**APPENDIX 3**

SPECIFICATIONS

for the development and implementation of the Intranet System of the

People’s Advocate Office (the Ombudsperson’s Office)

(Appendix 3 - Business Requirements)

[**1. General definitions**](#_gjdgxs)3

[**2. The People’s Advocate (Ombudsperson) field of activity**](#_30j0zll)3

[**3. References**](#_1fob9te)4

[**4. Terminology and abbreviations**](#_3znysh7)4

[4.1. Abbreviations](#_2et92p0) 4

[4.2. Key Terms](#_tyjcwt) 4

[**5. System’s usage**](#_3dy6vkm)5

[**6. Project development phases**](#_lb1mk92i9hv4)6

[6.1 Inception phase](#_ljglhzv9cwz0) 6

[6.2 Development phase](#_tuvaygf7h98r) 7

[6.3 Training phase](#_rsg5ldtg6dtd) 7

[6.4 Maintenance phase](#_zflkjaoxs4ft) 8

[**7. Business model of the object of automation**](#_4d34og8)8

[7.1 Business roles](#_2s8eyo1) 9

[7.1.1. Intranet system actors](#_17dp8vu) 9

[7.2.1. Business roles](#_3rdcrjn) 11

[7.3.1. Services](#_26in1rg) 12

[**8. Functional Requirements for the System**](#_35nkun2)14

[8.1. System’s Functional Model](#_1ksv4uv) 15

[8.1.1. UC 01 Intranet System's Use](#_44sinio) 15

[8.1.2. UC 02 Business Process](#_z337ya) 26

[8.1.3. UC 03 Intranet System Administration](#_3j2qqm3) 39

[**9. Requirements for the system as a whole**](#_1y810tw)43

[9.1. Requirements for the system’s architecture](#_4i7ojhp) 43

[9.2. Requirements for the information security and protection](#_2xcytpi) 43

[9.3. The requirements regarding the information integrity](#_1ci93xb) 44

[9.4. Requirements regarding the migration of the existing information](#_3whwml4) 44

[9.5. Requirements for the system performance](#_2bn6wsx) 45

[9.6. Requirements for the hardware and the communication channel](#_qsh70q) 46

[9.7. System Reliability](#_3as4poj) 46

[9.8. Obsolescence Technologies](#_1pxezwc) 47

[9.9. Method of Testing and Acceptance;](#_49x2ik5) 47

[9.10. Documentation and Training](#_2p2csry) 48

## 1. General definitions

Full name: *Intranet System of the People’s Advocate Office (the Ombudsperson’s Office)*

Short name: *IS of the Ombudsperson’s Office or IS*

Institution name: *People’s Advocate Office (the Ombudsperson’s Office) (hereinafter - the Ombudsperson’s Office).*

The system to be implemented aims at the creation of an environment of collaboration and documents’ exchange inside the Ombudsperson’s Office and also at uniting all subdivisions and their representatives into a unique informational system, regardless of their geographical situation. The implementation of such a system would lead to the improvement of the processes of work within the organization, would open the extended possibilities over the skills of information analysis and reference, the control over the documents’ flows.  
Important criteria to consider in the IS implementation is that the intranet system is a private network intended to be accessible only to the organization's staff, thus the final product should fulfill the end users expectations and to provide an ‘easy to use’ user interface.

## 2. The People’s Advocate (Ombudsperson) field of activity

The People’s Advocate (hereinafter-Ombudsperson) institution is a public authority, autonomous and independent from any other public authority, under the law. The institution’s field of activity is based on the protection and promotion of human rights, including prevention of torture and other cruel, inhuman or degrading treatment in the society.

The activity of the Ombudsperson, his representatives and of the staff working under their authority has public nature.

At the request of persons whose rights and freedoms have been infringed, the Ombudsperson should document the petitions, carry out investigation activities under the terms of the law in collaboration with public authorities that have the obligation to communicate any information, documents or other acts that they possess related to the petitions submitted. At each phase the result of their activity is reviewed and documented, so at the final stage a folder with all documents is stored and can be used in later perspectives.

At the request of a state authority, the Ombudsperson should provide reports which must contain information regarding their activity and may contain recommendations regarding the amendment of legislation or measures of other nature for the protection of individuals’ rights and freedoms.

The Ombudsperson has an internal established hierarchical structure with its divisions, subdivisions and territorial branches where every employee has his role with different responsibilities and empowerments. For every new case, there are roles responsible to document it and to assign it to appropriate person that has the duty to create tasks and to monitor the investigation process.

The intranet system is expected to provide the ability to create virtual folders for each cases of investigation, to which users will be able to assign documents and to track all their activities.

Currently, all the documents and folders are mostly present in a paper-based format and are not properly stored in a database or in any other structural form that could allow easily to identify the set of statistical data necessary to be stored into the intranet system.

## 3. References

The technical requirements are elaborated according to the Intranet System Concept of the Ombudsperson’s Office. All references to the regulatory enactments and guide books of international practices and general ideas about the system are specified in the Concept of Intranet System (Appendix 4).

## 4. Terminology and abbreviations

### 4.1. Abbreviations

**ERMS** – Electronic Record Management System

**IS** –Intranet System

**The Ombudsperson’s Office** – The People’s Advocate Office

**NPM** – National Mechanism for the Prevention of Torture

**WAN** – Wide Area Network

### 4.2. Key Terms

**Classification (data management)** – The identification and systematic arrangement of business activities and/or the data into categories, according to the logically structured conventions, methods and procedure rules, presented in a classification system.

**Classification schemes** – Hierarchic arrangement of classes, files, sub-files, volumes and data.

**Document** – Registered information or object that can be treated as a whole.

**Electronic Record** – Record presented in electronic form.

**File** – An organized unit of data grouped according to the principled of connection to the same subject, activity or transaction.

**Note**: This is the definition of file in the Data Management. As it can be seen, this definition differs from that used in the sphere of Informational Technologies.

**Metadata** – Data describing the context, contents and structure of data and their management in time.

**Data** – Information created, received and kept as proof by an organization or person for the fulfillment of the legal liabilities or business transactions.

## 5. System’s usage

The Intranet System is elaborated for the employees of the Ombudsperson’s Office for the internal use and meant to implement a modern solution of collaboration between the subdivisions of the Ombudsperson’s Office aiming at the improvement of information processing, workflows definition and management, grouping documents, which as a result would lead to the increase of the quality of public services provided and to the transparency of decision-making. The Intranet System is defined as the totality of information storage and organization procedures, definition and management of workflows, measures of storage and use of the information meant to contribute to the fulfillment of the Ombudsperson’s Office and NPM objectives.

The major objectives of the Intranet System of the Ombudsperson’s Office:

* Enhance communication and reduce the effective time to answer to interpellation: integrate the system with email management engine and build an effective automated notification sender.
* Introduce a reliable and efficient management system for the dossiers of investigation powered by flexible and predefined workflow procedures in order to ensure fast documents delivery to recipients and deadline monitoring.
* Improve the work processes within the organisation: introduce the concept of tasks management.
* Increase the transparency of decision making through monitoring of tasks’ fulfillment, saving the history of actions done and storing all documents in one place.
* Make organisation a unique structure: introduce templates for internal documents and clear description of the internal processes available to everyone in the system.
* Make organisation reliable and efficient: give internal visibility to every process and offer statistical reports.
* Reduce the risk of processes to fail caused by the lack of information from decision maker’s part.
* Implement a secure and protected collaboration environment within the Ombudsperson’s Office and NPM which would include not only the subdivisions of the central office but also the branches in the territory.
* Ensure clear and unique structuring according to the hierarchy defined by the Ombudsperson’s Office’s employees.
* Ensure the formation of a data repository for the storage of documents executed within the Ombudsperson’s Office as well as the documents borrowed from external systems.
* Homogenise the information, messages and actions in the central office and the branches in the territory.
* Offer authentic, true, up-to-date and consistent information to all involved actors.
* Ensure guaranteed rapid access to the data and information regardless of the location according to the access rights and pre-defined roles.
* Reduce costs, increase quality and diversity of communication means.
* Ensure the fulfillment of an advanced and easy to use mechanism for information searching according to different criteria and keywords.

## 6. Project development phases

The development and implementation of the IS of the Ombudsperson’s Office should be divided into four phases: inception, development and implementation, training and maintenance; that will provide a clear visibility on the development progress and will increase the confidence in final result. After each phase progress reports should be presented in Romanian and English languages.

### 6.1 Inception phase

The main scope of the inception phase is to do a thorough analysis of the project from different perspectives and verify and finalise the concept of the final product upon the Intranet System Concept document in Appendix 4. As part of the inception phase the implementing company is expected to process all project related documentation with a responsible person from the Ombudsperson’s Office and as a result the following list of tasks should be accomplished:

* Make an evaluation of the infrastructure system that best meets the project needs;
* Assess the technical specifications of the existing hardware (target platform) and, if considered necessary, specify enhancements to ensure its ability to satisfactorily host the Intranet System;
* Provide an evaluation of system architecture proposed for implementation;
* Agree on technologies to be used for implementation of IS;
* Elaborate the user experience and user interface design with visual models (mockups);
* Review the use cases and business requirements;
* Provide the concept for the mechanism to be user for reports and graphs creation in the system;
* Create the backlog and establish the priorities;
* Create the project roadmap.

During the inception phase the development company is expected to do an evaluation of the existing hardware equipment necessary to setup the system infrastructure. After the evaluation the company shall prepare and present the list of new equipment, if any, with the description of their technical specifications needed to be bought in order to build an efficient infrastructure system that meets performance and security requirements.

### 6.2 Development and implementation phase

The development and implementation phase can start immediately as the inception phase results are validated and all potential blocking issues are resolved.

During the development and implementation phase the implementing company is expected to present to product owner the progress reports and a demonstration of the functionalities developed every two or three weeks. The reports shall be written in Romanian language. The English translation of the reports should be provided.

The implementing company is responsible for the quality of the delivered product, however for a better communication and a more quick feedback it is recommendable that the implementing company configures a test environment and provides access to the responsible persons from the Ombudsperson’s Office that will have the possibility to do user acceptance testing.

In parallel with the development the IT Company should work with the responsible person from the IT department of the Ombudsperson’s Office and provide assistance in the setup of the infrastructure system for the IS .

By the end of development and implementation phase, the implementing company is expected to prepare and provide to the Ombudsperson’s Office the list of project related documentation specified in chapter 9.10 “Documentation and Training”. As part of the training phase, the Ombudsperson’s Office may require changes and updates to the initial version of the documentation, if that will be needed.

### 6.3 Training phase

At the end of the development and implementation phase the implementing company should provide a number of training sessions to a group of employees from the Ombudsperson’s Office. The purpose of the training sessions is to guide users, explain all functionalities of the final product and to clarify any questions that may appear, so at the end, the persons who attended the trainings, should be able to work efficiently with the system.

The format of different training sessions that should be offered by the implementing company is specified in chapter 9.10 “Documentation and Training”.

The entire training phase should be planned efficiently within a month, therefore the Ombudsperson’s Office will create the training schedule in advance and will provide it to engaged IT Company before the development phase ends.

The training session is recommendable to start before development and implementation phase is completed and to continue as part of maintenance phase.

### 6.4 Maintenance phase

The maintenance phase involves making changes to hardware, software, and documentation to support its operational effectiveness if needed. The implementing company is expected to provide a post development professional support for a period of 2 months from the day the final product is validated by the product owner and is delivered on production environment.

During the maintenance period the implementing company has the responsibility to make changes, improve system's performance, correct problems (software bugs), enhance security, or address user requirements that were not fulfilled during the development phase.

Any other requests, that were not previously discussed and are not present in the document of Business Requirements, cannot be addressed during this maintenance phase and should be reported internally to Project Manager for analysis.

The above described phases should be part of the work packages defined in the Appendix 2 - Tender Proposal Form, as this also is documented in the Appendix 5 - Planning.

## 7. Business model of the object of automation

The business model to be automated includes:

* The totality of tasks and processes that are at present defined at the Ombudsperson’s Office.
* The staff engaged at present in the activity of the Ombudsperson’s Office (including the staff in the territory)
* Other potential roles identified in the process of Intranet System’s implementation, which at present are not part of the Ombudsperson’s Office.

The Intranet system must create conditions of work for:

* Not less than 50 users in the central headquarters of the Ombudsperson’s Office.
* Not less than 50 users in the Ombudsperson’s Office branches in the territory or NPM employees.
* The number of petitions which should be processed: approximately 3500-4000 petitions a year.
* The number of documents of input-output: approximately 20-30 a day.

### 7.1 Business roles

#### 7.1.1. Intranet system actors

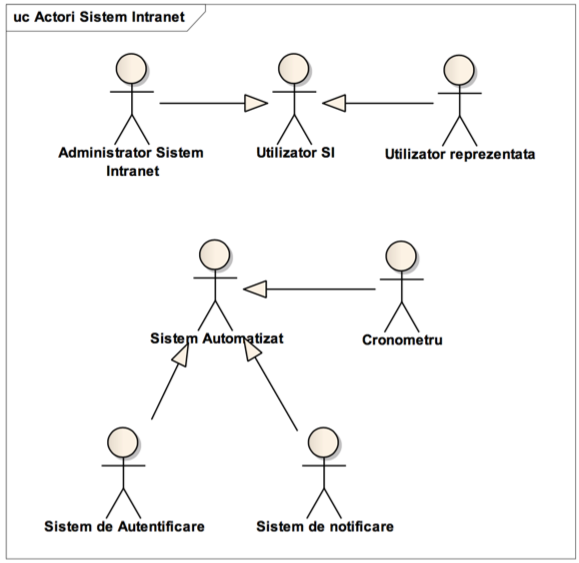


Fig.7.1.1. Intranet System Actors

|  |  |
| --- | --- |
| Actor | Description |
| **IS Manager** (Administrator Sistem Intranet) | |
|  | The person with management roles within the system at informational level, the system entity's management, the conferring of roles and rights. |
| **Chronometer** (Cronometru) | |
|  | A system actor that takes care of the lapse of time, receives orders and activities for execution at different moments of time in the future, regardless of the fact that these have periodical or onetime character.  The periodical character consists in the fact that the same action will take place at predefined intervals of time, while the activity with onetime character will be consumed at the defined moment of time.  The actor at the moment of lapse of time creates an event or rules and application. |
| **Automated System** (Sistem automatizat) | |
|  | The automated system is a virtual role that includes all system roles, which act automatically and are guided and initiated depending on certain events taking place in the system or after the lapse of time (in the case of Chronometer role) |
| **Authentication System** (Sistem de autentificare) | |
|  | A unique system that manages the users in the domain preserves the information about the system users, the personal data, and the methods of authentication. It is referred to as Domain Controller. |
| **Notification System** (Sistem de notificare) | |
|  | An automated system that aims at delivering messages to the Intranet system users by email or by creating messages in their workspaces. |
| **Branch User** (Utilizator reprezentanta) | |
|  | The user that accesses the Intranet System within the branches in the territory of the Ombudsperson’s Office or which are part of the NPM. The user can access the system by Internet connection. |
| **IS User** (Utilizator SI) | |
|  | The informational entity having a record in the system of users' management, has assigned two or more roles in the system with the access to other system functional objects. |

#### 7.2.1. Business roles

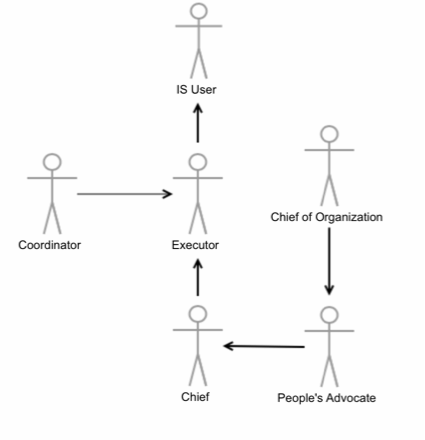


Fig.7.2.1. Business Roles

|  |  |
| --- | --- |
| Role | Description |
| **People’s Advocate** (Avocatul Poporului) | |
|  | The person in charge with the ability to give notice of documents, approve documents in the final version, examine and investigate petitions, issue orders and dispositions. |
| **Chief** (Conducator) | |
|  | The chief is the role entitled to view all activities and entities in the subdivision under control. It has extended rights to view and intervene with the subdivision's process of work, and it is also entitle to manage the workspaces created in the subdivision under control. |
| **Chief of the Organization** (Conducator Organizatie) | |
|  | The person that is entitled to give final approval to the decisions taken in the organization that are connected directly to the administrative positions. |
| **Coordinator** (Coordonator) | |
|  | The person with extended tasks aiming at the approval of certain actions fulfilled by an Executor. The coordinator inherits all Executor's tasks. |
| **Executor** (Executor) | |
|  | The IS user that deals with the execution of a task or fulfills any action in the System on a document, the modification of the properties of an entity, the addition of a new entity.  The executor may be part of different subdivisions and departments within the Ombudsperson’s Office. |

#### 7.3.1. Services

|  |  |  |
| --- | --- | --- |
| Nr. | Name of the Service | Notes |
| 1. | Intranet | The unique point of entry in the Intranet system. It is preserved as a web application with the internal use available for all Ombudsperson’s Office employees in the central office and those working in the branches in the territory and the NPM. Authorization restrictions will be applied when accessing certain Intranet parts. |
| 2. | Dossier Management  (Folder Management) | The service allowing to the users the management of electronic dossiers in a centralized manner. |
| 2.1. | Dossier versioning control | After each document’s modification (out of the system), on upload the system will store document as a new control version and will allow the posting of comments regarding the fulfilled changes. |
| 2.2. | Workflow | A flexible mechanism that will provide the ability of definition of the steps / persons that must transmit the document for examination, to add modifications, notes, change status and archive the dossier when necessary. |
| 2.3. | Search and identification | Allows to the users the localization of metadata, classes, sub-files, volumes and records. |
| 2.4. | Presentation | The system must be capable to present the contents of the classes, files, sub-files, volumes, documents or records. |
| 2.5. | Referencing | The system must allow to the users the processing, extraction, referencing and the use of entities. |
| 3. | Data Capture and Statement | The capture of the information (data, metadata, and documents, in some cases) and saving it in the system according to the classification scheme. |
| 3.1. | Files classification and organizing scheme | Allow the storage of an electronic record together with other data ensuring its context, by defining the method of organization of electronic data into electronic files and the relations between the files. |
| 3.2. | Retention and destruction | Defining the duration of system data life and the method of their destruction. |
| 4. | Tasks management | The service that will treat the non-finished processes as tasks assigned to the staff. |
| 4.1. | Monitoring the modification of statutes and notifying the users regarding the tasks statutes’ modification | The system will record any change of the task statute, to help the superiors to monitor its progress, The superiors will be notified at each modification of the statute. |
| 5. | Users management | The security service defining the authorized staff, their credentials and the levels of access. |
| 6. | Email | Helps the users to manage transparently and efficiently large email amounts, web forms and to send documents (as messages or attachments) within the Ombudsperson’s Office and/or outside this. |

## 

## 8. Functional Requirements for the System

The Intranet System is meant to offer a single access point to the common workspace. The Intranet offers a web interface accessible to ALL Ombudsperson’s Office employees.

The Intranet System is also available to authorized employees situated in other offices of the Ombudsperson’s Office and the branches in the territory by Internet connection. The available information will be meant for the internal use and confidential security levels, usually templates, documents and document projects that will later become public.

Besides the web interface, the Intranet will offer a way of access to the file systems by means of a LDAP protocol to allow the employees the access as they got used to – by creating and storing files on a file service.

### 8.1. System’s Functional Model

#### 8.1.1. UC 01 Intranet System's Use

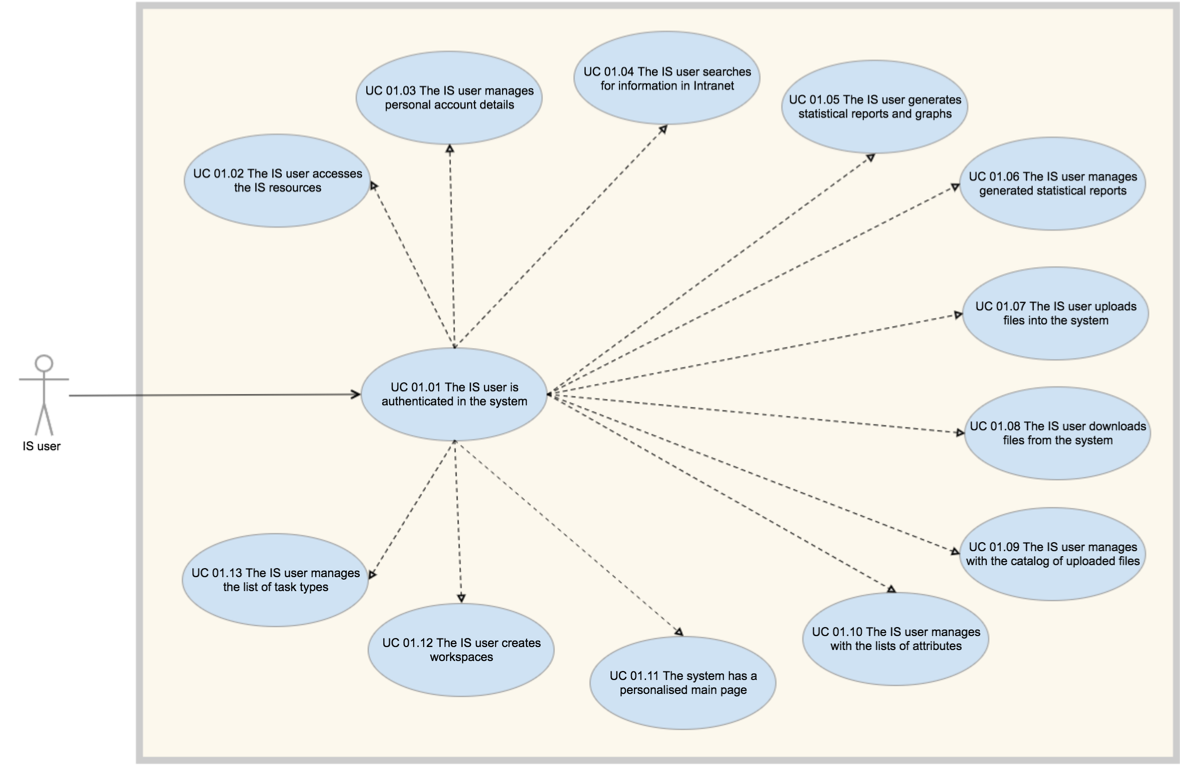


Fig. 8.1.1.1 Intranet System’s Use

|  |  |
| --- | --- |
| Use Case | Description |
| **UC 01.01 The IS user is authenticated in the system** | |
|  | **Actor:** IS user  **Aim:** Authentication in the system aiming at the acknowledgment of a person and the fulfilment of certain activities and tasks.  **Constraints:**  *Precondition*: The user must have a prior record in the system  *Postcondition*: The user accesses the informational resources within the IS  *Basic script:* **Authentication in the Intranet System**   1. The IS user opens an Internet Browser accessible in the system 2. The IS user types the Intranet System address (ex. [https://intranet](http://intranet)) 3. The user enters the username and the domain password and presses the button for the confirmation of the inserted information 4. The Authentication System validates the user name and the password in the Domain repository 5. The Authentication System records the information about the system login event 6. The IS User is redirected to the IS Main Page   *Alternative Script:* **5a. The Authentication System does not validate the entered credentials**.   1. The system makes a record about the incident 2. The system informs the user about wrong credentials 3. The system requires repeated insertion of the login information   *BR 1-01 The Intranet System is accessed from any computer within the Ombudsperson’s Office*  The user may get access to the Intranet system (with the use of the personal authentication) from any computer within the organization including the offices of the branches  *BR 1-02 The Intranet System has a unique Authentication System*  The information about the Intranet System's users must be kept by an external system (Domain Controller) to preserve the user's uniqueness in the system even if different sub-systems need additional authentication and identification  *BR 1-03 The Intranet System must be accessible via Web Browser*  *BR 1-04 The Main Page must be personalized*  The Main Page of the Intranet System must be personalized depending on the role of the IS User that accesses this page and on his/her access rights. Such a person must view only those elements of the page to which s/he would further have access for viewing. |
| **UC 01.02 The IS user accesses the IS resources** | |
|  | **Actor:** IS user  **Aim:** Getting access to the informational resources within the Intranet System from the main Interface or by the transmission of its reference through a communication system (emails) or accessing it by means of some references from certain documents.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The User must have access rights to this informational resource  *Postcondition:* The informational resource is undertaken by an application within the soft package installed on the IS User's computer.  *Basic script:* **The IS User accesses the informational resource**   1. The Intranet System checks the access rights to the system resources 2. The IS user accesses the reference to the informational resource allowed for the level of his access. 3. The Intranet system renders to the user the informational resource. 4. The Informational Resource is overtaken by an application on the user’s computer setup to process this type of informational objects.   *Alternative Script:* **1a. The User has no access rights on the resource**   1. The Intranet System does not display resources’ download option   *BR 1-05 The Intranet System resources must have different access options*  The Intranet System Resources have as access options:   * Resource download * Resource upload * Resource delete   A resource (document) can be visualised and edited on the user’s computer only. |
| **UC 01.03 The IS user manages personal account details** | |
|  | **Actor:** IS user  **Aim:** IS user accesses the personal account area to view and update the personal details.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Basic script:* **The IS User updates personal details**   1. The user accesses the personal account page 2. The user edits the personal details 3. The system validates updated details 4. The system saves updated values 5. The system records the information about the account update event   *Alternative Script:* **3a. The system does not validate introduced details**   1. The Intranet System shows a warning message so user may correct the information.   *BR 1-06 IS user may update only his account data* ‐  The email cannot be edited from account page and it is read only.  *BR 107 IS user has read access to the account pages of all IS users.* |
| **UC 01.04 The IS user searches for information in Intranet** | |
|  | **Actor:** IS user  **Aim:** Searching the informational resources within the Informational System according to certain searching criteria.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Postcondition:* The results of the search must contain metadata of the informational resource as well.  *Basic script:* **The IS User searches for information in the Intranet system**   1. The IS User inserts the keywords in the search box 2. The IS User selects the area in which the search will be executed 3. The IS user presses the search button 4. The Intranet System gets access to the database and fulfils the search 5. The Intranet System gives the list of found resources   *BR 1-08 The search results are displayed in a format of a table and divided into pages*  *BR 1-09 The search results can be ordered by columns.*  *BR 1-10 The search results can be exported in a CSV file.* |
| **UC 01.05 The IS user generates statistical reports and graphs** | |
|  | **Actor:** IS user  **Aim:** Generate statistical reports based on set criteria and export results in the format of a graph or table.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition:* The User has access to the reports mechanism  *Basic script:* **The IS User generates statistical reports**   1. The user accesses the page for generating reports 2. The user selects the area on which the report should be generated 3. The user follows instructions to create a query using AND, OR and NOT logical operators 4. The user specifies start and end period for the report 5. The user presses button to generate the report 6. The system validates the report generation form 7. The system displays the report on the page in a table format 8. The system records in events log information about generated report 9. The user selects the format of graphic view from predefined list (e.g. pie chart, 2D columns, lines) 10. The user selects the criteria for the chart to be generated 11. The system displays the report in a chart view on the page 12. The user exports the report in CSV format 13. The user exports the graphical presentation of the report in the PNG/JPG format. 14. The user saves the report into the system to the catalog of reports. The table and chart if generated.   *Alternative Script:* **1a. The User has no access rights on the resource**   1. The Intranet System restricts user access to the reports mechanism   *BR 1-11 The system has a built-in mechanism for generating reports*  A statistical report should communicate clearly the criteria used for its generation, then to present the data collected and statistics drawn from that data. For example, for a case under processing (a dossier object) a statistical report may contain the number of open, in progress and completed tasks. As input parameters to the running of reports (depending on the type of the entity) there may be:   * Period of time (Registration Date) * Period of time (Date of last resolution) * Registration office (central office or branches in the territory) * Lawyer (person) * Executor (person) * Executor(Ombudsperson’s Office department or subdivision) * Entity status (registered, assigned, examined, etc) * Resolution ( to be examined, taken off the role, rendered according to the competence) * Topic (according to the list of topics approved by the Ombudsperson’s Office) * Notified body (according to the nomenclature of state institutions within * the Ombudsperson’s Office)   The reports may be run with the use of a single parameter and by the accumulation of several conditions by means of "AND/OR" conditions. |
| **UC 01.06 The IS user manages generated statistical reports** | |
|  | **Actor:** IS user  **Aim:** The statistical reports are saved in the system in the catalog of the reports available for view and edit to users with appropriate access permission.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition:* The User has access to the catalog of statistical reports  *Basic script:* **The IS User manages statistical reports**   1. The user accesses the catalog of reports 2. The user updates report description 3. The system records in events log information about report edit operation   *Alternative Script:* **2a. The User has no access rights to edit the report**   1. The Intranet System restricts user access to edit the report 2. User view the report 3. User downloads the report   *BR 1-12 The user is able to add a description to a report saved into catalog of the reports*  To have a better understanding of a generated report the user should be able to add a description to the report. Basically a user should have edit access to any of reports generated on his account and a manager user should have edit access to all reports. |
| **UC 01.07 The IS user uploads files into the system** | |
|  | **Actor:** IS user  **Aim:** The Intranet System is defined as the totality of information storage.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Basic script:* **The IS User uploads files to the system**   1. The user accesses the system entity to which he wants to add an attachment 2. The user selects upload option 3. The user selects one or multiple files from local storage 4. The user presses upload button 5. The system validates the file extension and file size 6. The user add a comment to the uploads 7. The user presses confirm option to complete the upload 8. The system uploads the file and generates the download link (attachment link) 9. The system records in events log information about upload operation   *Alternative Script:* **2a. The User has no access to upload option**   1. The Intranet System restricts user access to upload option   *Alternative Script:* **5a. The system does not validate the uploads**   1. The system informs about upload restriction 2. The user can do another selection for the files or can abort the operation   *Alternative Script:* **7a. The User aborts the operation**   1. Files are not uploaded to the system 2. Upload form is closed   *BR 1-13 The user is able to do single or multiple files upload to the system*  *BR 1-14 The system validates the uploads by file extension and by size*  The list of supported file extensions to be confirmed.  The max size for a file to be confirmed.  The system should not overwrite files with the same title if exists. |
| **UC 01.08 The IS user downloads files from the system** | |
|  | **Actor:** IS user  **Aim:** The IS user downloads files from the system for view and edit operations.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Basic script:* **The IS User downloads files from the system**   1. The user accesses system entity that contains attachments 2. The user accesses download link 3. The file is downloaded on user’s computer   *Alternative Script:* **2a. The User has no access to download attachments**   1. The Intranet System restricts user access to download option   *BR 1-15 The user should be able to download files from the system* |
| **UC 01.09 The IS user manages with the catalog of uploaded files** | |
|  | **Actor:** IS Manager user  **Aim:** The uploaded files should be structured in catalog for an easy management  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The User must have appropriate access permission to the catalog of uploads.  *Basic script:* **The IS User manages the uploaded files**   1. The user accesses the catalog of uploaded files 2. The user searches files by system entity to which files were attached 3. The user filters results by columns 4. The user downloads a file on user’s computer 5. The user access delete option for a file 6. The confirms delete operation 7. The system records the delete action in the events log 8. The system changes download link with a text saying “File removed” in the related system entity. The entity to which file was attached.   *Alternative Script:* **1a. The User has no access to the catalog of uploaded files**   1. The Intranet System restricts user access to the catalog   *Alternative Script:* **5a. The User has no access to delete file**   1. The Intranet System restricts user access to delete option   *BR 1-16 The IS user should be able to view and manage the catalog of uploaded files*  Basically not all users that have read access to the catalog should have access to delete files from the system. |
| **UC 01.10 The IS user manages with the lists of attributes** | |
|  | **Actor:** IS Manager user  **Aim:** The IS user manages with the lists of attributes used by the users to create dossiers into the system.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The User must have appropriate access permission to the lists of attributes  *Basic script:* **The IS User manages the attributes**   1. The user accesses the menu of attributes 2. The user opens a specific list of attributes 3. The user creates a new attributes 4. The system validates the attribute fields 5. The system records the create action in the events log 6. The user removes an attribute 7. The system check if attribute is not in use by an dossier in the system 8. The system records the delete action in the events log   *Alternative Script:* **3a. The User has no permission to create attributes**   1. The Intranet System restricts user access to create option 2. The user has only read access   *Alternative Script:* **7a. The User has no access to delete file**   1. The IS finds a relation of the attribute in the system 2. The IS informs user that attribute is used in the system 3. Attribute is not removed   *BR 1-17 The IS user is able to manage the lists of attributes in the system*  The attribute element represents the data that is used in the system by users to create other entities i.e. dossiers. Attributes are selected within a form using a drop down list element. The list of attributes to be confirmed with the final format of dossier and other entities in the system. |
| **UC 01.11 The system has a personalised main page** | |
|  | **Actor:** IS user  **Aim:** On login IS redirects user to Main Page that reflects the information related to the current account.  **Constraints:**  *Precondition*: The User has an active account in the system.  *Basic script:* **The IS User navigates through Main Page**   1. The User authenticates in the system. 2. The user accesses personal account page 3. Personal account page is opened   *Alternative Script:* **2a. The User accesses a help page**   1. Help page is displayed   *Alternative Script:* **2b. The User accesses a task**   1. Task is displayed   *Alternative Script:* **2c. The User accesses a dossier**   1. Dossier is displayed   *Alternative Script:* **2d. The User accesses a working group**   1. Working group is displayed   *BR 1-18 The Main Page must be personalized*  The main page (dashboard) of the IS should offer a clear vision of main components/areas of the system, like: reference to assigned tasks, to Help pages, quick access to search, access to system menu and to User Account menu. Some of Main page areas will be automatically adjusted to display data related to logged in user i.e. assigned tasks or the list of working groups, dossiers. The final design and format of home page should be established during the development phase once the most of the functionalities will be implemented |
| **UC 01.12 The IS user creates workspaces** | |
|  | **Actor:** IS user  **Aim:** The creation of workspaces for the storage and accessing in common of the  informational resources  **Constraints:**  *Precondition:* The User must be authorized within the Intranet System  *Precondition:* The User must have permission to create workspaces in that site  *Postcondition:* The system creates workspaces and assures the full rights to the users  *Basic script:* **The IS User creates workspaces**   1. The user accesses the Workspaces menu 2. The user selects the option to create new workspace 3. The user fulfils the set of metadata of the new workspace (title, description, references on the page of the parent site, other metadata) 4. The user add members to the new workspace 5. The user presses the button confirming the intent to save the information 6. The Intranet System saves the newly created workspace 7. The Intranet System notifies all members about the creation of a new workspace   *Alternative Script:* **2a. The user has no permission to create workspaces**   1. The Intranet System restricts user access to create option   *BR 1-19 The system must have a mechanism/interface for the creation of workspaces*  The new workspaces are necessary for the organization of the common work on a problem or the assignation of an ad‐hoc working group, such as setting out the opinion on certain problems, creating informational notes, delegation, conference etc. |
| **UC 01.13 The IS user manages the list of task types** | |
|  | **Actor:** IS user  **Aim:** A IS user with appropriate access permission may update the list of task types to be used in the system when a new task is created.  **Constraints:**  *Precondition:* The User must be authorized within the Intranet System  *Precondition:* The User must have permission to create task types  *Basic script:* **The IS User add a new task type**   1. The user accesses the Task Types list 2. The user selects the option to create new task type 3. The user fulfils the set of metadata of the new task type (title, description, other metadata) 4. The user presses the button confirming the intent to save the information 5. The Intranet System saves the newly created task type 6. The Intranet System displays the list of task types   *Alternative Script:* **2a. The user has no permission to create task types**   1. The Intranet System restricts user access to create option   *BR 1-20 The IS user must have possibility to manage the list of task types that are used in the system when a new task is created* |

#### 8.1.2. UC 02 Business Process

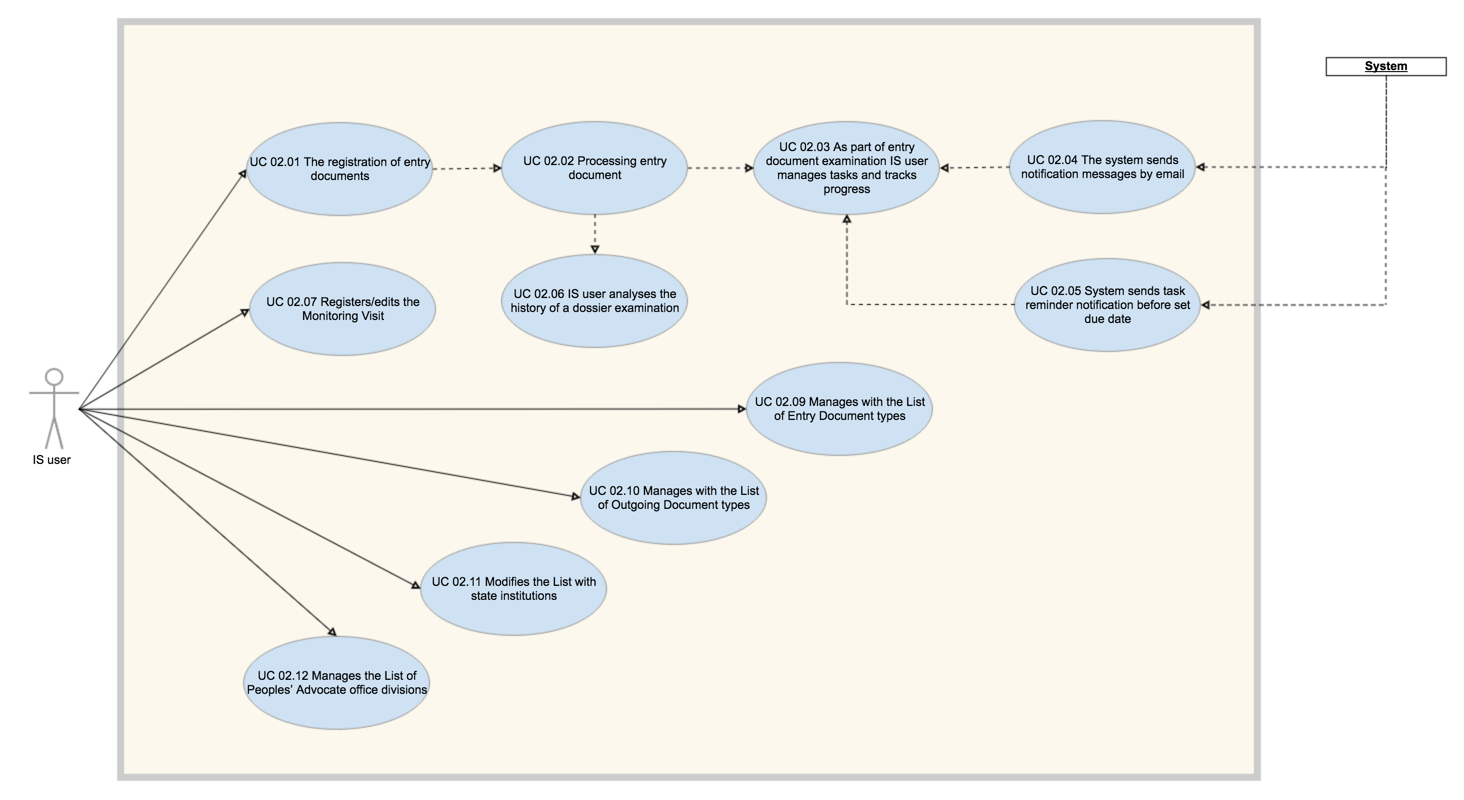


Fig. 8.1.2.1 Business Process

|  |  |
| --- | --- |
| Use Case | Description |
| **UC 02.01 The registration of entry documents** | |
|  | **Actor:** IS user  **Aim:** The registration of entry document for examination within the The Ombudsperson’s Office.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Basic script:* **The IS User creates new dossier and specifies the entry document type**   1. The user accesses the catalog of dossiers 2. The user creates a new dossier 3. The user specifies the type of entry document 4. The user uploads the entry document to the dossier 5. The user completes in the form of evidence and control of dossier 6. The IS user saves the dossier 7. The system validates the dossier form 8. The system saves the dossier and shows the list of dossiers   *Alternative Script:* **1a. The User does not have permission to register a new petition**   1. The Intranet System restricts user access to create option   *Alternative Script:* **7a. The system does not validate the petition form**   1. The system highlights the fields that were not validated 2. The user updates the data in the fields and resubmit the form   *BR 2-01 The user is able to register entry document into the system.*  The basic fields in the registration card are:  - Petitioner  - Type of entry document, number of files (unique)  - Petitioner, data, cover letter’s index  - Data, entry index  - Short petition’s content  - Executor  The format of Entry document number can be composed from one or two digits and should be unique in the system.  *BR 2-02 The user creates a dossier in the system for every new entry document*  Dossier (or Folder) - a representative system object that has the scope of tracking within the system the life cycle of any request appeared from a person whose rights and freedoms have been infringed, reported to Ombudsperson.  The management of a dossier is represented by a list of activities that are taking place in the institution, that need to be tracked within the intranet system.  A high level representative dossier registration and processing action flow diagram is presented in Fig 7.1.2.2. |
| **UC 02.02 Processing entry document** | |
|  | **Actor:** IS user  **Aim:** The examination of entry document within the Ombudsperson’s Office. In the entry document process all branches of the Ombudsperson’s Office in the territory and the NPM are involved.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The entry document registered in the system (UC 02.01)  *Basic script:* **The IS users process entry document**   1. The user opens the menu of dossiers 2. The user searches for the dossier 3. The user opens the dossier 4. The user opens the assigned task and set the status to in progress 5. The user performs document’s examination (outside of the system) 6. The user updates the dossier with comments 7. The user attach to the dossier any number of deeds of reactions specifying for each one the type of the document from a predefined list. 8. The IS user sets task in completed state 9. The system sends notifications about dossier update to all dossier’s members 10. The dossier manager user creates a task and assigns to IS user to continue examination. 11. The system notify the assigned user about created task 12. Upon all tasks are completed manager user decides on the petition resolution.   *BR 2-03 The user is able to add comments to the dossier*  *BR 2-04 The deeds of reaction may be assigned to dossiers*  A deed of reaction may be assigned to one or several entities in the system. For example, a deed of reaction solves several cases (petitions) addressed to the Centre. The User must have the possibility to connect this deed with several entities in the system. This will be done when creating references between, for example, a petition and an outgoing/entry document.  *BR 2-05 The outgoing documents may be assigned to a dossiers*  When outgoing document is assigned to the dossier the user must specify the type of outgoing document, to fill in the form all mandatory fields, and to provide a comment.  The format of Outgoing document number can be composed from one, two or three digits and should be unique in the system.  *BR 2-06 The system saves the history of actions taken to fulfill a dossier examination.* |
| **UC 02.03 As part of entry document examination IS user manages tasks and tracks progress** | |
|  | **Actor:** IS user  **Aim:** As part of a dossier investigation and analysis work an intranet user creates tasks, assigns to other IS users and sets due date.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The entry document registered in the system (UC 02.01)  *Basic script:* **IS user create tasks, set due date and add assignees**   1. IS user accesses the dossier 2. IS user accesses create new task option 3. IS user introduces all required data into the form: assignees, title, description, due date etc. 4. IS user submits the task 5. IS validates the form 6. IS sends a notification to assigned user 7. IS system records the event to the logs 8. Task is created and set in Open state and has a visibility into dossier. 9. If assignees are not members of the dossier they are automatically added by the system.   *BR 2-07 The user creates tasks that are directly related to the dossier*  *BR 2-08 One or several persons may be appointed as task Executors*  One or several persons may be appointed as Executor.  In this case the notification system will send the message to all persons mentioned in the list.  *BR 2-09 The user sets due date for task to be completed* |
| **UC 02.04 The system sends notification messages by email** | |
|  | **Actor:** Intranet System  **Aim:** The Intranet System offers a mechanism of quick and in time notification of users involved in a process. The IS notification center is configured to send automatically notifications with details to related IS users.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Basic script:* **IS sends notifications**   1. IS user creates a new dossier 2. IS user add a new member to the dossier   2.1 System sends notification to new member   1. IS user creates a new task   3.1 System sends notification to task assignees   1. IS user changes the status of assigned task   4.1 System sends notification to dossier owner   1. IS user adds a comment to the dossier   5.1 System sends notification to all members of the dossier   1. IS user updates the dossier   6.1 System sends notification to all members of the dossier   1. IS user changes the status of the dossier   7.1 System sends notification to all members of the dossier  *BR 2-10 The Intranet System must have a notification system.*  The notification system will send the messages regarding the undergoing changes during the works in the petitioning process, the message Template and the list of actors, to whom the messages will be delivered, will be defined at the moment of implementation. |
| **UC 02.05 The system sends task reminder notification before set due date** | |
|  | **Actor:** Intranet System  **Aim:** The IS sends reminder notification N number of days before task due date in order to ensure assignee is aware about upcoming deadline.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The entry document registered in the system (UC 02.01)  *Precondition*: The dossier is created (UC 02.01)  *Precondition:* Task is created (UC 02.03)  *Basic script:* **IS sends reminder notification N days before set due date**   1. IS verifies the task is not in completed status 2. IS verifies the current date is the N days before due date 3. IS system verifies if the reminder was not send already 4. IS system sends a reminder notification to task owner and task assignees   *Alternative Script:* **1a. Task is in completed status**   1. IS does not send the reminder notification   *Alternative Script:* **2a. Current date is not the N days before due date**   1. IS does not send the reminder notification   *Alternative Script:* **3a. The reminder was sent one time**   1. IS does not send the reminder notification   *BR 2-11 The system sends reminder notification for a task N days before due date*  The N days before due date is a configurable option that by default must be 3 days. In case the task due date is less days than days specified for the reminder, then no reminder notification will be sent. |
| **UC 02.06 IS user analyses the history of a dossier examination** | |
|  | **Actor:** IS user  **Aim:** The IS user analyses the history records of actions done to complete the examination process of an entry document.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The entry document is registered in the system (UC 02.01)  *Precondition*: The dossier is created (UC 02.01)  *Basic script:* **IS user open the history of a dossier**   1. IS user accesses menu of Dossiers 2. IS user searches for a dossier 3. IS user opens a dossier from the list 4. IS user accesses the history records of the dossier 5. IS user is able to view the summary of actions done during examination process with date, hour, by whom and other info.   *Alternative Script:* **3a. User is not member of the dossier**   1. The system informs the user that he is not member of this dossier and has no access to open it   *BR 2-12 The IS saves the history of a dossier processing*  The history module will give more informative notes about the phases through which the dossiers were passed.  History details to be considered:   * For every document upload to the dossier should require a comment to be added, document type to be indicated and in history will save all available administrative metadata (date and time, user, file size etc.) * For every completed task the system will log in the history: task assignee name, date and hour, task status and other info that may be considered as important.   Uploaded documents has an unique download link and can be accessed by any user that is member of working group and by IS user with global access permission. |
| **UC 02.07 Registers/edits the Monitoring Visit** | |
|  | **Actor:** NPM Executor  **Aim:** Registration and editing of monitoring visits in the state institutions  **Constraints:**  *Precondition:* The User must be authorized in the system  *Precondition:* The User must have the necessary rights  *Postcondition:* The system registers the monitoring visit  *Basic script:* **The User registers the monitoring visit**   1. The User accesses the registration/editing function of the monitoring visit 2. The system displays the registration of the monitoring visit 3. The User fills in the fields in the form 4. The User presses the visit saving button 5. The system checks how correct the form has been filled in 6. The system saves the visit in the database 7. The system displays the list of monitoring visits   *Alternative Script:* **6a. The system does not validate the inserted information**   1. The system displays the form with the information inserted previously and the list of errors 2. The User corrects the mistakes 3. Continues by executing the clause 4 in the basic script   *BR 2-13 The deeds of reaction may be assigned to one or several entities*  A deed of reaction may be assigned to one or several entities in the system. For example, a deed of reaction solves several cases (petitions) addressed to the Centre. The User must have the possibility to connect this deed with several entities in the system. This will be done when creating references between, for example, a petition and an outgoing/entry document.  The lists have a paging function (initially 20 inscriptions per page) with the possibility to modify this value (e.g. 20 , 50 , 100) |
| **UC 02.09 Manages with the List of Entry Document types** | |
|  | **Actor:** Manager User  **Aim:** IS user can add a new Entry Document type for a use in the system  **Constraints:**  *Precondition:* The User must be authorized in the system  *Precondition:* The User must have the rights necessary to modify the list of entry documents  *Postcondition:* The User modifies the list of entry document types  *Basic script:* **The User adds a new entry document type**   1. The user opens the list of entry document types 2. The system displays the list of existing entry document types 3. The User chooses the function of adding a new entry document type 4. The system displays the form for the registration of a new entry document type 5. The User fills in the fields in the form 6. The User confirms saving the data in the form 7. The system checks if the information and duplicity has been filled in 8. The system saves the data in the database 9. The system returns the list of entry documents types   *Alternative Script:* **3a. The User chooses the functionality of editing an already existing entry document type**   1. The system displays the form with the entry document type details 2. The User makes the necessary modifications in the data about the entry document type 3. Continues by executing the clause 6 in the basic script   *Alternative Script:* **7a. The system does not validate the correctness of the information**   1. The system displays the form filled in with the inserted information and the list of errors 2. The User corrects the information 3. Continues by executing clause 6 in the basic script   The base list of entry documents types (provided in Romanian):   * Cerere (Petitie): cerere scrisa / cerere verbala / sesizare din oficiu. * Scrisoare oficiala * Scrisoare simpla * Cerera a cetatenilor * Proces verbale * Nota informativa * Raport special * Interpelare * Raspuns * Informatie * Sesizare * Proiect de lege/Hotarire de Guvern   The lists have a paging function (initially 20 inscriptions per page) with the possibility to modify this value (e.g. 20 , 50 , 100) |
| **UC 02.10 Manages with the List of Outgoing Document types** | |
|  | **Actor:** Manager User  **Aim:** IS user can add a new Outgoing Document type for a use in the system  **Constraints:**  *Precondition:* The User must be authorized in the system  *Precondition:* The User must have the rights necessary to modify the list of outgoing documents  *Postcondition:* The User modifies the list of outgoing document types  *Basic script:* **The User adds a new outgoing document type**   1. The user opens the list of outgoing document types 2. The system displays the list of existing outgoing document types 3. The User chooses the function of adding a new outgoing document type 4. The system displays the form for the registration of a new outgoing document type 5. The User fills in the fields in the form 6. The User confirms saving the data in the form 7. The system checks if the information and duplicity has been filled in 8. The system saves the data in the database 9. The system returns the list of outgoing document types   *Alternative Script:* **3a. The User chooses the functionality of editing an already existing outgoing document type**   1. The system displays the form with the outgoing document type details 2. The User makes the necessary modifications in the data about the outgoing document type 3. Continues by executing the clause 6 in the basic script   *Alternative Script:* **7a. The system does not validate the correctness of the information**   1. The system displays the form filled in with the inserted information and the list of errors 2. The User corrects the information 3. Continues by executing clause 6 in the basic script   The base list of outgoing documents types (provided in Romanian):   * Interpelare/Solicitare * Raspuns prealabil/definitiv * Demers * Aviz * Sesizare * Cerere de chemare in judecata/concluzie –iesire * Propunere de modificare a legislatiei * Acord de conciliere * Proces verbal   The lists have a paging function (initially 20 inscriptions per page) with the possibility to modify this value (e.g. 20 , 50 , 100) |
| **UC 02.11 Modifies the List with state institutions** | |
|  | **Actor:** Manager User  **Aim:** Modification of the list with state institutions that will be monitored  **Constraints:**  *Precondition:* The User must be authorized in the system  *Precondition:* The User must have the rights necessary to modify the list of institutions  *Postcondition:* The User modifies the list of state institutions  *Basic script:* **The User modifies the list with state institutions**   1. The User accesses the function of modifying the list of institutions 2. The system displays the list of state institutions 3. The User chooses the function of adding a new institution 4. The system displays the form for the registration of the institution 5. The User fills in the fields in the form 6. The User confirms saving the data in the form 7. The system checks if the information and duplicity has been filled in 8. The system saves the data in the database 9. The system returns the list of registered institutions   *Alternative Script:* **3a. The User chose the functionality of editing an already existing institution**   1. The system displays the form with the institution’s details 2. The User makes the necessary modifications in the data about the institution 3. Continues by executing the clause 6 in the basic script   *Alternative Script:* **7a. The system does not validate the correctness of the information**   1. The system displays the form filled in with the inserted information and the list of errors 2. The User corrects the information 3. Continues by executing clause 6 in the basic script   The lists have a paging function (initially 20 inscriptions per page) with the possibility to modify this value (e.g. 20 , 50 , 100) |
| **UC 02.12 Manages the List of Ombudsperson’s office divisions** | |
|  | **Actor:** Manager User  **Aim:** Modification of the list with state institutions that will be monitored  **Constraints:**  *Precondition:* The User must be authorized in the system  *Precondition:* The User must have the rights necessary to modify the list of Ombudsperson divisions  *Postcondition:* The User modifies the list of divisions  *Basic script:* **The User modifies the list Ombudsperson’s office divisions**   1. The User accesses the list of Ombudsperson divisions 2. The system displays the list of existing divisions 3. The User chooses the function of adding a new office division 4. The system displays the form for the registration of the division 5. The User fills in the fields in the form 6. The User confirms saving the data in the form 7. The system checks if the information and duplicity has been filled in 8. The system saves the data in the database 9. The system returns the list of registered Ombudsperson divisions   *Alternative Script:* **3a. The User chose the functionality of editing an already existing Ombudsperson’s office division**   1. The system displays the form with the division’s details 2. The User makes the necessary modifications in the data about Ombudsperson’s office division 3. Continues by executing the clause 6 in the basic script   *Alternative Script:* **7a. The system does not validate the correctness of the information**   1. The system displays the form filled in with the inserted information and the list of errors 2. The User corrects the information 3. Continues by executing clause 6 in the basic script   Each user in the system will require to have specified from a dropdown list Ombudsperson’s office division he belongs to (Relation one to one).  Organizational diagram presented in Fig 7.1.2.3.    The lists have a paging function (initially 20 inscriptions per page) with the possibility to modify this value (e.g. 20 , 50 , 100) |

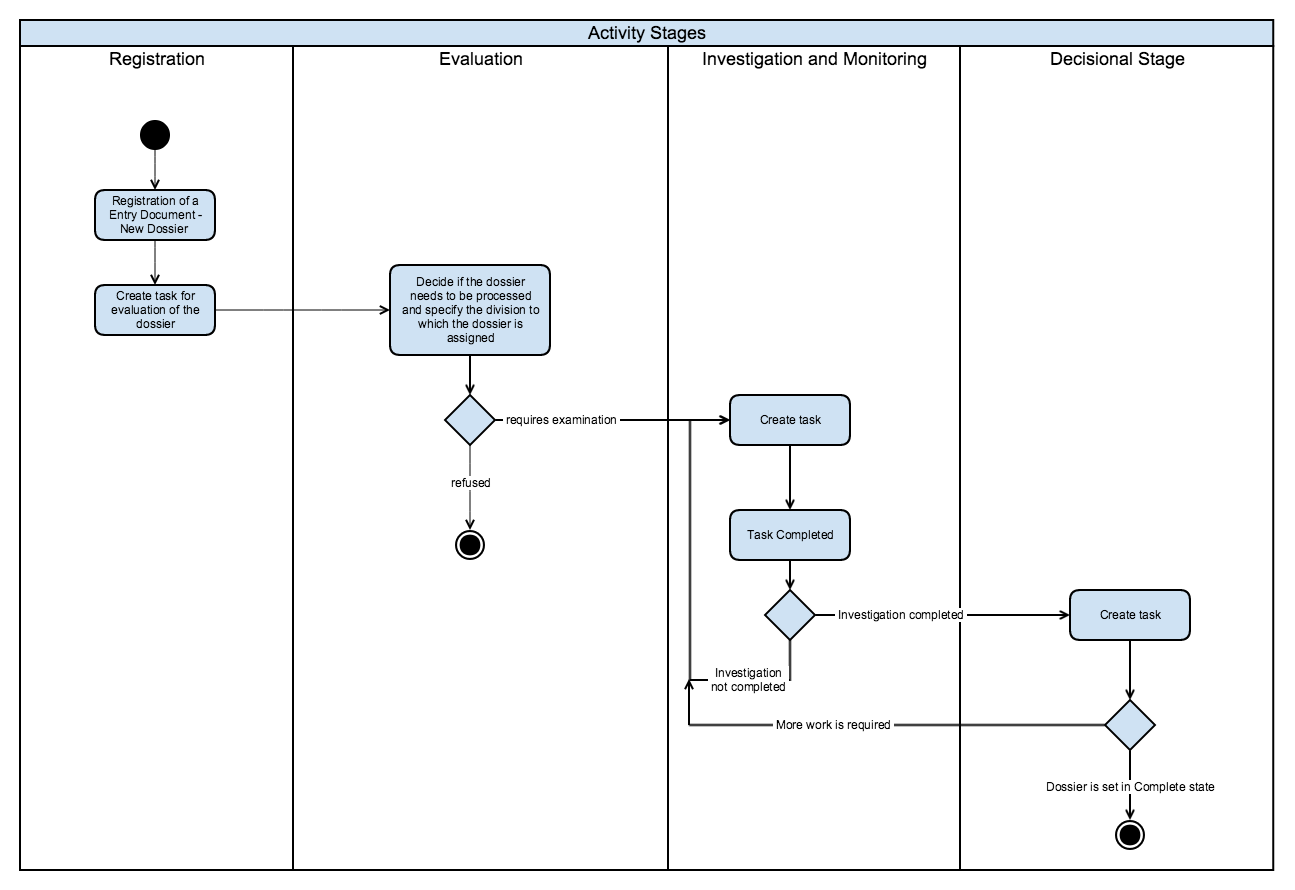


Fig. 8.1.2.2 Dossier registration and processing activity flow diagram by stages.

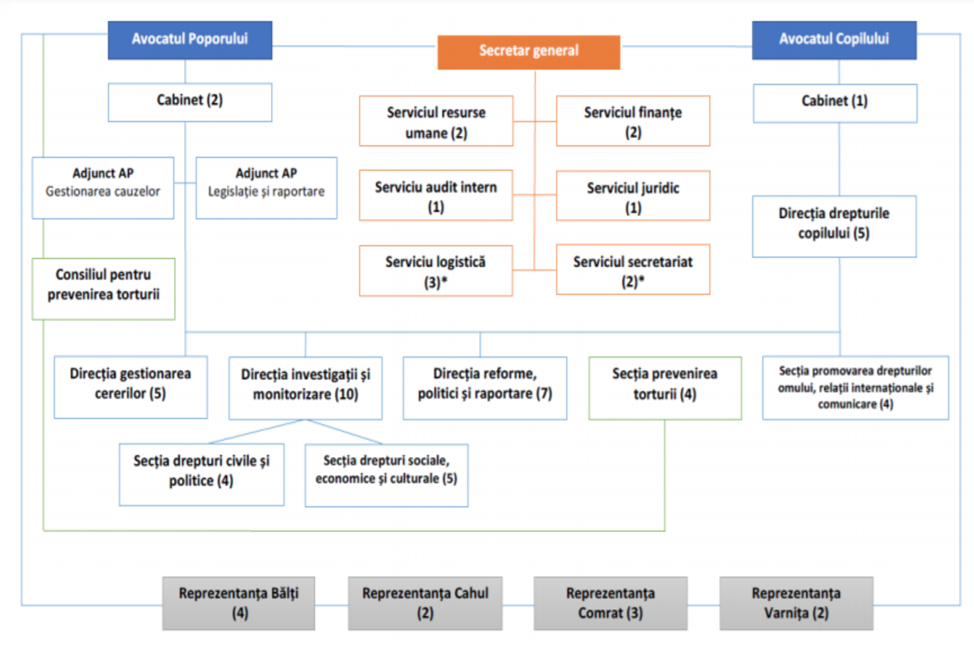
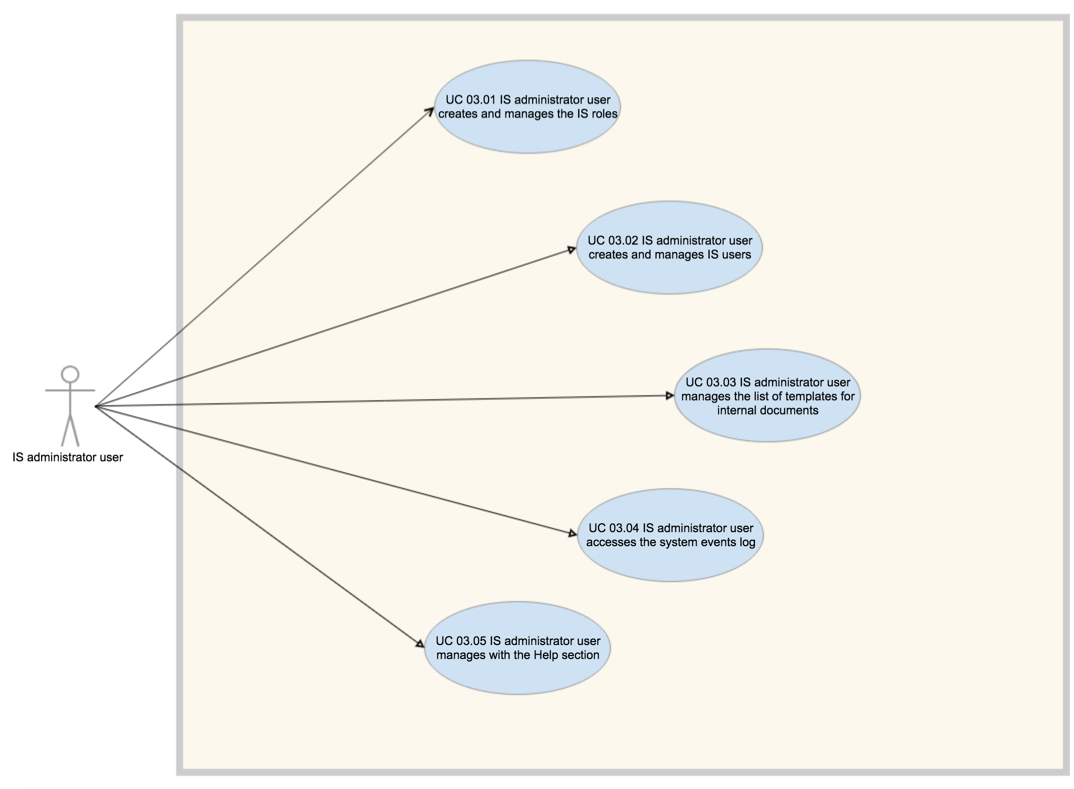


Fig. 8.1.2.3 Ombudsperson’s Office Organisational Diagram

The Organizational structure of the institution may change in years thus the system should offer the possibility to edit or add a new division when it is required (UC 02.12).

#### 8.1.3. UC 03 Intranet System Administration

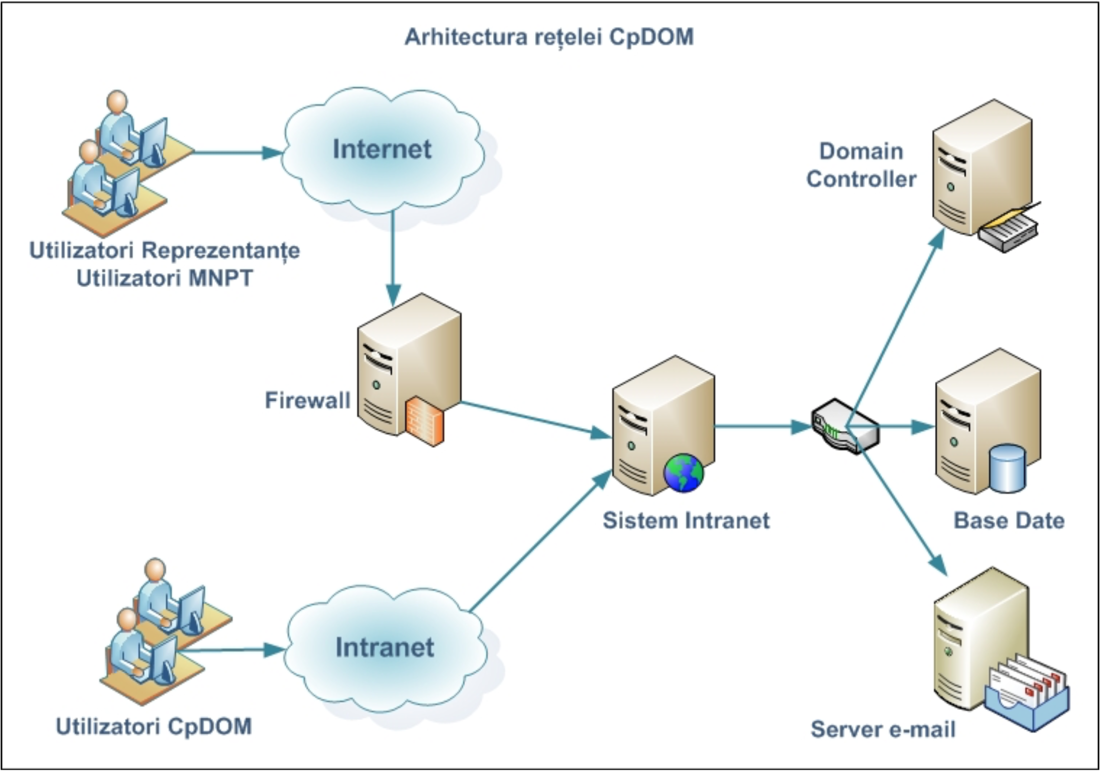


|  |  |
| --- | --- |
| Use Case | Description |
| **UC 03.01 IS administrator user creates and manages the IS roles** | |
|  | **Actor:** IS administrator user  **Aim:** IS administrator user has access to create and manage the list of roles.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The User must have administrator access rights into the system  *Basic script:* **The IS User administrates the IS roles**   1. The IS checks the access rights to the system resources 2. The IS administrator user accesses the list of roles 3. The IS administrator user administrates the IS roles   *Alternative Script:* **1a. The User does not have administrator access rights into the system**   1. The IS user does not have access to the IS roles   *BR 3-01 The system provides a list of predefined access rules that restricts user access to the system resources and system operations*  *BR 3-02 The user can select one or many access rules to a Role*  Administrator user should be able to create, edit and delete the roles from the system. For the case when a role is assigned to an account in the system on delete operation the user is required to select another role for related accounts.  *BR 3-03 The Administrator role has all access rules assigned and cannot be edited or removed from the system.* |
| **UC 03.02 IS administrator user creates and manages IS users** | |
|  | **Actor:** IS administrator user  **Aim:** Intranet system is a private network to be accessed by authorized users that may access the system only if there is an associated user account in the system. An IS administration user has all the options to administrate the list of IS users.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The User must have administrator access rights into the system  *Basic script:* **The IS administrator user manages the catalog of employees**   1. The IS checks the access rights to the system resources 2. The IS administrator user accesses the catalog of employees (IS users) 3. The IS administrator user manages the catalog of employees   *Alternative Script:* **1a. The User does not have administrator access rights into the system**   1. The IS user does not have access to the catalog of employees   *BR 3-04 The system validates the employee data -*  The system should validate that introduced data format, mandatory fields and to check the records are unique. Every employee must have unique email.  *BR 3-05 The administrator user may activate and deactivate a user accounts*  To keep user history into the system, users accounts cannot be deleted. Accounts that becomes inactive administrator user should be able to deactivate.  *BR 3-06 The system notifies user via email when account is activated*  Email notification is sent when a created user account is activated. Email notification will contain the access link to the IS, user login name and login temporary password generated by the system. IS user should be able to change temporary password. |
| **UC 03.03 IS administrator user manages the list of templates for internal documents** | |
|  | **Actor:** IS administrator user  **Aim:** IS administrator user monitors the list of templates to be up to date and documented properly.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The User must have administrator access rights into the system  *Basic script:* **The IS administrator user upload a new template**   1. The IS administrator user accesses the list of templates 2. The IS administrator user uses option Create to add a new template entry 3. The IS administrator upload the template file and completes the required fields 4. The system validates the introduced data, file type and file size 5. The system records in events logs the information about the new template creation   *Alternative Script:* **1a. The User does not have administrator access rights into the system**   1. The IS user does not have access to create a new entry.   *BR 3-07 Templates can be created and removed from the system only by users with appropriate permission.*  The templates list can be managed by any other user if has appropriate permission assigned. The view (download) permission is a separate rule so any of IS users should be able to access the list of templates and to download it. |
| **UC 03.04 IS administrator user accesses the system events log** | |
|  | **Actor:** IS administrator user  **Aim:** IS administrator user monitors the system events log and may export filtered result  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The User must have administrator access rights into the system  *Basic script:* **The IS administrator accesses and searches through events log**   1. User access the system events log page. 2. User selects log filtering rule. 3. User exports the result in CSV format.   *Alternative Script:* **1a. The User does not have administrator access rights into the system**   1. The IS user does not have access to the system event logs.   *BR 3-08 The IS saves into event log the user actions across the system*  The event log should be displayed in the format of the table and the user should be able to filter and search events by a specific column. The events are kept in the system for a set period of days, default 3 months.  The list of actions that should be logged and the format of the messages have to be identified and specified in the development phase. |
| **UC 03.05 IS administrator user manages with the Help section** | |
|  | **Actor:** IS administrator user  **Aim:** The IS user creates pages with guidelines for how to follow internal process and for any other user instruction purposes.  **Constraints:**  *Precondition*: The User must be authenticated in the system.  *Precondition*: The User must have appropriate access permission to administer the help pages.  *Basic script:* **The IS User creates help pages**   1. The IS administrator user accesses the help menu 2. The user selects create new page option 3. The user introduces all the information formated properly (rich text) 4. The user saves the page (not visible to user with read access only) 5. The user publish the page (visible to all IS users) 6. The system records the publish action in the events log   *Alternative Script:* **2a. The user does not have access to create page option**   1. The system restricts user access to create option 2. The user has read access to all published pages   *BR 3-09 IS user creates pages in the help menu*  Wiki or Help is an area where registered user will find useful information about the Intranet System, definitions and details about internal processes. It is intended to guide IS users in their daily interactions with the system. The user should be able to format the text and to insert images on the page. |

## 9. Requirements for the system as a whole

### 9.1. Requirements for the system’s architecture

Since the Ombudsperson’s Office and NPM is a geographically dispersed organization, that has branches in the territory (Balti, Cahul, Comrat), the requirements for the system architecture must allow the integration of all offices in an unique collaboration system. That is why the system would be implemented by setting a WAN network according to the architecture at a higher level that is presented in the following figure.



### 9.2. Requirements for the information security and protection

In their activity the employees of the Ombudsperson’s Office receive for examination and process a high amount of confidential information. That is why it is very important that the Intranet system, which will collect and save a big part of this information, has an increased degree of security against the outer accessing and the unauthorized accessing from the inner side of the system. Any action that will be fulfilled in the IS will be controlled and authorized. In this respect, the equipping of the IS with authorization and authentication components is required, which will assure its informational security – the posting protection, the undesired modification or deletion of the confidential information. All users registered in the system, will be part of user groups or will have proper roles. The user groups will be entitled to different information management rights in different system compartments, thus besides the fact that a more efficient management will be assured, a better protection of the information will also be guaranteed.

Any activity of the users in the system must pass through an early audit and information system in the case of accessing or attempt to access the confidential information.

The access from the Ombudsperson’s Office branches in the territory and within the NPM must be a secured one.

The informational security also includes mechanisms for the protection of the information by creating the reserve copies and for the data recovery in case of failure in relatively short terms by maximal recovery of the information.

In order to assure a better protection, it is required that the Database is placed on a server other than the server of application.

Not to allow the infiltration of different outer programs designed to destroy, overtake the control upon the information, its distortion – the system must be protected by an antivirus system, which will scan the whole information entering and leaving the system.

### 9.3. The requirements regarding the information integrity

The information integrity is a subject covering the informational security (the application of the soft information protecting methods) and the physical security of the room in which the informational system is implemented.

Ombudsperson’s Office at present has a room with conditions of work adequate for keeping the Intranet system servers and a specialist in the information system that could overtake the maintenance and monitoring of the IS after a training session provided by the implementing company.

The system must be equipped with information backup and restore functionalities in the event of some technical problems leading to losing or deteriorating the current information.

### 9.4. Requirements regarding the migration of the existing information

At present the Ombudsperson’s Office has no desktop system for the petitions’ recording. This system is old having limited possibilities in respect of attaching documents, the information structuring, reporting possibilities; moreover it cannot be accessed by the Ombudsperson’s Office employees from the branches in the territory.

All other activities, records, documents and reports of the Ombudsperson’s Office can be found on the employees’ computers in different formats without being unified.

Because of all constraints described above, an automated migration, or a bulk upload into the system is not a requirement and Ombudsperson’s Office employees will have to migrate necessary information into the IS manually.

### 9.5. Requirements for the system performance

The time of response desired by the users also depends on outer system factors, including:

* Width of the network band;
* Network’s use;
* Network’s latency;
* Configuration and use of different server resources.

The performance requirements will be checked on a clean medium used at large scale, using modern browsers agreed with the recipient.

|  |  |
| --- | --- |
| **Ref** | **Requirement** |
| **PRQ001** | The system must offer adequate response time to satisfy the business needs, for the tasks frequently fulfilled under standard conditions, for example:   * <50> authenticated and active users; * <50%> of the total anticipated amount of managed system documents; * The performance must be consistent for at least <ten> transaction attempts. |
| **PRQ002** | The system must be capable to display the results of a simple search in a period of <5 seconds> and a complex search (which combines four or several terms) within <10 seconds>, regardless of the depositing capacity or the numbers of system files and records. |
| **PRQ003** | The system must be able to overtake and display in <5 seconds> the first page of a record that have been accessed in the last <2> months. |
| **PRQ004** | The system must be able to overtake and display within <20 seconds> the first page of a record that has not been accessed in the last <6> months, regardless of the capacity of depositing or the numbers of system files/records. |
| **PRQ005** | The system must offer comparable response when the classification scheme grows significantly in size, in order to adjust to the needs. |
| **PRQ006** | *The requirements above are not applied for the editing of media files, big files downloads, reports elaboration. These are not considered “typical scripts of use”.* |

### 9.6. Requirements for the hardware and the communication channel

The Hardware equipment must allow the good functioning of the system in the limits of performance parameters exposed in this document. Since the Ombudsperson’s Office has no existing infrastructure on which the intranet system could be set up, this should be proposed for implementation within this project.

The list of hardware equipment already purchased and available in the inventory of the Ombudsperson’s Office is presented below:

|  |  |  |
| --- | --- | --- |
| Hardware | Units | Model |
| Server | 2 | Fujitsu PRIMERGY RX300 S6 |
| Router in main office | 1 | Router Juniper |

### 9.7. System Reliability

The implementation of the Intranet system will increase the dependence of the IT network users, to the extent to which these will not have the possibility to work if the system becomes unavailable. That is why measures must be taken, so that the system’s availability is as big as possible. Besides that, the system must correspond to a series of characteristics allowing to the users the fulfillment of ordinary tasks offline – the same as with the distance users.

|  |  |
| --- | --- |
| **Ref** | **Requirement** |
| **PRQ007** | The system must be at the user’s disposal for <15> hours during <5> working days. |
| **PRQ008** | The planned unavailability of the system must not exceed <5> hours a day, and be done in the period of time 22.00‐7.00, or during the weekend, with the preventive coordination of the Ombudsperson’s Office’s management. |
| **PRQ009** | The unplanned unavailability of the system must not exceed <3> hours within a period of <three> months. |
| **PRQ010** | The number of unplanned unavailability incidents must not exceed <3> hours within a period of <three> months. |
| **PRQ011** | In case of software or hardware failure, the system recovery must be possible in a functioning condition within a term of <1 hour> at most. |

### 9.8. Obsolescence Technologies

Long-term electronic records are confronted with technological risks of three kinds:

* Media support degradation;
* Hardware obsolescence;
* Formats’ obsolescence.

The details may be found in ISO 18492, and in great amount of published guides, produced by the institutions for the storage of the cultural thesaurus and others.

The risks of the media support’s degradation and hardware’s obsolescence must be attenuated by the dependence of external procedures, processes and decisions. One of the attenuation measures is to be based on the archive media and hardware, use on a large scale, as well as with the smallest degree of obsolescence.

The most difficult problem for a longer period of several years consists in the format’s obsolescence. In present, there exists no simple, generic method that would guarantee access to the long-term electronic registrations. The consensus could be obtained by an information storage strategy only in largely accepted, stable, open (for example, formats that are completely documented in publicly available specifications) having a long lifetime such as XML and PDF/A.

### 9.9. Method of Testing and Acceptance;

The system’s testing will be fulfilled in two phases (methods):

* The testing in the process of system’s implementation by the implementing company, with the application of the rigors specific to the software development’s methodology in the company.
* The testing by the Ombudsperson’s Office employees aiming at accepting the system.

The Ombudsperson’s Office must have the possibility to present their opinion about the correctness of the system’s implementation by the early opinion (known as “early feedback”), this allowing to diminish the effort to correct errors or configure some components of the system at an early stage of product’s implementation, also some modules of the system may be tested by the Ombudsperson’s Office’s employees while other functionalities are in process of implementation. This would lead to the diminishment of the total time of system’s implementation.

The system’s acceptance will be fulfilled as a result of UAT exercise (User Acceptance Testing). As a result of this exercise, the implementing company, in common agreement with the persons in charge for the implementation of the IS within the Ombudsperson’s Office, defines a series of critical scripts which will be run later when delivering the system and in case of their successful running, the system is considered accepted from the functional point of view. The non-functional defects will be categorized separately and the acceptance will undergo the general acceptance procedure.

The general acceptance procedure is developed by the implementing company, coordinated and approved later by the Ombudsperson’s Office.

The acceptance procedure must contain quantitative parameters for the system’s quality. As a rule, these parameters must be categorized and later agreed at the level of defects (defects of 1, 2, 3 category etc). The number of accepted defects according to the categories must be mentioned in the acceptance criteria.

### 9.10. Documentation and Training

It is important to assure the persons’ training concerning the information management principles at all levels, especially concerning the subject of capture of records, documents’ control and management of their lifecycle.

The training is also necessary, for the elucidation of the aspects connected to the service of the relationships with clients’ type (green line) and providing information and also connected to the standards of information management. This thing extensively involves the administrative staff at the first stages of IS implementation.

Aiming at assuring an adequate level of competence, it is necessary to execute intensive trainings for a group of employees from different departments, including for the system administrators. The training will be made in the Romanian language, but it is expected that the formatters will be able to communicate in the Russian language. The following training sessions are necessary:

* Formatters’ formation – extended training for a user group (2-3 people), so that these could transfer the knowledge to the other colleagues.
* Users’ formation – basic training to cover the most of the Ombudsperson’s Office’s staff, regarding the basic characteristics of the system and the users’ roles. (2 groups of 8-10 persons). The training sessions, will be actually extended for a longer period of time, so that the staff could participate without disturbing the basic activities and so that in this session the employees of the branches in the territory of the Ombudsperson’s Office could also participate.
* Administrators formation – extended training for a group of 3-5 interne/administrative functions of the system and its components.
* Manager’s formation – short-term sessions, that will initiate the managers at different levels into the character of the basic analysis, approval and signing tasks.

The IS for the Ombudsperson’s Office and the NPM should be implemented using a modern programming language based on a modular architecture that will allow further extensibility and integration with potential new IT infrastructure that is not in the current project scope. The entire solution and configuration activities should be very well documented. The Ombudsperson’s Office and the NPM staff should be delivered a set of technical documents and user guides that will ensure correct future software utilization, development and configuration. The IS for the Ombudsperson’s Office is required to have only Romanian language for the user interface and all the user guides and training documentation should be provided in Romanian language.

The documentation will include:

* User guidebooks – these will describe to the user the characteristics of the system they interact with. In the case when the solution is based on several components, a user guide for each of them will exist.
* Administration guides – these will describe the system’s administration, configuration and maintenance functionality. In the case when the solution is based on several components, a user guidebook for each of them will exist.
* Setup guides and also the general setup guide, in the case when the solution is based on several components.
* Training materials prepared for the training sessions mentioned above.
* Basic knowledge, including answers to frequent questions (FAQ), best practices, etc.
* The documentation will be prepared in one language and must include an electronic format as well.
* The documentation on paper mount is optional and may be included as a part of the offer.
* Any source code and setup configuration developed during this project will be transferred to the Ombudsperson’s Office, so that this is capable to continue the development and configuration in the future.