**Council of Europe - Project on Preventing Money Laundering and Terrorist Financing in Serbia**

**(PMLTF-2022-IT-01)**

**Technical Specification for the Procurement of a Case Management System for Supporting
Police Business Processes Related to Combating Money-Laundering and Terrorism-Financing**

|  |  |
| --- | --- |
| PMLTF-2022-IT-01 | Date: February 2022 |

The Council of Europe is currently implementing a Project on Preventing Money Laundering and Terrorist Financing in Serbia. The Swedish International Development Cooperation Agency and the Council of Europe signed an agreement on the funding of the project “Preventing Money Laundering and Terrorist Financing in Serbia” in December 2019.

The project aims at supporting Serbia in addressing systemic deficiencies and difficulties to combatting money laundering and financing of terrorism (ML/FT) by focusing on specific segments of the prevention and enforcement system where such issues have been identified.

|  |  |  |
| --- | --- | --- |
|  |  | **Disclaimer:**The views and opinions presented in this document are those of the experts and should not be taken as to reflect the official position of the European Union and/or the Council of Europe. |

# Background

The Council of Europe is currently implementing a Project on Preventing Money Laundering and Terrorist Financing in Serbia. The Swedish International Development Cooperation Agency and the Council of Europe signed an agreement on the funding of the project “Preventing Money Laundering and Terrorist Financing in Serbia” in December 2019.The project aims at supporting Serbia in addressing systemic deficiencies and difficulties to combatting money laundering and financing of terrorism (ML/FT) by focusing on specific segments of the prevention and enforcement system where such issues have been identified.

The analysis (needs assessment) was conducted focused on Police’s existing IT capabilities to conduct financial investigations, whose main findings were:

1) Different Police units and departments have specific competences, duties and scopes of work, but they share several common business needs related to:

* Case registration, assignment and administration, including references to external institutions
* Registration/administration of persons and their roles in the case/investigation
* Task management with case docket – recording and reporting on conducted tasks and activities, sent and received documents with categorization and subcategorization
* On-click and batch generation of outgoing documents, from customizable templates
* Searchable repository of electronic documents and files (PDF, Word, Excel, photo/audio/video)
* Statistical and performance reporting, including custom (ad-hoc) reports

2) The only police unit which has a somewhat functional software application for the automatization of its business processes is the Unit for Financial Investigations (UFI) which uses 12-year old software application called eDocumentus. Existing data from the old application should be migrated to the new system in the largest extent technically possible.

3) All departments intensively collaborate or rely on the Criminal Analytics Service and the new software application must facilitate collaboration between the CAS and different departments.

## 1.1 Project description

The project “Preventing Money Laundering and Terrorist Financing in Serbia” aims at supporting Serbia in addressing the remaining Anti-Money Laundering/Countering Financing of Terrorism (AML/CFT) regulatory shortcomings thereby strengthening the country’s AML/CFT prevention and enforcement regime. This overall objective will be achieved by developing an effective and sustainable framework for preventing and suppressing money laundering and terrorist financing in Serbia, inclusive of primary and secondary legislation, organisational solution, and specialisation.

The project is funded by Sweden, represented by the Swedish International Development Cooperation Agency and implemented by the Council of Europe.

## Primary users of the future application and their roles in combating money-laundering and terrorism financing

Based on provisions of the Law on Police, Law on the organization and competence of state authorities in combating organized crime, terrorism and corruption, Regulation on principles for internal regulation of the Ministry of Interior, as well as on the Ministry of Interior’s internal organisational acts (Information bulletin) - conducting financial investigation and investigative actions related to the criminal offences of money laundering and terrorism financing falls under the jurisdiction of the **Service for Combating Organized Crime, Anti-Corruption Department and Counter-Terrorism Service**. Anti-corruption department and both Services are organizational units within Criminal Police Directorate.

More precisely, within the Service for Combating Organized Crime, conducting financial investigation and investigative actions related to the criminal offences of money laundering and terrorism financing are under the jurisdiction of the Unit for Financial Investigations and the Department for Combating Organized Financial Crime.

This organizational structure represents the current situation and it will be necessary to confirm it during the implementation of the project. More detailed information related to the organizational structure will be defined during the project implementation and final specification of workflows, in accordance with the organizational units’ competences, while ensuring the possibility of workflows adjustments in the event of changes in organizational structure, names of organizational units, normative framework, work processes, etc.

**Unit for Financial Investigations**

The Unit for Financial Investigations (UFI) conducts financial investigations and cooperates with competent organizational units of the MoI, judicial and other state bodies, organizations and agencies and institutions, legal entities and individuals (natural persons) in order to achieve financial investigations’ goals. It coordinates international cooperation in the scope of financial investigations.

The Unit for Financial Investigations has two departments:

* Department for conducting financial investigations of Organized Crime, and
* Department for conducting financial investigations in the regions.

The Department for conducting financial investigations of Organized Crime is responsible for the planning, implementation and realization of financial investigations of organized crime, as well as for finding and seizing property which is suspected to be acquired by criminal offences related to organized crime. The Department collects, prepares and uses data through automatic processing and sets specific requirements regarding the use of data. It cooperates with other state bodies and competent institutions, as well as with other organizational units of the MoI.

The Department for the implementation of financial investigations in the regions performs tasks related to financial investigations at the regional level.

The Department for conducting financial investigations in the regions has its units:

* Section for Planning and Coordination of Financial Investigations;
* Section for Financial Investigations in Belgrade;
* Sections for Financial Investigations in Niš (with units in Vranje, Leskovac, Pirot and Prokuplje), Kragujevac (Jagodina, Požarevac and Smederevo), Kraljevo (Kruševac and Novi Pazar), Šabac (Valjevo and Sremska Mitrovica), Užice (Čačak and Prijepolje) and Novi Sad (Sombor and Subotica).

The Section for Planning and Coordination of Financial Investigations performs financial investigations and cooperates with competent judicial authorities. The Section collects and analyses data and evidence about the property, legal income and living expenses of the defendant, as well as of the persons related to defendant. It identifies monetary transactions which aim is to transfer into legal cash flows money acquired by criminal activities, as well as persons participating in those transactions. It cooperates and jointly works with other ministries, state bodies and organizations and security services in conducting financial investigations.

**Department for Combating Organized Financial Crime**

The Department for Combating Organized Financial Crime is responsible for preventing, detecting, and suppressing all forms of organized financial crime in the territory of the Republic of Serbia, as well as for cooperation and joint work with other ministries, other state bodies and organizations in the Republic of Serbia in the fight against all forms of organized financial crime. It organizes and participates in international and national police actions to suppress all forms of organized financial crime.

**The Department for Combating Organized Financial Crime is consisted of:**

* Section for Combating Money Laundering;
* Section for Combating Forgery of Money and Other Means of Payment and
* Section for Combating high corruption.

The Section for Combating Money Laundering works on prevention, detection and suppression of money laundering. It detects, monitors and analyses the state and movement of financial flows during which the money acquired by performing illegal activities is deposited, its stratification, as well as its integration into legal cash flows. The Section prepares plans, information and reports on the state of crime in the area of money laundering. The Sector cooperates and performs joint operational work with other ministries, as well as with other bodies and organizations in the Republic of Serbia on the tasks of detecting, preventing and suppressing money laundering.

The Anti-corruption Department prevents, detects and suppress corruption in the territory of the Republic of Serbia, as well as coordinates work on the tasks of detecting criminal offenses in this area. Also, it cooperates and jointly works with other ministries, other bodies and organizations in the Republic of Serbia on the tasks of detecting, preventing and suppressing all forms of corruption. It plans, organizes and participates in international and national police actions to combat corruption.

**The Counter-Terrorism Service is consisted of:**

* Department for Prevention and Combating Terrorism;
* Department for Prevention and Combating Extremism;
* Sections in Belgrade, Vranje, Novi Sad and in Novi Pazar.

The Department for Prevention and Combating Terrorism is responsible for preventive action and solving of the crime of terrorism and other criminal offenses related to it.

The Department for Prevention and Combating Terrorism is consisted of:

* Section for Prevention and Combating Terrorism;
* Section for Prevention of Misuse of Public Resources and the Internet and
* Section for International Exchange of Intelligence-Operational Data.

The Section for the Prevention and Combating of Terrorism performs tasks of planning, organizing and coordinating work related to the monitoring of all security-interesting phenomena and events on the territory of the Republic of Serbia and the territories of other countries. The Section collects operational and intelligence information regarding persons, groups and organizations whose actions are or can be linked to terrorism, with the aim of preventing the execution of terrorist actions in the Republic of Serbia or preventing the use of the territory of the Republic of Serbia for the preparation or execution of such actions in other countries. The Sector undertakes actions aiming at preventing terrorism and detecting early radicalization and its suppression.

It creates a collaborative network for collection of information to prevent and solve the crime of terrorism and related crimes. It cooperates with the organizational units of the Ministry, the security services, as well as with other competent state bodies with the aim of exchanging operational-intelligence data and information for joint engagement in preventing, detecting and solving the crime of terrorism and related crimes. It cooperates with competent institutions in order to gather information and relevant evidence regarding financial transactions and other activities that can be used for the purpose of terrorism. It cooperates with persons and institutions responsible for the protection of critical infrastructure, as well as for preventing the misuse of chemical, radiological, biological and nuclear material for the purpose of terrorism.

Activities of all above mentioned units (services and departments) which are conducting financial investigations and combating money laundering and terrorism are supported by Criminal Analytics Service. This is also organisational unit within Criminal Police Directorate. The Criminal Analytics Service gathers all information collected in financial investigations (so called operational material), analyses them in every needed aspect and makes raw data usable for further actions.

The Criminal Analytics Service performs criminal analysis on data from ongoing cases and monitors and reviews police measures and actions. It collects and systematizes operational material, to manage and make decisions on the engagement of police officers. It applies analytical tools and software for data analysis for discovering the perpetrators of criminal acts, as well as for securing traces of the criminal act and objects that can serve as evidence.

Based on the established system for criminal analysis, it performs work coordination and information exchange at the level of the criminal police and with other security services. The Service monitors the work of operational teams, in order to improve the work processes and reduce the risk of overlapping investigations. It collects, systematizes, and analyses information in order to prepare a Serious and Organized Crime Threat Assessment.

The Criminal Analytics Service is consisted of:

* Department for criminal-operational and strategic analysis;
* Department for Work Coordination and Data Exchange and
* Department for development and administration of special purpose systems and networks.

## 1.2 Goals of this procurement

Based on the conducted analysis, different user needs were identified. The identified needs are divided into specific chapters, as described later in this document. This assessment represents a comprehensive list of user needs, i.e. it defines the specification of the required functionalities of a software solution for case management, the implementation of which would lead to a rounded and complete IT support system for the main lines of work within the MoI, related to financial investigation processes.

**General requirements:**

* Centralized web-based architecture, with the focus on high security and high availability
* Automated, centralized backup of all user data
* Role-based, hierarchical access privileges
* Intuitive and efficient user interface
* Strict audit log (capturing details of all user activities within the application)
* Sustainable total costs of ownership

**High-level functional requirements:**

* Case registration and administration, including references with external institutions
* Registration and administration of persons and their roles in the case/investigation
* Repository of identified assets and properties (by category, type and economic value) owned by the investigated person or other connected persons (spouse, children, relatives, business partners…) that may be linked with money-laundering activities.
* Task management (planning and recording conducted activities in the case)
* Robotized tasks (default execution of standard activities for each newly created case)
* Calendar management (task/event scheduling, alerts for upcoming events and deadlines) to support the organization of work in accordance with deadlines and available resources
* Case docket - chronological overview of conducted activities, sent and received documents
* On-click generation of standard outgoing documents, from customizable templates
* Interoperability (electronic data exchange) with internal and external information systems
* Searchable electronic repository of files with OCR support, including documents, spreadsheets, images, audio and video recordings
* Pre-processing and transformation of raw financial transaction spreadsheets into single common format, for further criminal analytics
* Ability to produce statistical and performance reporting, including custom reports

This project will finance the development of all the required functionalities of the future system, and in the rest of the document the required functionalities are grouped by importance/priorities of implementation for the user.

## 1.3 Expected deliverables of the project:

For the successful implementation of this phase of the project, the following services must be performed:

* Development of an intuitive and fully functional application to support the Anti Money Laundering and Counter Terrorism Financing activities, in accordance with the requirements specified in this document.
* Created user profiles/roles for all types of users, in accordance with their workplace and job description characteristics.
* Migration of existing cases from the eDokumentus system used by Financial Investigation Unit
* Provision of training for all users and roles
* Delivery of user manuals for the use and administration of the application (PDF versions)
* Warranty period of 12 (twelve) months

## 1.4 Required vendor qualifications

Lot 1

* The company/legal entity must be registered in a member state of the Council of Europe;
* Experiences in designing and implementing information systems in public administration or judiciary;
* At least 3 references for successful implementation of relevant projects in previous 5 years;
* The supplier must have procedures and rules to guarantee the quality of project management and the confidential information that it will possess during the implementation of the project. To meet this requirement, the supplier must be certified for the ISO 9001 and 27001 quality management system.
* At least 5 full-time experts or experts hired on the basis of a long-term cooperation agreement:
* At least one employee with an expert level of knowledge to install and configure the platform on which the offered software solution would work. Official certification, e.g. MCSE/MCSA, Red Hat RHCSA/RCSE, etc. will have priority in the evaluation.
* At least one architect/expert for the data warehouses. Official certification will be considered an advantage in the evaluation process.
* At least 3 full-time senior developers
* At least one senior database administrator for the offered solution (Microsoft, Oracle, IBM, etc.). Official certification will be considered an advantage in the bid evaluation process.
* At least one project management professional with a PMP, Prince or similar certification.
* At least one software testing (QA) expert.

Lot 2

• At least three years of experience in the provision of similar services

• Proper fulfilment of minimum three similar orders on delivering, installing, configuring IT systems during the last three years

• Minimum annual average turnover of EUR 80,000 (or equivalent in other currency) during the last three years (2020, 2021, 2022)

• License on the original equipment manufacturing and proposed solutions, or an authorisation that the tenderer is a dealer/partner/reseller of the proposed solution in Serbia, including the authority to sell, upgrade, supply, service and maintain the proposed solution.

## 1.5 Implementation timeline

**Lot 1:** The required application should be developed in maximum 10 months (305 calendar days days), and the following phases are envisaged:

* Clarification and refinement of functional requirements in cooperation with end-users (by the end of the 1st month of the project at the latest)
* Installation of the development and test environment on the bidder's equipment (end of the 1st month of the project at the latest)
* Iterative development of the application, using agile project methodology, with continuous integration and testing (from the 2nd to the 8th month of the project)
* Installation of the production environment on the server infrastructure of the Ministry of Interior (end of the 9th month of the project at the latest)
* Necessary configurations in the application in accordance with user needs and user roles (end of the 9th month of the project at the latest)
* Training of all types of users and administrators (during the 10th month of the project)
* Putting the software solution into production use (end of the 10th month of the project at the latest)

**Lot 2:** The required hardware should be delivered and installed in the following order:

* Delivery and installation of desktops latest by the end of the 3rd month of the project
* Delivery and installation of scanners latest by the end of the 6th month of the project

# Technical specification for procuremenet of a case management system for AML/CFT

## 2.1 Users Roles

The application needs to have a developed flexible roles administrative management, in the context of defining the level of privileges for certain roles in the application, including but not limited to the following:

a. Administrative clerk (administrative staff performing scanning and uploading of documents (received and sent) in the application, registering a new case that has yet to be assigned to specific Police Officer by the head of organizational unit.

b. Police Officer (officers who manage new investigation cases. The Police Officers act as case owners but as well they can be assigned a role of case contributors in others cases with different level of access.

c. Head of organizational unit (organizational units within the Police, that are responsible for supervising the performance in all cases that are being processed with that organizational unit), can assign cases to subordinate Police Officers, monitor and observe all cases and operatives under their command, setting deadlines for completing tasks, generating reports, acting upon individual cases, communicating with other organizational units within the Police.

d. Administrator (who has the role of administering users, opening new users accounts, changing passwords, removing users, changing rights, adding characteristics to categories of users, adding, modifying or removing the organizational units within the Department etc.)

Fine-grained customization of user roles (adding or removing specific privileges) in accordance with their roles in the work processes must be possible at the administrative level, without the need to engage a programmer.

## 2.4 Introductory remarks related to case management application

Police investigation cases in the future application will be assigned to specific Police Officers and in a logical sense Police Officers are considered the "owners" of the cases.

The case is initially formed in the application with a set of basic data and at the moment of creation it is still not assigned to anyone. The head of the department/unit/service should then be able to assign the newly formed case to work to the desired police agent. The application should also provide for the possibility of random assignment, i.e. to suggest the next random agent who, according to the number of cases in the work, should receive the next case, but the manager must retain the possibility to make the final decision to which Police Officer a case will be assigned.

A user with appropriate privileges (manager/head of the organizational unit) must also be able to delegate (transfer) an existing case initiall assigned to a specific Police Officer to a different Police Officer, if the existing owner of the case is on sick leave, is on vacation, retired, no longer in service for any other reason, etc.

**Contents of the case**

The case owner (the Police Officer in charge) must be able to enter, classify and update natural and legal persons, criminal offenses, upload incoming and outgoing documents and designate their senders/recipients, upload electronic evidence (photos, videos, sound recordings, etc.), register properties, activities in case, plan and schedule tasks and events etc.

The application must have the ability to create references between related cases, to merge or split investigative cases, while retaining all previously registered data and activities on the cases being merged/separated.

**Case contributors**

In most use scenarios the case will be processed by Police Officer assigned with the case. But in some scenarios (i.e. complex cases) the application should allow the Police Officers to assign contributor role to other users. The Case Contributor should be allowed to have limited access over the case information and the system must create the possibility for the case owner to assign different level of access in different level of objects for the case contributor. The system should allow the users to update the case data/information, to attach to the case all type formats of communication that they have about the case (documents, data, etc), to link different cases that can be related, cases and as well to keep all time parameters of the case processing.

**Calendaring function with alarms**

An important aspect of the functionality of the future system should be warnings on incoming deadlines (e.g. dates by which, for example, a response to the request should arrive, some action should be completed, etc.)

The application must enable managers to have daily insight into the statuses of all cases assigned to Police Officers under their jurisdiction, as well as provide mechanisms for direct communication with the operative working on the case, through the application itself.

Tasks and activities in the case can also have deadlines for being completed. Similarly, requests for information sent to external institutions will have deadlines for registering received responses, or warning/alarm would be triggered to notify the operative of missed deadlines.

Before the expiration of the task completion deadline, or document reception deadline, the Police Officer should be automatically notified by the application that the deadline for completing the case is close/approaching. If the task is not completed, or document received, and the deadline has expired, a notification should be automatically sent to the acting officer, **and** his superior/manager (head of the organizational unit).

**Case related Communication**

During their daily work, Police Officers will communicate internally with their colleagues and contributors/assistants on case.

In addition, the application must allow managers/superiors to overview the progress of cases within their jurisdiction and to provide a communication mechanism (i.e. mechanisms to exchange messages) with their subordinate operatives directly through the application user interface, with written trail remaining in the case history.

It should be noted that the term “message” refers to a structure comprised of:

1. Title/subject of the message
2. Reference to case number
3. Recipient
4. Urgency level (low priority, normal priority, high priority)
5. Confidentiality level
6. Due date (deadline) for response (optional)
7. Date/Time of sending
8. Text of the message (body)
9. One or more attachments

The Text of the message should support basic set of rich-tech editing features.

The Vendor is encouraged to envisage as simple as possible messaging mechanism that fulfills the intended purpose of the internal messaging system, and not to develop “over-engineered” concept of messaging.

**Case Archival**

At the end the investigation process and usual case processing “lifetime”, the application should allow users to finalize the case, and to archive the case data with due respect to laws and bylaws of the Republic of Serbina regulating archival od documents and personal data protection.

This is particularly important for cases where no links to money laundering activities were found while investigating a person and his/her relatives, but significant amount of personal data was collected during the investigation.

# Functional Requirements for the Application

## 3.1. Functional Requirements

Functional requirements have been grouped into the general and specific requirements. The tables show the general functional requirements for the **Case Management System** (hereinafter **System**), and the specific or special system requirements. **All the requirements in this document are mandatory – there are no optional requirements.**

The Bidder shall commit to every function/requirement in the given tables of this document and enclose the completed tables in their Bid. In the column „Bidder response“ the Bidder must state how the function/requirement will be met, by using the following marking system:

|  |  |
| --- | --- |
| **Bidder response** | **Description of how the requirements shall be met** |
| A | Exists as a function and is already implemented with at least one client – may be presented on the client’s premises  |
| B | Exists as a function, but not implemented with any client – may be presented on the Bidder’s premises  |
| C | Function requires little modification of the existing similar function, and will be realized in a set time limit  |
| D | The function will be developed. |
| E | The function cannot be developed by the bidder |

All the functions in this document are required, and all responses marked by the Bidder with A, B, C and D are the subjects of delivery and the Bidder must deliver these within the bid-price.

The Bidder must enclose a description of the bid software solution, and other relevant accompanying documentation that describes how the bid solution will be developed/customized and implemented.

The software solution should be a web application with responsive user interfaces, which is supported by desktop, mobile and tablets.

## 3.2 Software architecture and 3rd party licenses

The software solution is expected to be functionally expanded in the future, and to offer to its users extended access to new features and new data over time. Therefore, the architecture of the system must support such scenarios from the first day. Additionally, the software solution should enable interoperability with other systems, by providing web services APIs.

**Network Topology**. The system should be able to work in intranet of the MOI/Police, while end users will access it through secure connectivity from their desktop and laptop computers using any HTML5 compliant web browser. The application must not require any kind of browser plugins to work properly.

The software should put no limits to the number of documents and records that can be archived and indexed, which should be limited only by hardware and storage size.

Software licenses for databases, applications development and other third party licenses that are needed for the System development/implementation and work should be provided by the contractor as part of system development.

## **3.3 General Requirements**

The development of the software solution shall be guided by the modular principle , to allow for further expansion and additions of new functions or improvements in the future.

The software solution must be as simple to use as possible and user-friendly, and its functionalities shall be ergonomic and have a logical and consistent user interface across the entire application.

The language of the user interface is Serbian (both Cyrillic and Latin scripts must be supported).

The application must be developed using iterative project methodology. Continuous integration and continuous deployment (CI/CD) approach is highly desirable.

## **3.4 Security and Data Integrity**

Potential vendor must keep in mind that the future application is going to store the information with limited access data and classified data. The software architecture and design considerations of the application must respect that fact by applying the following principles:

1. Software development using proven and secure software libraries and components, as well as strict validation of input data on both the client and server side
2. Following secure coding practices to prevent common security vulnerabilities, such as buffer overflows, injection attacks, and cross-site scripting.
3. Strict encryption of data in transit (HTTPS protocol), and in the case of particularly sensitive data such as passwords, etc. - encryption on disk/storage.
4. Limiting access to certain system functionalities and certain data, based on roles and/or workplace. For example, a user with the role "head of department" in Čačak must not be able to see cases and case details that are under the authority of the head of department in Kraljevo.
5. Preventing unauthorized access to the application at the network level (Firewall)
6. With the aim of ensuring business continuity, regularly backing up data, replicating data to multiple geographically distant locations, and having a well documented and tested disaster recovery plan in place.
7. Regularly updating and patch the software components to address known vulnerabilities and prevent potential attacks and security exploits
8. Monitoring system activity and recording activities in the system audit log.

Above listed are just a few illustrative safety measures that the vendor is expected to take. The vendor can and should implement all other mechanisms that can help ensure maximum security and safety of the application and data.

The software solution should consistently log users activity into the system audit log, so that there would be a possibility to determine who did what and when from the first opening the case to the last information entered into the system.

A specific system auditor role should be implemented to prevent unauthorized data alteration and manipulations. The detailed system security/audit log file should be prevented from deletion and accessible only where a privileged Police official and the Auditor person enter both their passwords.

This should prevent the log files from being manipulated or altered by a single person.

## 3.5 Operating environment

The Ministry of Interior/Police will provide the necessary hardware and networking infrastructure where the production version of the application would be hosted.

The following server infrastructure will be provided by Ministry of Interior/Police for installing the future application (the Police uses VMWare virtualization infrastructure).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Quantity** | **RAM** | **CPU** | **DISK** |
| App | 2 | Minimum: 32 GBPreferred: 64 GB | Minimum: 4 core @ 2.2 GHzPreferred: 8 core @ 2.2 GHz | Minimum: 2x300GBPreferred: 2x500GB |
| DB | 2 | Minimum: 32 GBPreferred: 64 GB | Minimum: 4 core @ 2.2 GHz Preferred: 8 core @ 2.2 GHz | Minimum: 2x300GB for OS + 2x1TB for the content Preferred: 2x500GB for OS + 2x2TB for the content |

# Training of all users and roles to work with the application

The vendor must deliver comprehensive trainings to all users, by defining and providing:

* User Roles: Identify the different user roles and their corresponding training needs. For example, administrator, or document scanning clerk will require different training than a Police Officer.
* Training Materials: Develop comprehensive training materials, including written documentation, video tutorials (if possible), and interactive training modules that address the specific needs of each user role.
* Training Environment: Create a training/testing environment that mirrors the live production environment, allowing users to practice using the application without fear of making errors.
* Learning objectives: Define clear learning objectives that specify what users will be able to do with the application after completing training.
* Training Schedule: Establish a training schedule that takes into account the availability and schedules of the users and trainers.
* Technical support: Ensure that users have access to technical support and resources to help them troubleshoot issues and answer questions about the application, at least during the first 12 (twelve) months of the application use (minimum warranty period).
* Training related to functioning of the software solution within the infrastructure the Ministry of the Interior.

The total number of trainees is expected not to exceed 100.

# Client-side hardware and software configuration

If the proposed solution is based on the Microsoft products, application users are licensed to access Microsoft environments as part of global agreement of the Government of Serbia with Microsoft, under the Microsoft Enterprise agreement framework.

If the proposed solution is not based on Microsoft technologies, the bidder must provide the relevant licenses for each user that will access the software application (e.g. Oracle. IBM etc.).

Typical workstations that will be used to access the software solution will need to have the following minimum configuration:

* Operating system Microsoft Windows 10;
* CPU Intel 8th generation or newer
* 8GB RAM
* 500GB hard drive (or SSD)
* Web browser Microsoft Edge 112, Google Chrome 112 or Mozilla Firefox 112

All the potential additional costs stemming from the need to order additional hardware and software components must be included in the bidding price.

The Bidder must adjust their application solution to the abovementioned resources provided by Ministry of Interior/Police, in order to ensure the **normal** functioning of the application and database.

Normal functioning, i.e. acceptable performances, is defined as response time of application not longer than 3 seconds when entering, modifying, viewing and deleting data, and the response time of application not longer than 10 seconds for generating summarized and periodical reports, except for custom (ad-hoc) reports where response time can be maximum 30 seconds.

# Project implementation and realization

The period of project implementation and realization must not be longer than 365 calendar days, excluding the warranty period.

The Bidder shall give details of their suggested methodology of implementation, as well as the most detailed plan of project realization possible with all its relevant activities, performers of activities, deadlines, and potential bottlenecks and key points. It is expected that the Supplier offers a plan of the implementation realization of the software solution in phases:

* Inception report;
* Limited Business Analysis phase – to clarify requirements;
* Joint design of the software application, with the emphasis on the user interface design and concepts
* Iterative software development with continuous integration and continuous deployment (CI/CD), automated testing, and monitoring. Vendor is encouraged to utilize popular DevOps platforms such as GitLab, Atlassian, Jenkins, Microsoft Azure DevOps or similar platforms.
* Implementation of testing/training environment (“application playground for users”)
* Testing of software solution in close collaboration with end-users with various roles;
* Producing the technical blueprints, project documentation and user manuals;
* Training of administrators and system users;
* Establishment of production environment;
* Production (roll-out).
* Twelve-month warranty period/technical support (further support would involve maintenance contract).

The Bidder shall also compile a list of potential risks that can jeopardize the project realization, as well as suggestions for their minimization/elimination.

In establishing the system environment and necessary infrastructure, Ministry of Interior/Police’s ICT service will play a significant role. Procedures for setting up/installing the system and restoring functionality in the event of a disaster must be documented in detail, so that the IT administrator of the Ministry of Internal Affairs of the Republic of Serbia can carry out a complete installation and restore simply by following the technical documentation.

# Verification/Acceptance

Verifying the success of the completed phases of implementation and testing of the software solution shall be carried out by a professional commission consisting of a Supplier's consultant, and a person to be appointed by Ministry of Interior/Police and the Ordering Party (Council of Europe).

The exact list of team members that will monitor the implementation of the software application, manner of testing and reporting will be agreed during the project implementation and specified in the project inception report.

The elements of delivery which the Bidder must complete are:

* Software solution which meets all the agreed functional requirements
* Training of internal users
* Deployment of a testing/training environment on vendor’s own infrastructure
* Launching the new solution into production
* Production work of the new solution with good, acceptable performances
* Project and user documentation and instructions

The software solution that fulfils all the agreed functional requirements on the required software application will be verified as follows: the Supplier will carry out a presentation in a testing environment to the relevant representatives of the beneficiary (Police), representatives of the Council of Europe, and their advisors where they will directly see and confirm that all agreed functionality and content, has been executed and completed by the Supplier. A written protocol shall be made, serving as proof of the completion of the contractual obligations by the Vendor.

**7.1 Training verification**

For the training verification it is necessary that the Bidder:

* Develops the training program based on the requirements listed in this Technical specification,
* Completes the training of all the course trainees,
* Devises tests for the trainees which all the trainees must pass,
* Performs the testing of staff (in the conditions which the Ordering Party must establish), supervised by the authorized representatives of the Ministry of Interior of the Republic of Serbia.

**Training** isverified when all the requested trainings are completed and the testing of all the Police Officers and administrative staff is carried out. The obligatory condition is that all the staff pass the test with a minimum of 75% of completed tasks predefined by the minimum percentage of solved tasks. The minimal percentage of solved tasks is defined by the project coordinator from Ministry of Interior/Police, in collaboration with CoE. A written protocol will be made, serving as proof of the completion of contractual obligations by the Supplier.

**7.2 Verification of launching the solution into production work**

Verification of launching the new solution into production work is ascertained by performing Functional Testing and User Acceptance Testing (UAT). A written protocol will be made and it will be used as proof of the completion of contractual obligations by the Supplier.

The verification of the production work of the new solution with good, i.e. acceptable performances is ascertained by measuring the response of the application solution on an application sample chosen by the Ordering Party (Performance and Stress Testing). The measuring of the response will be performed in production conditions and in the period chosen by the Ordering party and in the presence of the Supplier and CoE representative. The measuring of the application solution response will also be performed in the intranet of the Ministry of Interior, at a minimal throughput of 40 Мbps, at a given workstation. A written protocol shall be made thereof, serving as proof of the completion of the Supplier’s contractual obligations.

The Vendor must submit a proposal for Functional acceptance tests for each phase.

The format of the Functional acceptance tests should be as follows:

|  |  |
| --- | --- |
| Number of the test: |  |
| Name of the test: |  |
| Relation to the Functional requests for the phase: |  |
| Steps in conducting the test: |  |
| Expected results: |  |
|  |  |

**7.3 Project documentation**

All the project and user documentation must be in **the Serbian language**

Project documentation shall include:

* Application architecture and logic data model;
* Physical data model, i.e. a complete database scheme (which includes all the objects in the database and data dictionary – purpose and meaning of all fields in all tables);
* Functional model of the software solution, with a description of each function;
* Model of roles, as a method of controlling data access;
* As-built design, which includes:
	+ A description of the requested system environment and its establishment/configuration,
	+ A detailed description of the necessary configuration of the host operating systems and software application installation procedure,
	+ A description and detailed specification of all the necessary and performed system settings for the software solution to function efficiently in the production regime, which includes but is not limited to:
		- all the settings on the “client” application side,
		- all the settings of the client operating system
		- all the settings of the server operating systems,
		- all the settings of the web environment,
		- all the settings of the ancillary software (OCR library, antivirus used by the Ministry of Interior etc.),
		- all the settings within the application system,
		- all the settings in the database.

**7.4 User documentation**

User documentation shall include:

* General instructions for using the application, i.e. user interface;
* User instructions (manual) for each of the installed and used modules, i.e. functions;
* „Оn-line help“ (in HTML) which is accessed directly when working with the application.

Verification of project and user documentation and instructions is ascertained by the delivery/availability of their electronic versions (Word, HTML and/orPDFfiles), as well as by the accessibility/availability of on-line help with the appropriate content during application use. A written protocol will be made thereof, which will serve as proof of the completion of the Supplier’s contractual obligations.

## Vendor’s obligations

## The contractor is obliged to:

* Deploy the executable versions of the Software Application, on the server equipment which is the property of the Ministry of Interior/Police in their designated premises.
* Thoroughly test Software, including, but not limited to, all of its subsequent releases/editions, subsequent upgrades, enhancements and subsequent versions. This must be documented in written form and it should include detailed description of tests, the manner of conducting tests, test results and List of program errors and important issues. Plans for testing must be reviewed by Ministry of Interior/Police to ensure that quality standards are maintained.
* Transfer its entire right, title, and interest in anything created or developed under this Contract including all patents, copyrights, trade secrets, and other proprietary rights.
* Execute and aid in the preparation of any papers necessary or helpful to obtain or maintain any patents, copyrights, trade secrets, and other proprietary rights under this Contract.
* Handover the source code for an unlimited use without copyright restriction and Installation of development and testing environment to Ministry of Interior/Police on optical medium or USB drive. The Source Code will be ownership of Ministry of Interior/Police of the Republic of Serbia.
* Vendor’s obligation is to submit a proposal for Functional acceptance tests for each phase.

In other words, the obligation of the Vendor is to perform complete installation, configuration, migration, integration and comprehensive implementation of the system-technological and application solution, from the level of installation and configuration of server-side operating systems, databases, application servers, ending with the installation of the application in production work, including the implementation of protection solutions from the loss of data (backup) and services, as well as the creation of detailed technical documentation which documents all the above-mentioned steps. All the above should be included in both the initial warranty and subsequent maintenance contract.

In addition, the supplier's obligation is to define and establish the set level of availability of the solution (99%) as a whole and the supplier's guarenteed response time when solving problems and implementing additional requirements, which are not found in this document).

The obligation of the Vendor is to guarantee that none part of the Software or documentation, covered by this Contract, shall contain the protection feature designed to prevent the use of the Software. This includes, but not limited to, any computer virus, worm, software lock, drop dead device, Trojan-horse program, trap door, time bomb or any other code or instruction that can be used for assessing, modifying, deleting, damaging or disabling the User Software or computer system. The Vendor is obliged to give the Source Code Application in ownership to the Ministry of Interior of the Republic of Serbia

 The Vendor shall compensate and enable integrity to the Ministry of Interior/Police from complaints or activities of any or all third parties, including losses, expenses, responsibilities, real compensations for a lawyer and other expenses that may occur form such complaints and activities, where the reason is that the Software infringes or violates the copyright, brand, patent or business secret of a third party, on the condition that:

- Ministry of Interior/Police immediately informs the Vendor in written on any complaints;

- The Vendor has a sole role of defending from any such complaint and all to carry out all the negotiations for reaching an agreement or compromise;

- Ministry of Interior/Police shall ensure reasonable cooperation with the Vendor.

In any activity based on the complaint for violation, the Vendor has, at his own expense, (i) obtain for the Ministry of Interior/Police the right to continue using the Software, or (ii) replace or modify the Software with the Software that does not cause violations but it ensures the same functionality.

# Warranty and system maintenance

The Bidder must include in the price the maintenance of the Application and the equipment, with a warranty period of at least 12 months, which will secure the normal operation of the application and database. The warranty period of the application begins with the date of acquisition (delivery and acceptance) of the information system. The warranty period for the hardware begins with the date of acquisition (delivery and acceptance) of the hardware.

**Note: Bids with a warranty period shorter than 12 months will not be accepted.**

As security for enabling the normal functioning of the software solution within the warranty period, the preferred Bidder must secure a single promissory note registered with their parent bank and a letter of authorization for the amount of 50% of the total worth of the contract.

If the Bidder fails to meet their obligations and deadlines stipulated in the technical specification, the Ordering Party has the right to activate the promissory note submitted as a guarantee of the completion of their obligations within the guaranteed period.

The Bidder must specify the price for the annual maintenance of the offered solution for every year following the offered warranty period, for 5 years.

Upon the completion of the project, the Bidder is expected to continue to perform the following:

1. After receiving a written notification from the Client regarding the irregular functioning of the software solution, they must identify the problem, fix the problem/make an intervention so the programs can function correctly, or recommend how the problems can be overcome.
2. All the irregularities in the functioning of the software that impact Ministry of Interior/Police's capacity to use the software solution productively must be resolved within 2 working days; more serious irregularities must be resolved within 5 working days.
3. The Bidder must expand or enhance the software solution, as requested by the Client and which are the subject of this procurement, which includes alterations of the existing and the creation of new reports, minor changes in the data entry application, modifications and viewing, and change in the data access policy, with no additional charge. "Minor changes" are defined as engaging the supplier up to 2 days per month.
4. To expand and enhance their solution at the Client's request (major intervention) which are the subject of this public procurement, and to create/modify the user documentation and to offer training to all the relevant users, with additional payment.

To perform additional training of users (whether new or current) regarding issues and areas which are specified and particularly requested by the Ordering Party, with additional payment.

**Annex 1 – Functional, performance and security requirements – Lot 1**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | **Function**  | **Description**  | Priority1 - High2 - Med.3 - Low | **Bidder response** |
| **MAIN PURPOSE OF THE APPLICATION AND GENERAL REMARKS** |
|  | **The intended purpose of the software solution** | The future software solution will be a centralized, web (cloud) based application used for opening, registering and managing cases related to investigation of money laundering crimes and terrorism financing. Each functional-organizational police unit that will use the application must maintain separate data and configuration (codebooks, internal systematization, list of users, reports and sections/statistics), due to the security and privacy of data within lines of work of each Police organizational unit within the scope of the project.In that regard, the software solution should be considered as multi-tenant software application with some slightly specific functionalities for different MOI/Police organizational entities, such as Financial Investigation Unit.The application user interface and its functionalities should be ergonomic and should implement easy to use, logical, intuitive and consistent UI concepts. | 1 |  |
|  | **Primary users of the application** | The following organizational entities of the Police were identified as the primary users of the future application:* Unit for Financial Investigations
* Counter-Terrorism Service
* Service for Combating Organized Crime
* Department for Combating Corruption
* Criminal Analytics Service
 | 1 |  |
|  | **Special role of the Criminal Analytics Service** | The Criminal Analytics Service (CAS) should have horizontal access to all lines of work, in the sense that it can communicate and exchange documents and other electronic content with all organizational units through the application, and additionally have an independent document repository, available only to the Criminal Analytics Service. | 1 |  |
|  | **Levels of hierarchy** | The access rights in the application should be such that Police Officers in charge of the case may see only their cases, with the possibility of granting access rights to the specific case (exclusively in "read-only" mode) to a colleague or assistant.The head of a hierarchically superior organizational unit has insight into all subjects of all organizational units below him, in accordance with the internal organization of the Ministry of the Interior, which is organized hierarchically according to the existing normative framework, as follows* + - Directorate (“Uprava”)
		- Service (“Služba)
		- Unit (“Jedinica”)
		- Department (“Odeljenje”)
		- Section (“Odsek”)
 | 1 |  |
|  | **Automation of repetitive, standard activities in case** | The aim of the future application should be to eliminate or greatly reduce repetitive and manual activities, such as drafting of output documents, requests for information, notices and contacting external registers and data sources, generating periodic reports etc. The application should incoroporate automated and semi-automated and background processes that include:* Generation of stadard/templated requests for information that are sent to external institutions for each newly opened case, or person who is subject of the investigation.
* Automatic download of information from several external registers based on the suspect's unique personal number (JMBG), license plate number, etc.
* Automatic setting of deadlines for completion of standard tasks, or for reception of responses to requests for information from external institutions
* Automatic background checking if the deadline has passed for receiving the response to the request for information, finalization of the task etc. and sending automatic reminders and alerts to the users if deadline passed
* Automation of backup procedures/scripts
* Bulk execution of other actions that are routine, repetitive, always conducted in the same way, etc.
 | 2 |  |
|  | **Batch-generation of standard documents** | Different lines of work have different needs for generating requests for information, letters and notices to external institutions, but they all have in common that certain repetitive documents are generated in each case and require a lot of manual activities from the Police Officer to prepare.The future application should enable the Police Officers to generate a whole set of standard requests for the delivery of information and other correspondence (output documents) for the selected person who is the subject of the investigation. The batch-generation of these documents should be done on the basis of templates in which information from the case (e.g. name, JMBG etc.) are inserted in the provided places in the text, with possible minor manual corrections of the text.Through the administrative part, it must be possible for users to change or adjust templates, without the need to engage a programmer. | 1 |  |
|  | **Data visualisations** | The application has to enable the visualisation of data through charts and generating reports that would play a great role in improving the functioning of the Financial Investigation Unit. The graphical representation of data would enable the top-management to have clearer overview of all cases, persons, assets and documents that were investigated in the reporting period. | 2 |  |
|  | **Production and testing environments** | The vendor should set up development/testing/training instance on its own infrastructure, throughout the entire development process.The production instance will be hosted on the Police virtual infrastructure. | 1 |  |
| **GENERAL REQUIREMENTS** |
|  | **Compatibility with major browsers** | The website must look and feel the same in the following HTML5 web browsers:a) Microsoft Edge v112 and newerb) Google Chrome v112 and newerc) Mozilla Firefox v112and newerd) Apple Safari 14 and newer**The support for legacy Microsoft Internet Explorer is not needed.** | 1 |  |
|  | **Automatic backup procedures** | The vendor must implement both automatic and manual backup mechanisms, daily, weekly, monthly and full backup of entire application content, including archive of documents.Backup and restore procedures have to me automated and documented so that a reasonably skilled IT person can independently perform both data backup and restore. | 1 |  |
|  | **Availability** | The application must be available 99% of time, except for pre-announced down-times required for maintenance, backup, or planned system upgrades.The vendor must announce requests for shutting down the application at least 2 (two) days in advance and with written consent of the beneficiary. | 1 |  |
|  | **Basic rich-text editor** | The application should provide basic reach-text editing features, where users can enter and format the text content directly from the application using at least:1. Letter stiles (bold, italics, underline)
2. Different types, sizes, and colors of font
3. Bullets and numbering
4. Different paragraph alignments (right, central, left and justified)
 | 1 |  |
|  | **Responsive UI design** | The user interface of the application should be responsive - the pages must render well on various devices and window/screen sizes, from desktop and laptop computers, over tablets to smartphones. | 1 |  |
|  | **Modularity and flexibility** | The application has to be implemented in such a manner that additional changes, improvements would affect other components as little as possible.The architecture of the software application must be flexible, adaptable, and scalable to support long-term increase and/or growth content volume within its database and content repository, by increasing CPU power, RAM, storage space and network bandwidth at the server-side, without the need for major software architecture reengineering. | 1 |  |
|  | **Software licenses** | Software licenses for databases, server operating systems, OCR libraries or similar third party licenses that are needed for the System development/implementation and work should be provided by the vendor as part of software solution. | 1 |  |
|  | **Number of documents and cases** | The software application should put no limits to the number of documents and cases that can be created and managed in the software solution, which should be limited only by hardware and storage capacity. | 1 |  |
|  | **Source code** | Source code developed in the scope of this project must be delivered in electronic format. The Source Code ownership will be passed to the Ministry of Interior/Police free from copyright, accompanied with the technical documentation detailing application build procedures and installation and configuration of the software solutionInstallation of development and testing environment on the equipment of Ministry of Interior/Police | 3 |  |
|  | **Production and testing environments** | The vendor should set up development/testing/training instance on its own infrastructure, throughout the entire development process.The production instance will be hosted on the VMWare virtual infrastructure of the Ministry of Interior of the Republic of Serbia. | 1 |  |
|  | **Data Validations** | The software solution must allow input forms to have validation checks upon business rules provided by the beneficiaries in order to avoid human errors. The exact list of validations on data entry forms will be identified during the joint design phase of the project.The application must unambiguously and clearly notify users of validation errors in case of:1. Mandatory fields not being populated
2. Fields with invalid content (e.g., numbers in text fields, text in numerical fields, letters in phone number, email address without @ sign etc.)
3. Date fields with inconsequent or impossible values (end-date before starting date, future or past dates where it does not make sense etc.)

In case of detected errors in input data fields, the fields that do not pass validation must be clearly highlighted/marked, without losing content/values in the correctly populated fields.Client-side validation can be an additional layer of validation but cannot be an alternative or replacement for proper server-side validation. | 1 |  |
| **USER ACCOUNTS AND PRIVILEGES** |
|  | **User accounts** | Access to the application must be provided only to authenticated users with appropriate access privileges (user roles), exclusively from the internal network of the Ministry of Interior (intranet). | 1 |  |
|  | **User roles and access rights** | Different types of users in an application must have different levels of privileges and permissions. A precise list of user roles and access rights will be defined during the joint design phase of the application, with key users, and will certainly include at least the following levels of access:* Administrator (top level) – creates and administers user accounts, assigns roles and access rights, administers codebooks, manages backups and monitors system usage (reviews the system log).
* Head of unit/department/department: Advanced users who have a high level of access and can perform most of the functional actions that an administrator can do, except for the administration of code books (contents of dropdown menus) and the like. They have insight into all cases handled by operatives under their authority. They can assign or re-assign cases to Police Officers. They can generate and read reports, etc.
* Police Officers: Manage the case/investigation and perform all actions on the case assigned to them. They can access and change data only in their own cases.
 | 1 |  |
|  | **Minimum Required Privileges** | User roles in the application should be defined on the principle of "minimum required privileges". User roles should not even see which functionalities are available to users with a higher level of privileges (e.g. to see all functions but for some to be greyed out/inactive in their account). | 1 |  |
|  | **Accounts creation and management privileges** | User accounts are created solely by a user with administrative privileges. When creating a new user account, an initial password is set, which must be changed after first successful login. | 1 |  |
|  | **User authentication** | When logging into the application, user authentication should be done based on the username and password to access the system. | 1 |  |
|  | **Session lifetime** | The software solution must provide session expiration setting. If a user is not active for a specified period, he must be automatically logged off. The period must be configurable via system parameters by the system administrator. Also, an active session must always terminate when the user closes the browser or explicitly logs out of the system. | 1 |  |
|  | **Password Complexity** | The software application must require users to create passwords that meet minimum complexity requirements, including the use of uppercase and lowercase letters, numbers, and special characters. Passwords should have a minimum length of at least 6 characters. | 1 |  |
|  | **Account Protection/Lockout** | The software application should lock user accounts for a specified period of time (e.g. 3 minutes) after a certain number of failed login attempts, to prevent brute-force attacks.Any such event should be recorded in the system security log with date, time, IP address. The system security log should only be visible to system administrators. | 1 |  |
|  | **Password security at rest** | Passwords must not be stored in the system in their original form, but exclusively as some form of hash function (eg SHA-3), using the implementation of the PBKDF2 standard, etc.Passwords or session tokens must not be transmitted or viewed as part of a URL. | 1 |  |
|  | **Two-factor authentication** | For users with a high level of privilege (e.g. system administrators), it is preferable that the application requires multi-factor authentication, such as 1. One-time code sent to the user's mobile phone or
2. One-time code generated by Google Authenticator or Microsoft Authenticator installed on users phone, or
3. Token generated using a USB key with a fingerprint reader (eg Yubikey) that supports FIDO U2F, FIDO2, OTP, PIV or OAuth protocols.

Alternatively, users can log into the application using the PKI infrastructure, i.e. smart cards with a qualified electronic certificate, protected by a PIN code. | 2 |  |
|  | **Forgotten Password** | When the user forgets the password, the application must not enable "recovery" of the forgotten password, but the password must be reset by sending a direct password reset link to the registered email address. After resetting the password, the user must log in again by entering a new password. | 1 |  |
|  | **Duration of the session** | If the user is inactive in the softwre solution for longer than the set time interval (number of minutes) at the system level (e.g. 30 minutes), the application should log him out automatically.Also, an active session must end when the user closes their browser or explicitly logs out of the system. | 1 |  |
|  | **Password change policy** | For regular password changes, the application must request the existing password and then enter the new password twice. | 1 |  |
|  | **Active Directory**  | The application should support authentication of users based on Active Directory | 3 |  |
|  | **Authentication by qualified electronic certificates** | The application should optionally have support for authentication using qualified electronic certificates on personal ID cards issued by the MoI/Police. | 3 |  |
| **Application Security Requirements** |
|  | **Secure Design and Coding** | The software application must be designed with security as a top priority, taking into account all common attack scenarios and potential threats.It should be developed using secure coding practices and programming languages, which help avoiding buffer overflows, use of deallocated memory etc. | 1 |  |
|  | **Authentication and authorization** | The software application must implement strong user authentication and authorization controls, such as two-factor authentication, role-based access control, and strict password policies. | 1 |  |
|  | **Data encryption** | The software application must encrypt sensitive data both in transit and at rest (on disk), using industry-standard encryption algorithms and key management practices. | 1 |  |
|  | **System Audit Log** | The software application must log all user activity, including successful and failed login attempts, as well as access to sensitive data and data changes/modifications. | 1 |  |
|  | **Secure deployment** | The software application will be deployed/installed in a secure environment of the Ministry of Interior, with secure configurations, firewalls, intrusion detection systems, and other security measures in place to prevent unauthorized access. | 1 |  |
|  | **Preventing Common Vulnerabilities** | Selected vendor must take maximum care of the security of the application, with a special emphasis on preventing the most common vulnerabilities such as (the list is not exhaustive):1) Using software platforms, libraries or components with known vulnerabilities;2) Access to resources without prior authentication;3) Bypassing the check of access rights of the registered user when accessing resources with strictly defined access rights;4) Displaying the contents of the entire folder when requesting a non-existent resource;5) Displaying details about an exception that occurred on the server side6) SQL injections;7) Buffer overflows;8) Permanent sessions;9) Cross-Site Scripting (XSS);10) Cross-Site Request Forgery (CSRF);11) Using HTTP GET methods for actions that change information;12) Allowing users to use weak/trivial passwords;13) Unsafe “forgot password” mechanism (i.e. sending passwords via email)15) Manipulation of parameters in HTTP requests;16) Predictable resource locations etc.Bidders are expected to provide a detailed and technically precise elaboration of all software and hardware security mechanisms that are foreseen during the implementation of the software application. | 1 |  |
| **CASE REGISTRATION AND MANAGEMENT** |
|  | **Registering a new case** | The application should allow a user with appropriate privileges to create a new case in the software solution, with the following initial data:* Case number (automatic or manual assignment)\*
* Date (automatic assignment with the possibility of manual modification)\*
* The main suspect who is the subject of the investigation\*
* Other persons who are subjects of the investigation
* Connected persons (parents, children, spouse, cousins, best-man etc.)
* Main criminal offense (selection from the dropdown menu)\*
* Minor criminal offenses (selection from the dropdown menu)
* Reference with the prosecutorial case number
* The name of the prosecutor in charge of the investigation
 | 1 |  |
|  | **Case creation privileges** | A new case in the application can be created only by a user with adequate privilege/role. | 1 |  |
|  | **Case searching and filtering** | The application must enable searching and filtering of cases according to different criteria, for example:* case number
* the name, date of birth, address or social security number of the person who is the subject of the investigation
* the case number in the prosecutorial office
* the main criminal offense (law article)
* secondary criminal offence (law article)
* the Police Officer in charge of the case
* to the name of the prosecutor who is competent for the case
* the name of any person in the case
* the monetary value of the potential crime.
 | 1 |  |
|  | **Automatic assignment of case numbers** | The application must have the ability to automatically assign the next available case number to the newly created case, in accordance with the Police case numbering rules for each case type. | 1 |  |
|  | **Case data corrections and modifications** | The application must enable the correction and modification of all data in the case, but only to users with appropriate privileges. All changes must be recorded in the system audit log. | 1 |  |
|  | **Preventing creation of duplicate cases** | The application should display notification/alerts if the user creates a new case with the same main suspect and the same criminal offense, as in another existing case registered in the application. | 1 |  |
|  | **Case assignments and re-assignment to Police Officers** | Heads of units must have the possibility to assign the newly created case to a specific Police Officer. The application must also allow random selection of Police Officer who will assigned the case. The superiors/managers must have the possibility to re-assign (transfer) the existing case, currently assigned to one Police Officer, to another operative, if needed (longer absence or vacation, illness, too many pending cases in work, retirement etc.) | 2 |  |
|  | **Case visibility and hierarchy** | Each Police Officer may see only his own cases (the cases assigned to him).Superiors (heads of services/units/departments etc.) must be able to see all cases of Police Officers under their line of authority.The head of the higher-level police organizational unit should be able to see the cases of all lower-level units and all Police Officers working in them. | 1 |  |
|  | **Automatic background checks of the lead suspect in the case.** | Upon registering the case and primary suspect (case holder – nosilac predmeta) the application should be able to perform checks in available national and international databases and registries based on his name and personal ID number. The background checks should not stop the user working further in the case. | 3 |  |
|  | **Classified (confidential) cases** | The application must allow certain cases to be marked as “classified” (confidential) and, accordingly, to limit access to exclusively a specific set of information, except for specially designated users with privileges to access “classified” investigation cases. | 1 |  |
|  | **Quick case overview****(Executive Summary)** | The application must have the ability to display summary information for the selected case, which allows the manager or superior to quickly get acquainted with case details and status of the selected case as quickly as possible. The case details should provide not only case number, case type, case status, date registered etc. but also:* Names of all persons (suspects) in the case
* Name of the Police Officer in charge
* References to other internal or external case numbers
* Name of the public prosecutor in charge of the investigation
* List of received documents (type of document, sender, date of receipt)
* List of sent documents (type of document, recipient, date of sending)
* Chronological list of conducted investigative and other actions in the case
* Calendar of planned tasks and activities in the case in the upcoming period
 | 3 |  |
|  | **Full-text search** | The application should enable user to search or filter cases search through all case metadata and all received and sent documents in the case at once (full text search). | 1 |  |
| **REGISTERING AND MANAGING TASKS AND ACTIVITIES IN CASE** |
|  | **Creating a task** | Users must be able to create new tasks, specify its title, its description, due date, priority level and status (scheduled/to-do, in progress, done). | 1 |  |
|  | **Task assignment** | Police Officers must be able to self-assign new task only.Superiors must be able to create, delegate or share tasks to other Police Officers.The application must provide notifications to users when tasks are assigned to them, or when tasks are updated (completion status changed, due date changed etc.). The notifications must be clearly visible on the front page, immediately after logging in to the application. | 1 |  |
|  | **Task searching and filtering** | Users must be abple to search tasks by title, status, priority, due date, and owner (assigned user - only for heads of organisational units).Police opratives can search and see only his own cases and tasks. Superiors should be able to see all tasks from all cases assigned to Police Officers under his competence/responsibility. | 1 |  |
|  | **Comments and remarks** | The application must allow Police Officers to post comments on tasks and attach files. | 1 |  |
|  | **Completed task summary** | Users must be able to designate task as done/completed with the short summary that can be automatically inserted into monthly report. | 1 |  |
|  | **Task reporting** | The application must provide task/activity reporting capabilities to superiors, to track task progress over time for all their subordinate Police Officers.The superior officers must be able to generate reports and statistics on tasks conducted on all cases within a unit/department in a given period. | 1 |  |
| **REGISTERING AND ADMINISTRATION OF PHYSICAL AND LEGAL PERSONS IN CASE** |
|  | **Registration of persons in case** | The software application shall provide a user-friendly interface for registering arbitrary large number of physical and legal persons in a court case, including the ability to enter personal and contact information. | 1 |  |
|  | **Personal and contact information about the persons in case** | The list of personal and contact information includes:* 1. First Name
	2. Parent’s name
	3. Last Name
	4. Date of birth
	5. Place of birth
	6. Unique Personal Number (JMBG) or company registration number
	7. Personal ID card number
	8. VAT number (for legal persons only)
	9. Passport number
	10. Job Title
	11. Company/Organization Name
	12. Email Address
	13. Phone Number (Work, Mobile, Home)
	14. Residential Address
	15. Social Media Profiles (Facebook, Instagram, LinkedIn, Twitter etc.)
	16. Relationship/Marital Status
	17. Spouse name
	18. Education
	19. Occupation/profession
	20. Name and address of the company of employment
	21. Photo
	22. Comment/Remark

The list is not comprehensive, and may include some other information on the basis of which the identity of the person can be determined (driver's license number, etc.) or contact can be made with him. The final list of fields will be determined in the application design phase, in cooperation with the users. | 1 |  |
|  | **Creating associations between persons** | The software application shall allow for the association of registered persons in case with specific documents, assets, other persons etc.For example, if one of the parties in the case is Petar Petrović, the application should enable Police Officer in charge of case, to record that Petar Petrović is the owner of a certain bank account, apartment or other real estate, vehicle, vessel, safe deposit box etc.Vendors are encouraged to propose the easiest possible and most intuitive way for Police Officers to achieve this functional requirement. | 1 |  |
|  | **Search functionality** | The software application shall provide a search functionality to easily locate registered persons by name, personal ID number, case number, or any other relevant search criteria. | 1 |  |
|  | **Personal data protection** | The software application must implement particularly strong security measures to protect the personalal and contact information of registered persons in case, in compliance with all relevant personal data protection regulations of the Republic of Serbia. | 1 |  |
| **REGISTRATION AND MANAGEMENT OF FINANCIAL AND OTHER ASSETS (FOR FINANCIAL INVESTIGATION UNIT ONLY)** |
|  | **Assets registration** | The application must provide means of registering financial, material and other assets that are suspected to be linked to money laundering, including bank accounts, owned companies, real estate, vehicles, motorcycles, vessels, and other assets. | 1 |  |
|  | **Warning on already registered property** | The application must warn the user (Police Officer) when registered property (e.g. bank account number, cadastre parcel number, car license plate, company registration number etc.) already exists in the existing case or in the another case. | 1 |  |
|  | **Categories and subcategories of assets** | Each specific type of asset may be categoritzed and subcategorized. For examples real estate can be categorized into apartments, houses, land, vehicles etc. while vehicles can be subcategorized into cars, SUVs, trucks, buses, commercial vehicles etc.Each of the category and subcategory can have some specific attributes (metadata) that better describe the nature and financial value of an asset. | 1 |  |
|  | **Financial information** | The application must allow for the recording of relevant financial information for registered assets, such as transaction history, account balances, and ownership details on the assets. | 1 |  |
|  | **Documents and evidences related to specific asset** | The software application should support for attaching documents or evidences related to specific registered asset. | 1 |  |
| **REGISTERING ACTIVITIES IN CASE OF THE POLICE OFFICERS** |
|  | **Registering activity** | The software application must support registering different types of activities in case, such as evidence collection, witness interviews, bank transactions chek, suspect interrogations, and other relevant activities. The operatives must be able to record these activities in case, including at least the following metadata:* Title of the activity
* Type of activity (from the drop-down list)
* Priority level
* Start date and time of conducted activity
* Status of the activity (in progress, finalized)
* Finalization date and time of the activity (if finished)
* Optional attached documents or evidences
* Brief summary of the activity (used for reporting) – specifically formulated in such a fashion that it can be automatically inserted into monthly report.
 | 1 |  |
|  | **Activity filtering** | :The software application must allow users to filter activities by various criteria, such as title, category, status, priority, due date etc. | 1 |  |
|  | **Reporting on the activities** | The software application must provide reporting capabilities to help Police Officers and their superiors track activity progress over time, including activity completion statuses, workload and productivity of specific operatives, time needed to complete activities, list of “in progress” activities etc. | 1 |  |
| **CALENDAR MANAGEMENT** |
|  | **Calendar Support** | The application must enable planning and time management of Police Officers in order to achieve specific goals or tasks in case.This includes tasks such as weekly task planning, setting reminders, scheduling meetings, and coordinating with other Police Officers or superiors to ensure operative schedules are aligned with each other. | 1 |  |
|  | **Calendar of vacations and other planned absences** | In order to act in a timely manner and avoid setbacks in investigations, the application must have a calendar of vacations, sick days and other planned absences of Police Officers, whereby all users of the application are required to enter planned/expected absences in the calendar.During the period of the announced absence, all notifications and warnings related to the Police Officer's cases should be received by his superior, so that he can assign the case to another operative. | 1 |  |
|  | **Task escalation in case of absence of the user** | The application should support the absence calendar, whereby all operatives should enter the planned days of absence (annual vacation, sick leave or other reason) into the calendar.The application should notify the superior if the arrival of an urgent request or task is recorded, and the Police Officer in charge of the subject is currently absent, so that another operative could act on the request.In the event that the planned absence is not recorded in the calendar, and the application detects that the operative has not logged into the application for more than 3 working days, the application should also forward all notifications and warnings regarding his cases to his superior.In the event that the superior is also on a planned vacation, or has not used the application for 3 or more working days, the notifications are redirected hierarchically to the next superior manager, up the command line etc.. | 1 |  |
|  | **Automatic reminders for expired deadlines** | The application must monitor the statuses of requests sent to external institutions.For each type of request, in the administrative part of the application it should be possible to set a statutory (or usual) deadline for receiving a response (for example, the deadline for receiving a response from Business Registers Agency may be 8 days, from Cadastre it may be 10 days, from commercial banks 5 days, etc. .)If it is not recorded in the case that a response to a certain request arrived within the deadline defined for that type of request, the application should display a notification/warning to the operator | 1 |  |
|  | **Plan of future activities** | The Police Officer must be able to recordin in the case his schedule/plan of the near-term planned activities.This plan of activities (“work plan”) must be visible to his superior through the application. | 1 |  |
|  | **Automatic monitoring of deadlines** | The Application must be able to monitor the fulfilment of the set deadlines for completion of the case and monitor course of action upon request.Deadlines may be related to expected reception of the response to the request for information from external institution, set task completion deadline set by the user manually, set deadline for completion of the activity by the superior etc. | 2 |  |
|  | **Scheduled standard operational procedures** | When opening a new investigation, the operatives usually always send the same list of requests for pinformation about the person who is the subject of the investigation to external institutions (commercial banks, cadastre, business registers agency etc.)The application must be able to batch-generate a list of standard output documents "on a click", based on predefined forms (templates), by inserting personal data (name, surname, JMBG, address, etc.) into the standard templates of these documents. | 1 |  |
|  | **Tracking the deadlines for responses from external institutions** | The application must track the status of responses to requests/notices sent to external institutions. If the response to a request has not been registered in the application within the given deadline (deadlines depend on the type of request), the application should display a warning to the Police Officer when logging into the application, for all his cases where the deadline for receiving response has expired. | 1 |  |
|  | **Management of tasks and events** | The application must allow users to enter in the calendar their future tasks and events, which can be planned for a specific day and time, or free in terms of date, but with a set deadline for completion.A task is an activity or action carried out by the user himself (eg operative) and which must be completed no later than the date set in the calendar. It can also be seen as a "to-do" list with a final deadline for completion, which is written into the calendar.Meetings, hearings, etc. are events planned or scheduled independently of the user, to take place on a specific day, at a specific time and in a specific place, where the presence of the user is expected or necessary and therefore entered in the calendar. | 1 |  |
|  | **Upcoming events notification** | The user (operator) must be able to set how far in advance he needs to receive a notification from the system about an upcoming event or approaching a set deadline for implementing a certain activity. | 1 |  |
|  | **Management-level access** | Superiors should be able to see the calendars of their operatives, in order to become familiar with their activities and planned tasks in the coming period. | 1 |  |
| **ELECTRONIC DOCUMENT/CONTENT MANAGEMENT SYSTEM** |
|  | **Electronic content storage** | The Application must provide a unique and centralized electronic storage of all documents in the cases.Users must be able to upload arbitrary number of documents in the formats that the police use in their work: PDF, Word (doc/docx), RTF, TXT, Excel (xls/xlsx), ODT.It must be possible to store (upload) and display/play electronic evidence in different multimedia formats:* 1. Photos (jpg/jpeg, png, gif, bmp, heif/heic)
	2. Sound recordings (wav, mp3, acc, ogg, flac, m4a)
	3. Videos (mp4/m4v, avi, mov, hevc)
 | 1 |  |
|  | **Approvals of draft documents** | The application should provide the possibility of sending working versions (drafts) of documents by the Police Officer to his superior (commander), for review and approval, if a certain type of output document requires explicit approval before being furthre processed or sendt to internal or external recipients. | 2 |  |
|  | **Organization of electronic content in the application** | The application must provide different ways of organizing and categorizing electronic content (documents, evidence, etc.), by investigated person/suspect, type, sender, recipient, date, category, subcategory etc.Users must have the possibility of assigning additional metadata to all documents in the software solution, that more closely describes the type and content of the document in the system and facilitates their later retrieval and filtering. | 1 |  |
|  | **Searching and filtering of documents** | The application should provide advanced document searching and filtering options based on categories and keywords that can be entered/associated with the document (metadata searching). | 1 |  |
|  | **Automatic import of financial transactions from uploaded Excel files** | The application must enable Police Officers to upload Excel files with money tranfers, submitted by the banks, and automatically parse/import individual transactions into the case without the need for manual entry. | 2 |  |
|  | **Non-exact and phonetic search capabilities** | The support for non-exact and phonetic searches (e.g. variant of Soundex) by keyword or phrase, is not mandatory, but will be considered as strong advantage of the offered solution. | 3 |  |
|  | **OCR and full text search** | The application must index all documents in the software solution and enable searching through their content (full-text-search), regardless of whether they are original text or scanned document (image).For scanned documents, the application must enable reliable optical character recognition (OCR) for Serbian Cyrillic and Latin and then automatically index the recognized text.**This requirement is critically important and absence of this feature in the proposed software solution will automatically disqualify potential vendor.** | 1 |  |
|  | **Digital signing with qualified electronic certificates** | The application should have support for digital signing of documents using qualified electronic certificates on personal ID cards issued by the MoI/Police. | 2 |  |
|  | **Document Archiving** | The application should provide the possibility of automatic archiving and/or deletion of old documents, in accordance with the internal rulebook on the storage and archiving of electronic documents in the Ministry of Interior/Police.The application must allow users to mark/designate some attached documents in the case for keeping indefinitely (no archival/deletion). | 1 |  |
|  | **Document Generation** | The application must provide ability to generate documents in multiple formats, such as MS Word (.doc/.docx), MS Excel (.xls/.xlsx) and Adobe PDF etc. by populating templates with “live” data from the application’s database. | 1 |  |
|  | **Editable templates** | The application must provide functionality for creating and updating templates for generating documents. | 2 |  |
|  | **Reports and statistics** | The application should provide the ability to generate various reports and analytical products on the types and number and documents etc. in the case, department/unit or entire database, on given day, or registered in a given period. | 1 |  |
|  | **Recording the reception of expected document** | Police Officers must be able to mark that a response to request for information or other expected document was received from the external actor.In that case, a alarm for document reception deadline should be cleared. | 1 |  |
|  | **Document location tracking** | In order to eliminate or reduce the possibility of losing documents from the case, the application has to enable recording/tracking of physical location of paper documents and files.The user must be able to enter in the application a comment or remark on the current physical location of specific document from the case (e.g. “given to head of the department”, or “forwarded to Criminal Analytics Service”) | 2 |  |
|  | **Documents sharing** | The application should have the possibility of internal sharing of documents between users (Police Officers, their superiors, criminal analysts, etc.) internally within the application, without the need to download the document and send it by email, via USB drives or any other similar method.The user with whom the document or multimedia file is shared may only have access in "read-only" mode, without the possibility of modifying or deleting the document, and for each sharing of the document and access to it, a record must remain in the system log of the application. | 2 |  |
|  | **Conversion of uploaded images to PDF documents** | The application must allow users to generate printable PDF from uploaded images, for easier printing and using as an evidence in the court. | 2 |  |
|  | **Automatic antivirus scanning of documents** | The application must perform an antiviral scan of each uploaded document to lower the risk of malicious or content infected by computer virus, Trojan etc.The Ministry of Interior/Police already have a organization-wide antivirus solution in place that must be configured for fully automatic operation, without the need for manual administrator's actions. | 1 |  |
| **INTEROPERABILITY – INFORMATION EXCHANGE WITH INTERNAL AND EXTERNAL INFORMATION SYSTEMS** |
|  | **Web services API** | The software solution must provide an web services API module which should serve as a gateway for connecting system to third party web service interfaces (e.g. National Bank of Serbia, Business Registers Agency, Cadastre). | 1 |  |
|  | **Web service standards** | The web services used for interoperability between the new software application and external systems must comply with industry standard web service specifications, such as SOAP (Simple Object Access Protocol) or REST (Representational State Transfer). | 1 |  |
|  | **Communication protocols** | The web services used for interoperability must use standard communication protocols, such as HTTP or HTTPS, to ensure compatibility and security when communicating with a wide range of external information systems. | 1 |  |
|  | **Message format** | The web services must use a standard message format for exchanging information between the information system and external systems. The message format shall support industry standard data formats, such as XML or JSON | 1 |  |
|  | **Authentication and authorization** | The web services must support authentication and authorization mechanisms, such as OAuth or SAML, to ensure secure access to data. | 1 |  |
|  | **Error handling** | The web services must define a standard method for handling errors, including error codes and descriptions, to help diagnose and resolve issues that may arise during interoperability.Users must be aware when web service that was expected to automatically acquire the information – failed. | 1 |  |
|  | **Data validation** | The web services must validate data received from external systems to ensure that it conforms to the expected format, data type, and content. | 1 |  |
|  | **Service availability** | The web services must be highly available and scalable to ensure that external systems can access the information system and its services at any time, not only during working hours. | 1 |  |
|  | **Web services performance monitoring** | System administrators must be able to track services usage, performance, and availability (i.e. the statistics of data exchanges with external systems, by type and number/count).Time limits for the execution of requests must be enabled, with adequate alarms in case that specific web service requests frequently fail. | 1 |  |
|  | **Acquiring the list of owned or controlled companies from the Business Registers Agency** | The application must have the ability to automatically check if the investigated person owns or manages a company or other organization registered with the Business Registers Agency. | 1 |  |
|  | **Acquiring the list of bank accounts for physical or legal person from the NBS** | The application must have the ability to automatically download a list of all existing bank accounts for an individual or legal entity via web service of the National Bank of Serbia. (<https://www.nbs.rs/sr/drugi-nivo-navigacije/servisi/sistem-veb-servisa-NBS/>).The application should support automatic electronic signing of XML requests to the National Banko of Serbia. | 1 |  |
|  | **Acquiring the list of owned properties (real estate) from the Cadastre** | The application must have the ability to automatically check if the investigated person owns land, houses or apartments, registered with the Republic Geodetic Institution (Cadastre). | 1 |  |
|  | **Acquiring the list of owned vehicles from the Police information system** | The application must have the ability to automatically check if the investigated person owns cars, motorcycles or other vehicles registered with the MoI. | 1 |  |
| **STORAGE AND TRANSFORMATION OF EXCEL AND OTHER FILES USED BY THE CRIMINAL ANALYTICS SERVICE** |
|  | **Sharing case files with the Criminal Analytics Service** | The application should enable Police Officers to store files and make them accessible on demand (i.e. “share”) to the Criminal Analytics Service, with appropriate descriptive metadata (case number, comment - note, etc.)The Criminal Analytics Service must access these files in read-only mode, but should be able to download a local copy of the files for their own needs. | 1 |  |
|  | **Access rights** | Police Officers can only see and access files that they have personally entered into the application.Superiors can see all documents of subordinate operatives and organizational units under their command.Criminal Analytics Service (CAS) must not be able to access any file attached to any case, unless that file was previously explicitly shared with the CAS by Police Officer who manages the case. | 1 |  |
|  | **Transformation and merging of Excel files in different formats** | Banks and money transfer institutions provide the same set of data describing financial transactions (money transfers), but these information are usually displayed in different columns of Excel tables, which differ from bank to bank (differences exist in the order of columns and formats of date, time, monetary amounts etc.).The application should enable automatic transformation and merging of selected Excel tables into a common/uniform format used by the Criminal Analytics Service. | 1 |  |
|  | **Preserving original (source) Excel files with financial transactions, after transformation** | After transformation and merging into common-format Excel file, the application must preserve and keep the original Excel tables with monetary transactions in the original format, as provided by the banks, as it may be required as an evidence in the court. | 1 |  |
|  | **Searching through Excel files** | The application must enable searching and filtering of stored Excel tables by a given text/phrase in the contents, in order to locate the Excel table containing specific name, date, amount, etc. | 1 |  |
| **PERFORMANCE & STATISTICAL REPORTS** |
|  | **Reporting subsystem** | The application should provide users with a functional reporting system, with a set of standard, pre-defined (standard) reports and statistical .The total number of predefined reporting formats and sections is expected not to exceed 15 , with the ability to produce custom (ad-hoc) report in accordance with the set criteria | 1 |  |
|  | **Periodic reports** | The application must be able to generate annual, six-monthly, quarterly statistical reports, as well as statistical reports for an arbitrary date range (number of new cases, number of cases in progress, number of resolved/inactive cases, average number of cases per operative, department, etc.) | 2 |  |
|  | **Professional looking reports** | Reports must be formatted in a consistent and professional manner so that they are easy to read and understand and can be printed so that the appearance on paper is professionally looking and readable (avoiding overly small fonts etc).All reports must be versioned, that is, they must bear the date and time of generation, so that users can easily compare different versions/iterations of the same report. | 1 |  |
|  | **Data visualisation** | Reports must have the ability to display not only tabelar data, but also graphs, pie-charts and other appropriate data visualisations to make the report more understandable. | 2 |  |
|  | **Custom (ad-hoc) reports** | It is desirable that the application supports creation of custom (ad-hoc) reports on demand, without the need to engage a software developer. The functionality and the ease of creating custom reports will be especially valued when evaluating proposals for the development of the software application. | 2 |  |
|  | **Exporting reports to Excel** | Users must be able to export data from a custom report into Excel or PDF file for further processing. | 1 |  |
|  | **Reporting module access rights** | The software application must ensure that only authorized users with adequate privileges can access and generate performance and statistical reports. Such privilege would be assigned only to selected user roles (i.e. heads of directorates, departments, units etc.)The software application shall provide an interface for administrators to set user permissions, including the ability to generate performance and statistical reports, without the need to engage software developer to configure user privileges.The software application must require users to authenticate their identity before granting access to the performance and statistical reporting functionality, and allow only users with the appropriate privileges to access and generate performance and statistical reports.The software application shall log all user activity related to generating performance reports and statistical reports into the system audit log. | 1 |  |
|  | **Scheduled automatic reports** | The application should have the ability to generate specified reports and statistics at certain intervals (e.g. every Friday, or every 1st working day of the month). These reports should be automatically distributed to configured list of recipients. | 3 |  |

**Annex 2 – Procurement of desktop computers and scanners – Lot 2**

**Technical requirements**

All computers and scanners shall be provided complete with the necessary cables, power adapters and/or parts such as to ensure that the unit/system is capable of operating to the required technical and quality specifications. All specifications details listed for each item are the minimum requirements. Any deviations from the required specifications, or additional features offered, must be clearly and unambiguously identified in the offer.

**Power standard**

The equipment must be designed for supply voltage in Serbia of 220 V (single-phase) with neutral, and 50 Hz nominal frequency. The quality and stability of the supplied voltage may undergo fluctuations (plus or minus) of 10%, and all equipment must be capable to operate on mains supply voltage with such fluctuations. All equipment must be designed for direct connection to the standard single phase power outlets in Serbia.

**Equipment configuration**

The items to be provided should not be hybrid configurations assembled from independently purchased parts, but designed as a unit and shall have a registered brand name and model. Computers must satisfy with Minimum System Requirements for installation of Windows 11 Pro, including Trusted Platform Module 2.0.

Equipment allowing capacity upgrading must be provided in a way that upgrades can be performed by installing additional RAM, without discarding the already installed RAM modules.

The Supplier shall furnish, install and commission all equipment, fittings and fixings, including final installation and connection and all miscellaneous items of equipment, fixings and fittings in order that the supplies are left in place tested, fully operational and ready for use.

The Supplier must provide necessary measures to prevent any damage during delivery and installation stage(s). If damage occurs it must be rectified in an appropriate way by the Supplier. Supplier must keep the work site clean and safe against fire and/or other hazards during any/all delivery and installation stage(s) until formal acceptance.

Equipment must conform and/or be compatible with standards, or with the commonly accepted best production practices currently in force, including any ISO, IEC or other relevant standards that may apply to each specific category of equipment.

The Supplier must provide evidence of his, or the manufacturer’s if the Supplier is not the manufacturer, current Quality Management System Certificate according to ISO 9001 or national equivalent, for each equipment item or group of items.

Suppliers are required to demonstrate that offered specifications are responsive to the tender dossier requirements identifying model and manufacturer of each individual item in their technical offer and providing necessary documentation such as catalogues, brochures, manuals and/or booklets that provide detailed technical specifications of equipment being offered thus enabling the contracting authority to check the information provided in the offer.

All desktop workstations must be compatible with Microsoft Windows 10 and Windows 11 operating systems.

All peripheral devices (printers and scanners) must be current model with Microsoft certified drivers available for Windows 10 and Windows 11.

All software that is delivered in this tender (such as Microsoft Windows system and Microsoft Office application suite) must be licensed to the beneficiary of this tender (Ministry of Interior of the Republic of Serbia) that will allow trained personnel of the beneficiary to perform software installation, update/upgrade, repair/debug and/or diagnosis/report activities without supplier assistance in the future.

**Technical documentation to be delivered**

Each item set of equipment shall be provided with an original set of users’ manuals (printed and / or on a CD/DVD) for all parts of the equipment. These manuals shall be supplied in English (mandatory), and Serbian language (will be considered as advantage).

The obligatory documents for the provisional acceptance.

• Original certificate of origin

• Warranty document, signed and stamped by the manufacturer and/or the supplier

• The Supplier should prove that the equipment proposed is produced by a manufacturer who is accredited by ISO 9001 or an equivalent standard.

No provisional acceptance can be pronounced without the presence of the complete set of documents. These documents or the declarations for the provision of the documents should be delivered with the bid.

**Warranty**

The Vendor should warrant that all items delivered shall be free of defects in materials and workmanship for a period of 5 (five) years for current model (in production) items and 2-year for spare/replacement items, after provisional acceptance and that in case of reported item malfunction would repair or replace the product at no charge.

Warranty for all items in this tender must be on “collect and return” basis, i.e. if an item cannot be repaired on site, the Vendor should organize the transport from the beneﬁciary’s premises to the service center.

**Beneficiaries may request to keep physical possession of a broken hard drives in some or all of their computers in order to ensure security and confidentiality of classified, proprietary or sensitive data related to Police investigations, without forgoing warranty. This is a mandatory requirement, and all Suppliers must explicitly state in their proposals that they understand and accept this requirement.**

The technical offer shall include an information of how the warranty will be provided including name of the service organization, contact person(s), postal address, telephone and e-mail address.

**Minimum technical specifications for the desktop computers and office scanners**

|  |  |  |
| --- | --- | --- |
| # | Item | Quantity |
| 1 | **Desktop computer*** Intel Core i5-12400 or newer/better processor (or AMD Ryzen 5 5600x or better)
* 16GB RAM (DDR4 or DDR5) or more memory (expandable to at least 32GB)
* 512GB SSD or greater capacity drive
* Optical drive (DVD+/-RW)
* Ethernet port (wireless adapter not allowed for security reasons)
* Minimum 4 USB-A ports and 2 USB-C ports
* Integrated or discrete graphic card with HDMI or DisplayPort output connector
* 22” TFT/IPS Display or bigger, 1920x1080 screen resolution or greater DisplayPort or HDMI connectivity
* Full size keyboard with Serbian layout + optical mouse (corded or wireless).
* Pre-installed Windows 10 Pro (or Windows 11 Pro) and Microsoft Office 2021 with **perpetual license**
* Warranty: On-site “Keep Your Drive” warranty, minimum 5 years
 | 35 |
| 2 | **Professional Office Scanner*** Scanner type: Duplex, ADF (Automatic Document Feeder) with minimum 50 pages ADF capacity
* Optical resolution: minimum 600 dpi color/grayscale/B&W
* Designed for high-volume scanning with daily duty cycle of 5000 sheets or more
* Scanning speed: at least 50 simplex pages / 100 duplex pages per minute at 300DPI
* Document size: A4, legal, and letter-sized documents or bigger
* Connectivity: USB 3.x, Ethernet
* Compatibility: Windows 10/11 and Mac OS
* Software: Included OCR capable scanning software (preferably Adobe Acrobat Professional)
* Warranty: 2 years or more
 | 5 |