the deliverables.

The Client shall submit its comments within seven days from the receipt of the draft report from the Service Provider, who will be obliged to make corrections in accordance with the comments submitted by the Client.

9. Required skills and expertize

- The service provider should be engaged in information security activities.
- The service provider should have successfully completed at least 2 projects of vulnerability scanning and penetration testing in last 3 years - similar complexity.
- The service provider should use licensed and/or „open source“ software testing tools that have right to use, as well as its own devices (i.e. laptop, desktop computers) that it uses for testing purposes.
- The service provider performs testing under the supervision of the client, according to the detailed plan previously agreed with the client.
- It would be desirable for the Service Provider to have at least one permanently employed or engaged professional with valid certificates (OSCP, OSCE, CEH, GPEN, GWAPT, GXPN, or eCPPT)
- Full-time employee or engaged professional, who will have the role of team leader should have the university degree in engineering from the technical faculty. Have at least 5 years of work experience in providing penetration test services
- It would be desirable for other full-time employees or professionals engaged on the project to have at least 3 years of work experience in providing penetration testing services in similar organizations.
- That the project participants have not been convicted.
- That there are no misdemeanor or criminal proceedings against the persons working on this project.
- The service is implemented in a way that will not lead to loss of functionality of tested systems. If the service provider cannot guarantee the preservation of system functionality and data security, the consent of the client is necessary for the implementation of risk activities.
- All activities that are part of this services as well as data related to this service, systems under test, testing results and other, represent strictly confidential information and can only be shared with the customer.
- After performed implementation of project, the service provider is obliged to remove all changes, if changes are made on existing systems and in the environment where this solution was tested. This includes removing accounts opened for testing purposes, installed test tools, and similarly.

9.1 Selection criteria

The service provider should submit:

- Evidence demonstrating required professional qualifications, skills and experience as defined in Section 2.3;

The service provider will be selected based on the following criteria:

- Formal education: 40%
- Evidence of the experience and qualifications: 60%

10. Contract duration and payments

The given timeframe for contract performance is 180 days from the Contract start.

The payment shall be made in single payment (100%) of total contract value after acceptance off all required reports.

11. Ethical considerations

Ethical considerations are deemed crucial when a Service provider is implementing the Testing project. Below are the basic principles and provisions that the contractor must adhere to during the implementation of the contract, but also in the period after:

- Confidentiality and Privacy:

- Ensure that all sensitive data collected from the organization is treated confidentially.

- Obtain proper permissions to access and use confidential data, adhering to data protection regulations.

- Informed Consent:

- When conducting interviews, surveys, or focus groups, obtain informed consent from participants before collecting their input.

- Clearly explain the purpose of the Testing project, how their data will be used, and any potential risks or benefits.

- Data Integrity and Accuracy:

- Ensure the accuracy and integrity of data collection, analysis, and reporting.

- Avoid manipulation or misrepresentation of data to present findings in a misleading manner.

- Impartiality and Objectivity:

- Maintain impartiality and objectivity throughout the implementation to avoid bias in data interpretation and reporting.

- Declare any potential conflicts of interest that might affect the testing outcomes.

- Full Disclosure:

- Transparently communicate the scope, objectives, methodologies, and limitations of Testing project to stakeholders.

- Disclose any affiliations or relationships that might influence the job outcomes.

- Respect for Stakeholders:

- Respect the perspectives and feedback of all stakeholders, regardless of their position or role.

- Ensure that participants' opinions are accurately represented in documents and reports.

- Avoid Harm and Unintended Consequences:

- Consider the potential impact of the testing findings and recommendations on the organization, stakeholders, and users.

- Avoid suggesting actions that could harm the organization's reputation or stakeholders.

• Transparent Attribution:

- Give proper credit to existing research, literature, and data sources that are used during the Testing project .

- Accurately cite references and acknowledge the work of others to avoid plagiarism.

• Feedback Incorporation:

- Engage stakeholders in providing feedback on the Testing project preliminary findings and recommendations.

- Consider their feedback and adjust the Testing project as necessary, reflecting a collaborative and responsive approach.

• Clear Reporting:

- Present findings and recommendations clearly and accurately, avoiding overstatement or exaggeration.

- Clearly distinguish between empirical data, analysis, and expert opinions.

• Communication and Accountability:

- Maintain open communication with the client, keeping them informed about progress and challenges.

- Take responsibility for the findings and ensure that they are communicated accurately.

• Professionalism:

- Adhere to professional standards and guidelines for research and consultancy.

- Demonstrate respect, integrity, and ethical behavior in all interactions related to the Testing project.

The contracting authority is the owner of all materials that will be the result of this job, and it is not allowed to distribute them to third parties or publish them under any circumstances without written permission.

12. Language

Official languages of the Terms of Reference are one of official languages of the Federation of BiH and English.

All documents and reports that are made by the Contractor under this Terms of Reference shall be delivered to the Contracting Authority in one of official languages in the Federation of BiH, while all the final deliverables must be provided in English as well.

In addition to the electronic copy, the Contractor shall also provide to the Contracting Authority hard copies of all final accepted deliverables.

All relevant costs pertaining to the service provider work (translation, local transport, etc.) will be included in the contract price for engagement of the service provider.

13. ToR Attachments