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 IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS – INFORMATION SECURITY MANAGEMENT SYSTEM)

Bosnia and Herzegovina, October 2023

Contents

1. Introduction

The purpose of the project of implementation of information security management system (ISMS – Information Security Management System) is to systematically set up the framework for information security management in the LR and C institutions. 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 aim of the project is to ensure confidentiality, integrity and availability of information at the organizational level and at the process level, including the implementation of technical security measures, where feasible.

The project scope includes integration of information security management process in all process of the LR and C institutions in which should ensure protection of data from unauthorized access, disclosure and modification and enable the availability of data to authorized persons when necessary. Information security management system should be in accordance with requirements of the ISO/IEC 27001 standard, unique and consistent for all LR and C institutions.

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 implementation of ISMS.

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

The functional requests of this projects are:

- Development of operational procedures and instructions related to the information security in accordance with the ISO/IEC 27001 and ISO/IEC 27002 standards, as well as with requirements defined in the Cyber Security Policy. This implies that information security processes are described at the operational level in steps and with descriptions of roles and responsibilities in those processes related to information security. For the following ISMS areas, procedures end instructions should be established (where applicable):

- Internal organization of ISMS
- information classification
- access control
- password management
- communication security
- operational security
- secure development and maintenance of the system
- security of information in relation to suppliers

- information security incident management

- Creating a list of information assets (server infrastructure, network devices, software licenses, applications, services, etc.) and determining their value in accordance with the information classification scheme;
- Procedure development and establishment of information security risk management process consistently in all LR and C institutions, including risk identification, analysis and risk assessment and definition of strategy for risk treatment including establishment of risk assessment methodology;
- Preparation of training program in the field of information security as well as preparation of materials related to the basic trainings on the development of information security awareness and trainings for persons responsible for information security in the LR and C institutions;
- Provision of the above mentioned trainings to the employees and persons engaged by the LR and C institutions;
- Creating a vulnerability registry and the registry of information security threats that are characteristic for IT infrastructure, systems and services used in the LR and C institutions;
- Determination of risk treatment plan in relation to the results of information security risk assessment;
- Defining information security in the project management process;
- Clock synchronization through all LR and C institutions;
- Definition of agreements on confidentiality and non-disclosure of information including relevant information security requirements aligned with the requirements defined in the Policy;
- Determination of information security continuity plans for critical business systems (primarily katastar.ba and E-GRUNT) as well as IT infrastructure and key services used in the LR and C institutions.

5. Methodology and work plan

Implementation of information security management system (ISMS) in the LR and C institutions 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. ISMS implementation plan
c. Training material and provide trainings
d. Procedure for assessment of ISMS performance
e. Procedure for inconsistencies and corrective measures management
f. Report on internal audit of ISMS

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.

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.

3. Preparation of the ISMS implementation plan

Service provider should confirm the understanding of the functional requirements of project by defining a detailed ISMS implementation plan which should be the key deliverable of this phase. In order to achieve mentioned in this phase, following activities should be performed:

- Forming an ISMS implementation team – The team will consist of a team on the side of the LR and C institutions, team of ISMS implementation service provider and, as necessary, representatives of existing IT system maintenance service provider. Team members and their roles in the project should be defined not later than two weeks from the Contract signing.

- Defining the scope of information security management system – In accordance with the requirements defined in the Cyber Security Policy, ISMS should be implemented as a unique system in the LR and C institutions. The service provider should identify organizational structure and processes in the LR and C institutions in which the information system will be integrated. The purpose of this step is to familiarize service provider with organization in order to understand processes and detect key risks and open questions, if any, that may arise during implementation. The service provider should have a goal to protect information, in terms of ensuring confidentiality, integrity and availability and to be consistent through entire organizational structure and for all processes in the LR and C institutions.

- Development of the ISMS implementation plan – based on previous two steps in which team was formed and the scope of ISMS was determined, development of a detailed implementation plan is necessary, in terms of defining the phases, activities, responsibilities for all activities, results of all activities and the time in which the ISMS implementation activities take place.

As a result of this phase, service provide should deliver ISMS implementation plan in the written form that will contain specified elements, then ISMS scope with organizational structure and process map, including both risks and recommendations for their mitigation, and finally a defined team for implementation with all of the above mentioned members and their roles. The Service provider shall submit a ISMS implementation 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 ISMS implementation plan shall be delivered within 7 calendar days from the date of receiving the comments of the Work group.

4. ISMS implementation

- Performing assignments through above mentioned functional requirements – The service provider is expected to fulfil all functional requirements in line with requirements and standards defined in the Cyber Security Policy and ISO/IEC 27001 and ISO/IEC 27002 standards, through documented procedures where necessary, plans and forms that relates to the ISMS.

- Defining the training program and providing ISMS training during the project – The service provider is obliged to define training program related to the information security in the LR and C institutions. Guidelines for definition of this program are given in the Cyber Security Policy in the Chapter 5. Development of awareness of information security competencies importance and improvement. Also, service provider should prepare training material and provide trainings within the ISMS implementation project:

- Basic training on development of awareness of information security which is intended to all employees and persons engaged by the LR and C institutions (approximately 900 employees). The goal of this training is to strengthen information security measures related to the human segment and to highlight human factor as a key factor in information protection. This training should contain basic concepts and definitions important for understanding of information security area, then policies whose requirements relates directly to employees and illustrative examples from practice related to the threats and possible information security incidents. The content of this training with mentioned topics and estimated deadlines are given in the Cyber Security Policy, Chapter 5 Development of awareness of information security competencies importance and improvement including topic suggestion and duration that is given in Table 1. Training content on the development of information security awareness. The education will be online with several appointments.

- Training intended for persons responsible for information security in each of the LR and C institutions (approximately 150 employees). This training should include the basic of the ISMS based on the ISO/IEC 27001 and ISO/IEC 27002 standards as well as key principles of data protection, then practical examples, technology implementation in data protection as well as definition of roles for cyber security experts in data protection and IT inf rastructure. The education will be online with several appointments.

Results of this phase are ISMS documentation that confirms that requirements and standards defined in the Policy are fulfilled, then training plan in the information security area as well as materials related to the basic trainings on the development on information security awareness and trainings intended to the persons responsible for information security in the LR and C institutions.

The Service provider shall submit a training program and training material not later than twelve weeks from the Contract signing. The Work group shall submit their comments within 7 calendar days. The updated training program and training material shall be delivered within 7 calendar days from the date of receiving the comments of the Work group. The service provider should complete all training within twenty weeks of signing the contract.

5. Adoption of the ISMS and further steps

- Implementation of the ISMS performance evaluation process – Service provider should define procedure of the ISMS evaluation process using the guidelines given in the Cyber Security Policy, in Chapter 6. Monitoring, measurement and internal audits of information security system as well as in the requirements of ISO/IEC 27001 standard.

- Implementation of the inconsistencies and corrective measures management process – The service provider is expected to define procedures for inconsistency and corrective measure management responding to the requirements defined in the Cyber Security Policy and ISO/IEC 27001 standard.

- Conducting internal auditors in relation to the requirements of the ISO/IEC 27001 and generating internal audit reports – The service provider is expected to perform one internal audit of ISMS together with the members of LR and C institutions team, with the aim to demonstrate how the internal audit process is performed. Also, the service provider is obliged to prepare report of internal audit with all necessary elements that report should contain in accordance with ISO/IEC 27001 standard. Among other, the report should contain inconsistencies identified during the audit process as well as recommended corrective measures for inconsistencies removal.

At the end of this phase, the service provider is expected to deliver procedure for assessment of ISMS performance, then procedure for inconsistencies and corrective measures management, as well as report on internal audit of ISMS. The Service provider shall submit the specified documentation from this phase within 23 weeks of signing the contract. The Work group shall submit their comments within 10 calendar days. The updated specified documentation shall be delivered within 10 calendar days from the date of receiving the comments of the Work group.

Procedures and instructions, as well as other documents that are integral part of ISMS project should be in accordance with actual legislation in FBiH.

Procedures and instruction that should be prepared during this project should fulfil requirements of the ISO/IEC 27001 and to be in line with guidelines of ISO/IEC 27002 standard.

All ISMS documentation (procedures, guidelines, plans, forms, etc.) that will be generated during this project should be in formats adopted by the LR and C institutions.

The service provider is encouraged to work in parallel on multiple related deliverables wherever possible and where it is not conditioned on results or prior deliverable approval.

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 ISMS implementation.

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:

- If necessary, provide access to facilities, databases, systems, and technological platforms to which ISMS implementation 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 ISMS implementation 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 ISMS Implementation objectives and expectations.

10. Clear Scope and Objectives:

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

11. Regular Communication:

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

By providing these resources, the contracting authority will aim empower the Service provider to implement ISMS 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 ISMS implementation.

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 implementation.

- 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 activity: trainings, delivered procedures and reports, potential difficulties encountered and the manner of overcoming them;

- The main body of the report, organized by type of training (basic and training for IT persons), and type od delivered procedure (procedure for assessment of ISMS performance and procedure for inconsistencies and corrective measures management) as well as the report on internal audit of ISMS. 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.

- It would be desirable for the Service Provider to have information security management system implementation projects in the last 2 years that include the provision of information security training and are of a similar scope and complexity.

- The service provider uses a methodology of ISMS implementation in accordance with the ISO/IEC 27001 and ISO/IEC 27002 standards.

- It would be desirable for the Service Provider to have at least one full-time employee or engaged professional with a valid ISO/IEC 27001 LA (Lead Auditor) certificate. In addition to this, the advantage is if the person has an EU GDPR certificate.

- 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 performance of this service in similar organizations.

- Other full-time employees or professionals engaged on the project should have at least 3 years of work experience in in the performance of this service 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.

- All information related to this service is strictly confidential information and can only be shared with the customer.

9.3 Selection criteria

The service provider should submit:

- Evidence demonstrating required professional qualifications, skills and experience as defined in Section 3.2;

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 successfully completed trainings, acceptance documented procedure for assessment of ISMS performance, then procedure for inconsistencies and corrective measures management, as well as report on internal audit of ISMS.

11. Ethical considerations

Ethical considerations are deemed crucial when a Service provider is implementing ISMS. 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 ISMS implementation, 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 ISMS implementation outcomes.

• Full Disclosure:

- Transparently communicate the scope, objectives, methodologies, and limitations of the ISMS implementation 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 ISMS implementation 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 in the contract.

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

• Feedback Incorporation:

- Engage stakeholders in providing feedback on the ISMS implementation preliminary findings and recommendations.

- Consider their feedback and adjust the ISMS implementation 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 ISMS implementation.

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 service provider 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 service provider 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

Attachment 1: Table 1 Training content on the development of information security awareness

Table 1 Training content on the development of information security awareness

Information security awareness training		
No.	Topic	Duration (min):
1	Basic terms and definitions	15
2	Information security management system - internal organization - roles and responsibilities - documentation structure	30
3	Cyber security policy - Acceptable use of information assets policy - Mobile device usage policy - Teleworking policy	60

	- Password management policy - Clear desk and clear screen policy - Incident management policy	
4	Contribution to the effectiveness of the management of the information security system of each role in the LR and C institutions Consequences of non-compliance with policies and non-compliance with the requirements of the information security system	30
5	Examples of information security threats and incidents that have occurred in the LR and C institutions or in the business environment/regionally/globally - Email phishing attack - Ransomware attack - Unsecure website Incident of unauthorized access to information from the outside or leakage of information from the inside	30
6	Link to documentation and materials related to information security Contacts and addresses of persons who have roles in the information security system in each of the LR and C institutions;	15
7	Examination	30
Participants: All employees in the LR and C institutions and relevant contractors		