ANNOUNCEMENT OF THE INTERNATIONAL COMPETITION (TERMS OF REFERENCE)

Engagement of an IT company to develop and implement the Information System "Online Catalog of Current and Forecasted Climate-Related Transboundary Natural Disasters in Central Asia"

Position name	Company/Legal entity developing IT solutions and GIS
Host organization	Regional Environmental Centre for Central Asia (CAREC)
Implementation period	Up to 270 calendar days
Contract type	IT Services Contract (Legal Entity)

---

1. Rationale and context

As part of regional initiatives to improve landscape and climate resilience, digital tools for collecting, visualizing, and analyzing transboundary environmental risks are being actively implemented.

Climate change in the region is intensifying dangerous transboundary processes (in particular, mudflows, floods, and lake outburst hazards), leading to land degradation. Traditional methods of sharing environmental data are often fragmented. To overcome this barrier, the creation of a Regional Online Catalog of Current and Forecasted Climate-Related Transboundary Natural Disasters in Central Asia is being initiated—a comprehensive, turnkey web geoportal designed to promptly inform stakeholders about priority climate risks.

---

2. Objectives and tasks of the appointment

The Contracting Company's primary objective is the design, development, testing, and commissioning of a web-based geographic information system (IS "Online Catalog").
The system is designed to provide:

- Collection, secure storage and graphical visualization of spatial data on natural disasters in Central Asia.
- Integration of national data (including REST API gateways, GeoJSON , CSV formats) and open international resources.
- Direct two-way data exchange with state automated information management systems.

---

3. Recommended technology stack

The IT solution should be based on modern open standards and open source software (OSS) to avoid dependence on a single supplier:

- **Spatial data DBMS:** PostgreSQL + PostGIS .
- **Map publication:** GeoServer + GeoWebCache (with support for OGC standards: WMS, WFS).
- **Frontend mapping:** OpenLayers .
- **Authentication and Personal Account:** Keycloak with support for the Unified Identification System.
- **Infrastructure:** Nginx , Docker , secure HTTPS protocol (SSL certificates).

---

4. The scope of work and technical specifications are in Appendix 1.

---

5. Project stages, results and payment schedule (Deliverables)

Payment for services is made in tranches after official approval and confirmation of each stage by the Customer:

No.	Development Stage and Expected Result	Payment share	Deadlines (calendar days)
1	**Project launch** : Conducting an introductory meeting with the Client.	—	7 days after signing
2	**Stage 1: Primary documentation and design** : Logical diagram of the information system, detailed work plan, UX/UI design and adaptive layouts (3 options), technical specifications for the IT infrastructure.	**10%**	Up to 40 days from start
3	**Stage 2: Software** : Ready-made IS architecture, developed software modules, full-featured API, integration with web analytics tools.	**20%**	Up to 190 days from launch
4	**Stage 3: Commissioning** : Deployment of the information system on the Customer’s virtual servers, debugging of secure connections and test launch.	**15%**	Up to 220 days from launch
5	**Stage 4: Pilot operation** : Trial operation of the IS in real conditions, formation of a defect register (Bug Report), signing of the Pilot Completion Certificate.	**15%**	Up to 240 days from launch
6	**Stage 5: Acceptance of the IS** : Elimination of all category A, B, C bugs, regression testing, information security check, transfer of all source codes to the Customer’s balance.	**10%**	Up to 260 days from launch
7	**Stage 6: User training** : Conducting in-person training (at least 8 academic hours) for users and IT administrators nominated by the Customer.	**5%**	Up to 270 days from launch

8	**Step 7: Operational Documentation** : Transfer of complete user, administrator and programmer manuals.	**5%**	Up to 270 days from launch
9	**Final closing** : Provision of the final Certificate of Completion signed by all parties.	**20%**	7 days after approval of the Act

---

6. Qualification requirements for an IT company

To participate in the competition, companies must submit a portfolio and confirm compliance with the following criteria:

1. **Organization experience:** At least 2 successfully completed projects over the past 3 years on the development, implementation and maintenance of web-oriented information systems with the deployment of GIS/ geoservers based on international spatial data standards.
2. **Professional team (minimum requirements for experts):**
    - **K-1: Team Leader (Senior Specialist):** Higher IT education (academic degree is an advantage), at least 5 years of experience in web systems design, management of at least 2 similar projects.
    - **K-2: Frontend Developer:** Higher IT education, at least 5 years of experience in commercial web development and adaptive layout.
    - **K-3: Backend Developer:** Higher IT education, experience in building complex databases, integration buses and REST APIs for at least 5 years.
    - **K-4: GIS Expert:** Higher specialized education, at least 5 years of experience with GIS applications, GeoServer and spatial databases.
    - **K-5: UI/UX Designer:** Experience in interface design and development of adaptive graphic design for web portals for at least 3 years.

---

7. Warranty obligations

The winning company will grant perpetual licenses for all developed components and provide 12 months of free technical and warranty support for the IS from the moment it enters commercial operation. The contractor undertakes to resolve any identified functional discrepancies with the technical specifications within the contractual deadlines, at no additional cost to the Customer.

APPENDIX 1.

TECHNICAL REQUIREMENTS

To develop an online catalogue of current and projected climate-related transboundary natural disasters in Central Asia

Terms and abbreviations

CSV	from English Comma - Separated Values (comma-separated values) is a text format designed to represent tabular data.
HTTPS	HyperText Transfer Protocol Secure (HTTP) is a secure hypertext transfer protocol, an extension of the HTTP protocol that supports encryption via the SSL and TLS cryptographic protocols.
JSON	JavaScript Object Notation is a text-based data exchange format based on JavaScript.
KML	from English Keyhole Keyhole Markup Language (Keyhole Markup Language) is an XML-based markup language for representing three-dimensional geospatial data in Google Earth.
ESB	Enterprise Service Bus
OGC	Open Geospatial Consortium (OGC) is an international non-profit organization that works to develop standards in the field of geospatial data and services.
PDF	Portable Document Format (PDF) is a cross-platform, open format for electronic documents, originally developed by Adobe.
REST	from English Representational State REST is an architectural style for interaction between components of a distributed application over a network. REST is a consistent set of constraints that are considered when designing a distributed system.
SOAP	from English. Simple Object Access Protocol (SOP) is a protocol for exchanging structured messages in a distributed computing environment.
WFS	Web Feature Service - a spatial web service that defines interfaces and operations that allow querying and editing vector spatial data
WMS	Web Map Service is a standard protocol for serving georeferenced images generated by a map server based on data from a GIS database over the Internet.
WSDL	from English Web Services Description Language - a language for describing web services and accessing them, based on the XML language
XML	from English eXtensible Markup XML is an extensible markup language recommended by the World Wide Web Consortium (W3C). The XML specification describes XML documents and partially describes the behavior of XML processors.
AIUS	Automated information and control system
DB	Database
GAN	Global Area Network
GIS	Geographic information system (geographical information system, GIS)
GMO	Hydrometeorological situation
DMFE	Department of Monitoring and Forecasting of Emergencies
ESI	Unified Identification System
ESKMP	Unified system of integrated monitoring and forecasting

IS	Information System - Internet Portal
KR	Kyrgyz Republic
KazHydromet	National Hydrometeorological Service of Kazakhstan
Kyrgyzhydromet	Hydrometeorological Service of the Ministry of Emergency Situations of the Kyrgyz Republic
LAN	Local area network
MES	Ministry of Emergency Situations
PC	Personal computer
SW	Software
OSS	Open source software
RK	Republic of Kazakhstan
RT	Republic of Tajikistan
RU	Republic of Uzbekistan
Uzhydromet	Agency of the Hydrometeorological Service under the Ministry of Ecology, Environmental Protection and Climate Change of the Republic of Uzbekistan
CA	Central Asia
DC	Data center
ODCC	Observation Data Collection Center
CCC	Central Control Center

1. Introduction

1.1. The RESILAND CA+ program is an umbrella program that brings together national projects in Kazakhstan, the Kyrgyz Republic, Tajikistan, Uzbekistan, and Turkmenistan. Its goal is to enhance the resilience of regional landscapes in Central Asia by (i) increasing the area under sustainable landscape management in selected locations in the Kyrgyz Republic; and (ii) facilitating cooperation among Central Asian countries on transboundary landscape restoration.

1.2. To achieve these goals, RESILAND projects in Kyrgyzstan, Tajikistan, and Uzbekistan are funding the development of various online tools needed by countries in the region to collect, visualize, and analyze information and data on transboundary landscapes and climate disasters.

1.3. The KG RESILAND project supports the development of a Regional Online Inventory of Current and Projected Transboundary Climate-Related Disasters in Central Asia to inform governments in the region on priority areas requiring attention and actions to mitigate the impact of such disasters on landscape degradation.

1.4. The online catalogue will be a geoportal for collecting, storing, analyzing, and graphically visualizing geospatial data on climate-related transboundary natural disasters in Central Asia, including data on land degradation (a factor contributing to climate risk). The catalogue will include spatial databases from national and international resources and geospatial analysis tools. It will also include a user guide, a description of the data, and a methodological approach for systematizing it. As it becomes more comprehensive, the online catalogue will allow users to visualize areas in Central Asian countries vulnerable to the risks of current and future transboundary natural disasters, demonstrating to users the negative impacts on landscapes, thereby influencing the environment, economy, population, employment, and other areas.

2. General requirements

When developing, the Contractor must comply with:

- Requirements for websites of state bodies and local government bodies of the Kyrgyz Republic approved by the order of the Cabinet of Ministers of the Kyrgyz Republic dated February 17, 2023 No. 59-r.
- Requirements for the protection of information contained in the databases of state information systems approved by the Resolution of the Government of the Kyrgyz Republic dated November 21, 2017 No. 762.
- Resolution of the Government of the Kyrgyz Republic "Requirements for ensuring the security and protection of personal data when processing them in personal data information systems, the implementation of which ensures established levels of personal data protection" from November 21, 2017, No. 760
- Requirements for the procedure for the creation, development, commissioning, operation and decommissioning of state information systems approved by the Resolution of the Government of the Kyrgyz Republic dated December 31, 2019 No. 744
- On certain issues of implementation of electronic governance in the Kyrgyz Republic approved by the Decree of the Government of the Kyrgyz Republic dated December 31, 2019 No. 748, the IS and its components must be developed and installed on a turnkey basis;

- Develop a module for receiving data from government sources in Central Asian countries or universal download gateways (REST API / downloading CSV/ GeoJSON files);
- Develop a module for obtaining data from open sources;
- Develop a module for integration with the Unified System for Monitoring and Control of the Ministry of Emergency Situations of the Kyrgyz Republic;
- Develop a module for visualization of geospatial information;
- Develop a module for configuration and administration;
- Place the resource on the infrastructure of the Ministry of Emergency Situations of the Kyrgyz Republic;
- Conduct testing, training and implementation of the information system into industrial operation;
- Provide technical support for the IS for 1 year after the signing of the IS Acceptance Certificate by the Customer.

3. Purpose and goals of creating the ONLINE CATALOG IS

    - Purpose of the IS

The Online Catalogue information system should provide information on current and future transboundary hazardous natural processes, in particular, mudflows and floods, as well as information on climate change for monitoring and assessing areas unfavorable for human life.

The main goals of creating an IS

The "Online Catalog" information system provides visitors with essential information regarding transboundary areas prone to mudflows and climate information for the Central Asian countries.

Target audience

The target audience of the IS can be divided into the following groups:

- Civil servants;
- Development Partners and International Organizations;
- Business and media
- Civil Society.

4. Requirements for the IT solution technology stack

The minimum recommended technology stack for an online catalog can be defined as follows:

PostgreSQL + PostGIS – for storing spatial and attribute data;

GeoServer + GeoWebCache – for publishing and accelerated delivery of mapping services;

OpenLayers - for web mapping interface;

Keycloak - for authentication and authorization;

Nginx - for reverse proxying and TLS termination ;

Docker - for containerization;

REST API – for integration with external information systems.

The presented technology stack is recommended and exemplary and is provided to define basic architectural approaches to developing an online catalog. The IT solution developer, once selected as the winner of the selection process (competition/tender), has the right to propose alternative technology solutions, as well as modify or supplement the specified technology stack, provided that the proposed solutions:

1. provide functional equivalence or superiority to the proposed stack;
2. support international open standards for geospatial data exchange (OGC);
3. ensure scalability, security and stability of the system;
4. do not create technological dependence on one Contractor (vendor) lock-in);
5. ensure compatibility and integration with existing government information systems and geoinformation services.

All proposed changes or additions to the technology stack must be justified in the developer's technical proposal and agreed upon with the Customer at the system design stage.

5. Requirements for IS

- ### Requirements for IS in general

i. General description of upcoming work on the creation of the "Online Catalog" information system

The goal of the development is to create a web-based geographic information system designed for visualizing spatial data, viewing attribute information, and interactive user interaction with the map.

The system should provide quick access to basic geographic layers and associated data, including text information, photographs, and trend graphs.

The general description of the upcoming work on the creation of the “Online Catalog” information system includes:

1. The IC and its components must be designed and installed on a turnkey basis;
2. Develop a module for obtaining data from government sources in Central Asian countries or universal download gateways (REST API / downloading CSV/ GeoJSON files);
3. Develop a module for obtaining data from open sources;
4. Develop a module for integration with the Unified System for Monitoring and Control of the Ministry of Emergency Situations of the Kyrgyz Republic;
5. Develop a module for visualization of geospatial information;
6. Develop a module for configuration and administration;
7. Place the resource on the infrastructure of the Ministry of Emergency Situations of the Kyrgyz Republic;

ii. Information security requirements

The information system management system must provide a mechanism for backing up the structure and contents of the database.

Backup procedure:

- Automatic copying should be done every 12 hours.
- Manual copying must be performed by the employee responsible for maintaining the information system at least once a month, with an automatic message sent to the manager and the responsible employee if the period for the last copy exceeds 30 days.
- All virtual machines that will host the system must have backups enabled at least once a week.

iii. Access control requirements

Information posted on the IS is publicly available.

IS users can be divided into 4 groups according to their access rights:

1. Visitors
2. Authorized visitors
3. Editor (employee of the Ministry of Emergency Situations)
4. Administrator (employee of the Ministry of Emergency Situations)

Visitors have access only to the public part of the web platform module.

Authorized visitors have access to the public portion of the web platform module, as well as to specialized products available after authorization.

Access to specialized products must be provided using a unique login and password or the Unified Information System (ESI) system; a user registration system and the ability to change access rights must be provided.

The editor can edit section materials.

The Administrator can perform all the same actions as the Editor, and in addition:

- add users with Editor rights;
- add and remove sections of the web platform module.

Access to the administrative panel must be granted using a unique login and password. The login is assigned by the web platform module administrator. The password is generated automatically and sent to the user at the address specified during registration. The first time the user attempts to access the administrative panel, the system should prompt the user to change the password (by manually entering the new password).

To ensure protection against unauthorized access to the administrative section, we recommend adhering to the following rules when creating passwords:

1. The password length must be at least 8 characters.
2. The password must consist of numbers and Latin letters in different upper and lower case; it is advisable to include other characters available on the keyboard in the password (for example, the characters / ? ! < > [ ] { } etc.)
3. A password shouldn't be a dictionary word or a string of characters found next to each other on a keyboard. Ideally, a password should consist of a meaningless string of characters.
4. All passwords must be changed at regular intervals, with the ideal period being from three months to a year.
5. There must be a two-step authentication mechanism for the Editor and Administrator.

iv. Requirements for access to information

For " **Visitors"** only the following information is available:

Maps with various geospatial information, including:

- Mudflow risk map (Red/Yellow/Green zones).
- Map of historical flood zones, mudflows, etc.
- Mudflow and avalanche hazard map,
- Transboundary river basins
- Outburst-hazardous moraine lakes.
    - Vector information on mudflows.
    - Vector information on floods.
    - Raster information on mudflows.
    - Raster information on floods.
- Climate maps
- Map of vegetation degradation (NDVI) and desertification zones.
- Dynamics of changes in the area of glaciers and snow cover.
- Long-term climate trends (climate projections).
    - Climatological extremes
    - Köppen-Geiger climate map with description
- Tools on the map
    - Object identification
    - Ruler for measurements
    - Determining the coordinates of a point

- Draw a polygon
- Calculating the perimeter of a polygon
- Calculating the area of a landfill
- Ability to compare two maps

Other sections of the site are publicly available

to **"Authorized Visitors"** :

- Data from government agencies with restrictions
  - Information that each stakeholder can provide to other stakeholders;
  - General information on vector and raster data.
- Data from open sources
  - Vector layers with attribute information;
  - Raster layers with attribute information;
  - Tabular data

Tools on the map

- Spatial query with vector data
- Entering attribute information for your data

6. Requirements for the functions (tasks) performed by the information system

• Basic requirements

i. Structure of the online catalog module

The web platform module should consist of the following sections:

- Map
  - Possibility to download background from open sources;
  - Possibility of adding layers to the map;
  - Ability to change layer styles on the map;
  - Possibility to change the transparency of the map;
  - Possibility of preparing a map for printing a hard copy;
  - Possibility to view layer data in tabular form;
  - Possibility to use “Tools” on the map;
  - Possibility of downloading Table data in various formats;
  - Possibility to change the transparency of each layer;
  - Possibility of overlaying two maps on a map for comparison (a series of images and their comparison).
- Analytical block
  - Ability to use spatial analysis "Tools" for vector layers;
    - The query includes checking topological relationships (intersection, containment, touch, embedding).
    - Query using SQL queries to spatial databases.
- Integration bus
  - Message routing: Automatic delivery of data from sources (e.g. field sensors) to recipients (GIS servers, mapping web portals);
  - Data transformation: Adaptation of data formats, including complex geospatial formats (GeoJSON , WKT, KML);
  - Guaranteed Delivery: Reliable data exchange even at low network bandwidth, providing protection against losses;
  - Intuitive interface for connecting to other geoservices for data visualization.
- Settings
  - Ability to add a user
- Feedback

- Pop-up survey

ii. Navigation system (web platform module map)

The relationship between sections and subsections of the web platform module (web platform module map) is shown in Figure 1.

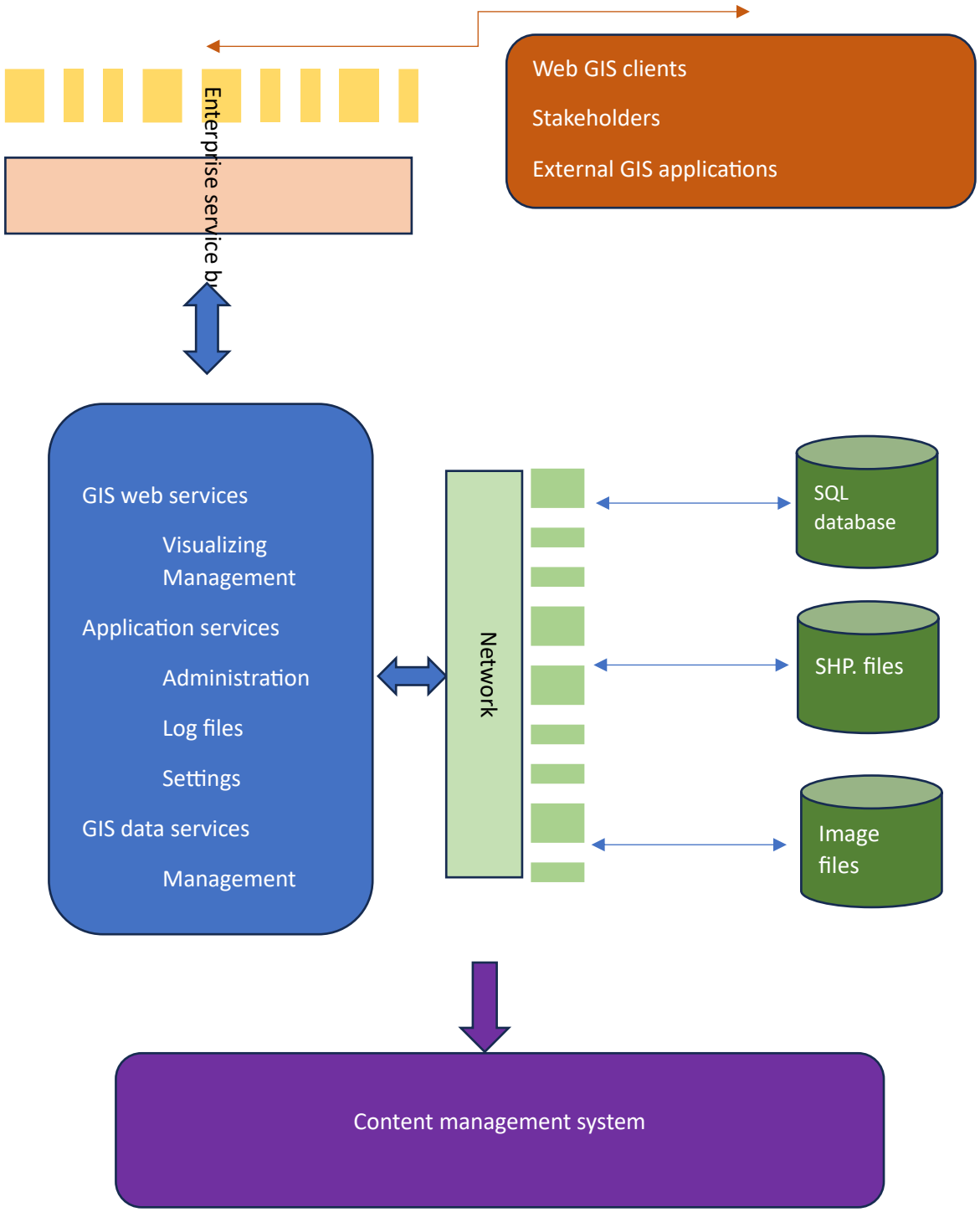

Figure 1– Web platform layout

- Requirements for the functional capabilities of the IS

i. Content management system (CMS)

To maintain the information system and operate the web interface of the content management system (CMS), personnel should not be required to have special technical skills, knowledge of technologies or software products, except for general skills in working with a personal computer and a standard web browser (e.g. Google Chrome or Mozilla Firefox)

The content management system (the administrative part of the web platform module) should provide the ability to add, edit, and delete content on static and dynamic pages. It should also be possible to add information without displaying it on the web platform module.

The project requires developing functionality for managing the display of tables and modules on the web platform via a content management system (CMS). This functionality should allow the administrator to hide or display tables and modules on website pages without having to access the source code. All changes should be immediately reflected on the website once applied in the CMS.

The content management system must meet the following requirements:

- implementation in graphical window mode;
- uniform design style;
- intuitive purpose of interface elements;
- displaying on the screen only those features that are available to a specific user;
- displaying on the screen only the information necessary to solve the current application task;
- displaying the progress of long processing processes on the screen;
- the dialogue with the user should be optimized to perform typical and frequently used operations;
- For mass data entry operations, the number of keyboard strokes required to perform standard actions should be minimized.

ii. Configuration module

For attribute information, the required input data is:

- Enter the region and district (the SOATE code is assigned automatically)
- coordinate indication (WGS 84, decimal)
- Enable/Disable Layer
- Adding/removing new layers

For each table

- displaying data in a table

An individual configuration module must be developed for each card.
Which includes:

- displaying a layer on a map
- display at the republic level
- region-level display
- district-level display

iii. Module for receiving data from the Unified System of the Ministry of Emergency Situations

Develop a data exchange process between the online catalog database and the ESKMP database. Ensure that information is transferred directly from the online catalog database to the ESKMP for visualization. Organize ongoing requests for information exchange.

Provide the ability to manually update information through the internal system.

iv. Development of a module for receiving operational data from the AMS or the developed IS DMFE (at the time of contract implementation)

Based on API requests (API documentation will be provided by the Ministry of Emergency Situations), the Contractor must develop a module for collecting data from the automated monitoring stations of the Ministry of Emergency Situations and recording it in the Information System Database. An algorithm for automatically querying missing data must be provided.

v. Development of a data editing module

The module must provide the ability to view all available data in the information system with the ability to filter and sort by various parameters.

The module should allow the user to make changes to existing data, including editing individual fields or entire records.

When saving changes to data, all related values should be automatically recalculated according to established rules and formulas. For example, if a value in one field changes, the related value in another field should be automatically recalculated.

Before saving changes, the module must check the entered data for correctness and compliance with established formats and restrictions.

The system must maintain a log of all data changes, including information about the time and the user who made the changes.

Users with administrative rights must be given the ability to view and analyze all changes made to the data, with the ability to track the change history.

Access to the data editing module must be limited and controlled based on each user's access level. All user actions must be authenticated and authorized before execution.

vi. Feedback module

Development and implementation of functionality for collecting user requests from the website, storing them in a database, and promptly notifying the administrator.

The form must contain the following fields:

Username (Type: text , Required).

Contact details (Type: email or tel , Required, mask validation).

Subject of the request (Type: select - drop-down list: "Technical support", "Sales", "Complaint", "Other").

Message text (Type: textarea , Required, 1000 character limit).

Personal data processing policy consent checkbox (Required).

User Flow

The user fills in the fields.

The client script checks the correctness of the Email /Phone.

Data is transferred to the server in the background.

The server checks the "hidden field" and limits.

The data is written to the database.

The administrator receives a letter.

The user receives a notification: “Your message has been sent successfully.”

Acceptance plan

Checking whether fields are required (the form does not leave empty).

Security check: Attempting to submit a form with a Honeypot field filled in .

Checking receipt of email notification.

Checking if a record appears in the database.

vii. API for external interaction and integration (ESB)

The API must meet the following requirements:

- meet all the canons of modern development (HTTPS, WebSocket , RESTful , Auth , etc.);
- Be as complete as possible and cover all functionality of the user and administrative parts of the system. All client components should operate using this API; be accompanied by comprehensive documentation with code examples, in a closed access environment;
- Provide an authorization system for third-party applications (e.g., token). Access is granted by the administration.
- For geospatial data, the integration bus must use OGC standards .

i. Public version of the site

The public version of the site must be a standalone website, meaning it must have its own domain name, hosting, and independent access from the Internet.

The public version of the website must be managed by the online catalog administrator using a content management system (CMS). Data on this website can be visualized, but clients will only be able to download this information with the administrator's permission.

- Design requirements

During development, the requirements for websites of state bodies and local government bodies of the Kyrgyz Republic approved by the order of the Cabinet of Ministers of the Kyrgyz Republic dated February 17, 2023 No. 59-r must be taken into account.

Websites for government agencies and local governments must be responsive (viewable correctly on mobile devices (smartphones, tablets), and display according to the user's preferences). The mobile version of the interface for "Visitors" should be as simplified as possible.
All pages of the website must be designed in a uniform style and stylistically linked to the state body and local government body.

Website design should be user-friendly. The volume of graphic design elements should not slow down the overall loading time or impact website performance.

When developing a website design, it is necessary to take into account the accessibility standards for information posted on the website pages for users with disabilities.

The interface design should be developed taking into account the maximum ease of navigation on the website and ensure the quick display of screen forms.

All screen forms of the user interface must be implemented in a single graphic design with the same arrangement of the main controls and navigation elements.

Page design should:

- Consider the design of the meteo.gov.kg website (meteo.kg)
- Please take into account the color policy of the gov.kg website .
- Consider the placement of text in 3 languages (Kyrgyz, Russian and English).
- The system's user interface design must be responsive and adapt to various device formats, such as PCs, smartphones, tablets, etc.
- When developing an information system, a user-friendly and intuitive interface must be developed for a user who is well versed in his or her subject area and is not an information technology specialist.
- User interfaces of information systems must be designed and developed using uniform principles of graphical presentation of information and organization of access to functional capabilities and services.
- The information system must ensure interaction between the user (person) and the system.
- The design of the presentation-level components of the information system must be developed taking into account the standard ergonomic requirements for the user graphical interface, ensuring the comfort and productivity of its users, as well as the fast loading of the pages selected by the user.
- When developing an interface design, usability and ease of understanding should be a priority. The design of user interface elements should evoke a minimal understanding of the actions the user will perform when interacting with one of them. Interface elements should not be associated with functions they do not perform. Design solutions should comply with current sanitary and ergonomic standards and most effectively evoke a positive emotional response in IS users.

The website design should not include:

- flashing banners;
- a lot of merging text;
- dark and aggressive color combinations and graphic solutions.

- Requirements for authorization/registration and personal account

i. Authorization

Registration/authorization is available on all pages of the site; the corresponding link is in the header of the site.

The authorization page contains:

- Authorization block
- Registration block

In the authorization block:

- an authorization form that contains the "login" and "password" fields
- A "Login" button, which, when clicked, verifies the user's login and password. If a user with the specified login and password is found, they are authorized.

Otherwise, an error message is displayed. If the number of login attempts exceeds the allowed limit (5), a captcha field (an image and a text input field) is additionally displayed.
- Forgot your password? link
- An alternative login option is via "Login to the Unified Identification System" (UIS)

In the registration block:

- Introductory text (headline and text message)
- The "Join" button is a registration button that, when clicked, takes you to the registration form.

ii. Registration

The registration page contains a registration form that allows you to

the user to register on the site.

The registration form contains the following fields:

- Login
- your name
- Mobile phone
- Email
- Password
- Confirm your password

All fields are required.

When submitting a form, a check is made to ensure that:

- The user login is unique
- The name is full and more than 2 letters
- The mobile phone number is complete and contains at least 9 digits.
- The email is complete and correct.
- The email address isn't registered in the website's user database. If it is, the user is prompted to log in or reset their password.
- Password must be at least 8 characters long
- The "Confirm Password" field is the same as the Password field.

After submitting the form, a pop-up window appears with the message, "Thank you for registering! Your account has been successfully created. An email containing your information has been sent to your email address."

Users register on the website as "Authorized Visitors." This means they have access to the public portion of the web platform module, as well as specialized products available after authorization.

iii. Personal account

After logging into the Personal Account, the user is taken to the main page of the Personal Account

The main page of the Personal Account contains the following blocks:

- menu of personal account subsections
- user personal data with the "Edit" button

iv. Changing personal information

On the Personal Data page, the user can change their data:

- Login
- Name
- Email
- Telephone
- Password

- Navigation

The user interface of a public and local website should provide a clear, intuitive representation of the structure of the information contained within, with quick and logical navigation to sections and pages. Navigation elements should ensure unambiguous user understanding of their meaning: page links should be provided with headings, and symbols should comply with generally accepted conventions. Graphic navigation elements should be provided with an alternative caption.

The system must provide navigation through all resources available to the user and display relevant information.

Filling the online catalog module (content).

The pages of all sections of the web platform module must be generated programmatically based on information from the database on the server.

Filling with information should be carried out using the page templates of the web platform module.

As part of the web platform module development, the Contractor must ensure that static information provided by the DMFE is entered into the dynamic sections being created (taking into account the functionality provided by this TOR). Text information must be provided by the DMFE as separate MS Word (DOC/DOCX) files.

- Requirements for linguistic support.

The development must take into account the requirements for websites of state bodies and local governments of the Kyrgyz Republic, approved by Order No. 59-r of the Cabinet of Ministers of the Kyrgyz Republic dated February 17, 2023. The web platform must be available in the state, official, and English languages.

The default version of the website is the official language version. Users can then select their preferred language version.

The website's language versions must correspond to the official language version. Translations of text materials into other languages are provided by the website owner.

Individual page templates are developed for each website version, preserving the portal's overall style. All graphic elements in the templates are in the corresponding language, and the menu structure and other navigation elements must match the structure of the corresponding version. Service fields and interface text elements must also be translated.

The user should be able to switch from one version to another at any time while browsing the website.

If, when switching languages, the page being viewed does not have an equivalent in the selected version, then a transition should occur to the first page of the current section, and if there is none, to the main page of the website in the selected language.

- Requirements for analytics and statistics of web platform usage

The custom web platform must be integrated with at least one of the following analytics tools: Google Analytics 4 or Yandex Metrica, to collect audience statistics.

Select an analytics tool (Google Analytics 4 or Yandex Metrica).

Create an account for the selected analytics tool, registered on the DMFE.

The system must provide the following data:

- Configure the web platform to integrate with the chosen analytics tool.
- Implement the necessary scripts and tags on all pages of the web platform.
- Conduct integration testing and data collection.
- Ensure collection and display of the following indicators:
  - Number of users over the entire period of use.
  - Number of users per day, month, etc.
  - User activity (number of active users for the selected period, average number of active users per day).
  - Building graphs based on analytics data.
  - Possibility to select data for different time periods.
  - Resource usage report by gender.

- Reliability requirements

The information system must maintain operability and ensure restoration of its functions in the event of the following emergency situations:

- In the event of failures in the hardware or software of the user's end device (workstation), leading to a reboot of the operating system, the program should be restored after the device is rebooted;
- In case of errors in the operation of workstations, restoration of the IS function is entrusted to the operating system of the device;
- In case of errors related to the workstation software, the operating system is responsible for restoring functionality.

The IS must prevent accidental calls to procedures, functions, and commands used in its functionality. All calls to functions, methods, and procedures must be thoroughly checked for accidental invocations.

The IS must be protected from misuse of functions by users.

The information system must ensure the correct handling of situations caused by invalid and inconsistent input data values. In such cases, the information system must issue appropriate alarm messages to the user and then return to the operating state that preceded the invalid command or incorrect data entry.

The information system, after carrying out work according to this Technical Assignment, must be resistant to software and hardware errors, with the ability to restore its operability and the integrity of its information content in the event of errors and failures of user workstations.

- Load testing requirements

The system being developed must be designed and implemented with high performance and fault tolerance in mind. Acceptance and load testing must confirm that the system can handle at least 500 concurrent user connections without failures, critical crashes, data loss, or unacceptable performance degradation.

When conducting load testing, at least the following parameters should be assessed:

system stability with simultaneous operation of at least 10,000 users;

response time of key user operations;

stability of the web interface, API and mapping services;

correct processing of user requests without errors and refusals;

maintaining data integrity and system operability under load;

the ability to restore normal operation after peak loads.

The results of load testing must be documented in a separate report indicating the methodology used, testing scenarios, achieved indicators, and conclusions regarding the system's compliance with established requirements.

- Safety requirements

The information system must comply with the general software security requirements when operating as part of information systems.

The principles of solution development must meet modern international standards for the level of information security and safety and include:

- means of encrypting information sent by users;
- methods for protecting the database from unauthorized access;
- logging and auditing, registration of all events and user actions;
- restricting user access to information system objects based on user identification, including by their role;
- access to data is limited by access rights that are determined by the roles of the IS users: the user interface displays only those tools, functions and methods that can be required by a user with a given specific access level;
- Flexible access rights management; enabling the Administrator to manage user accounts;
- protection of data transmission channels;
- the delimitation of access rights for users and IS Administrators will be based on the principle of "what is not permitted is prohibited";
- protection of transmitted information by encrypting confidential data during transmission over communication channels.

The technologies used in development must ensure secure access to data through authentication, identification, and user role-based rights.

When the system is operating at the backend level of the information system, logging of each user session must be implemented, indicating the MAC / IP address of the device (this requirement is determined by the DMFE), from which the login to the system was made, and the time of login to the system.

Automatic audit logging should also provide the ability to monitor the most critical (unique) data stored in the database and record all events and changes to any data in the system in accordance with the system settings.

The audit log must be created automatically and maintained continuously. Each operation in the audit log must be identified by user, date, and time. The audit log must be protected from modification and deletion of records.

Since the IS will work in conjunction with a web server, all requests must be transmitted over an encrypted HTTPS channel using an SSL certificate. This will maintain stable speed and a high level of security between the application and the web server.

- Requirements for protecting information from unauthorized access

During development, the requirements for websites of state bodies and local government bodies of the Kyrgyz Republic approved by the order of the Cabinet of Ministers of the Kyrgyz Republic dated February 17, 2023 No. 59-r must be taken into account.

The information system must comply with all established requirements in the current regulatory documentation of the Ministry of Emergency Situations for the protection of information from unauthorized access.

The information system must ensure that physical access to system elements is restricted, both to prevent disruption of the system's operation and to prevent unauthorized access to information.

The information system must implement a mechanism for security and protection of information based on the following basic principles:

- restricting access to the system based on user identification;
- restricting access to system objects;
- maintaining an audit log to identify unauthorized changes to the system;
- protection of data transmission channels.

The information system must provide access control to the System's information resources. The list of personalized data may be expanded during development.

The IS must ensure the provision of information for maintaining logs (Logs), which record information about system events and attempts at unauthorized access to information for all users of the IS.

Information security must include a set of organizational measures and hardware and software methods and tools to prevent unauthorized access to information resources. The information system must ensure the integrity, availability, and confidentiality of data during processing.

When developing an information system, the requirements of the information security policy in force in the Ministry of Emergency Situations must be taken into account in order to avoid the occurrence of conflict situations when carrying out information security measures.

User passwords must meet password complexity requirements to prevent brute-force attacks. The number of unsuccessful login attempts to the information system must be limited, and if this number is exceeded, the information system must be locked for a specified period of time. No one should have the right to modify or delete log entries.

- Requirements for the safety of information in accidents

The security of information at the level of information system software must be ensured by:

- emergency situations in the premises where the information system servers are located;
- network failures caused by power loss;
- failures of technical equipment.

In the event of a failure, the system has the ability to fully restore data through backup. At the software level, it is necessary to prevent partial or complete loss of user data and damage to the integrity of information stored in the database.

The system must provide backup copies of its own database, as well as system settings, which must be used for system recovery. Backup copies must be stored on non-volatile media (as determined by the Emergency Management Agency) and updated periodically as new data is received and/or at least once per day. Data recovery must be accomplished by selecting the last uncorrupted copy.

Information displayed in the information system must not lose its quality (relevance, completeness, reliability), be destroyed, damaged, distorted or lost in the event of any emergency situations: failure of technical equipment, loss of power in the electrical network, etc.

- Web platform accessibility for people with disabilities

During development, the requirements for websites of state bodies and local government bodies of the Kyrgyz Republic approved by the order of the Cabinet of Ministers of the Kyrgyz Republic dated February 17, 2023 No. 59-r must be taken into account.

Website accessibility for visually impaired and blind people is ensured by creating an alternative version of the website for visually impaired and blind people. To access this version of the website, a text hyperlink must be placed on the homepage.

If an alternative web site version for visually impaired and blind people is unavailable, the website of the state agency or local government must comply with the requirements of the standard "KMS GOST R 52872–2021." The standard "KMS GOST R 52872–2021" was approved by an order of the Center for Standardization and Metrology of the Kyrgyz Republic and contains requirements and recommendations for presenting digital content in a manner that makes it accessible to users with disabilities, including people with temporary disability, and the elderly.

To ensure full access to the website for visually impaired and blind people, all key information on it is presented in text form.

If graphic codes are used on a website to protect information from spam, an alternative sound code must be provided for blind users.

When placing electronic forms on a website that are intended to be filled out online, in the event of incorrect information being entered by the user, it is necessary to provide an automatic message about the error in text form.

Graphic files are accompanied by text explaining the image; when placing graphic information on website pages, an alt caption tag must be used to ensure it is interpreted by all users.

The website does not use background images that may obscure the site or distort the information.

To improve the readability of the agency's website for people with visual impairments, the contrast ratio of the image and background, as well as the text and background, should be at least 4.5:1.

When placed on a government agency or local government website, the ability to increase the font size without losing web content or functionality of the government agency or local government website (excluding captions and text images) is provided, without resorting to horizontal scrolling.

When posting information on the website, appropriate synchronized captions for audio and video content are provided.

- Requirements for patent and licensing purity

The Contractor shall use only intellectual property rights to which they have acquired (received) and are used without infringing the intellectual property rights of third parties or granted by the DMFE. This requirement shall ensure compliance with the copyright, related, patent, and other rights of the Contractors of the third-party components used. The Contractor undertakes to transfer, free of charge, the rights to use protected intellectual property rights to which belong to the DMFE and/or third parties and which were used by the Contractor.

- Requirements for standardization and unification

At all stages of project development, design solutions must be unified, which must be ensured by a uniform approach to solving similar problems, as well as by unifying technical, informational, linguistic, mathematical, informational, and organizational support. A uniform approach to solving similar problems must be achieved:

unification of the functional structure in terms of the implementation of automated functions and information links between them;

the same software and hardware method for implementing similar system functions and a single user interface that complies with international standards.

i. Unification of information support should be achieved through:

- use of a unified system of classification and coding of objects and their subsystems;
- use of national, industry and other standard classifiers applied in the practice of the facility’s operation;
- the use of standard forms of documents (reports) and rational limitation of their types of composition (in agreement with the Ministry of Emergency Situations);
- application of unified methods and means of collecting, preparing, monitoring and storing information arrays of the system.

Unification of mathematical software should be achieved through the modular principle of constructing algorithms and the typification of algorithmic modules.

ii. Software unification should be achieved:

- maximum possible use of standard software;
- using unified software modules in the development of application programs.
- Indicators establishing the required degree of use of standard, unified methods for implementing the System's functions, supplied software, typical mathematical methods and models, and typical design solutions:
- support for search engine implementation standards;
- support for distributed access to information;

- the ability to function on various hardware platforms.

The coding and classification system used to generate normative and reference information must meet the requirements for the classification and attribution of documents adopted in the territory of the Kyrgyz Republic, and also take into account international experience in creating similar systems.

The solution being developed must ensure the unification of functional tasks, operations and user interfaces.

- Requirements for information support.

The composition, structure, and methods of organizing data in the information system must be determined at the detailed design stage. Information exchange within the system must be carried out using a developed data transfer protocol. Data storage within the system must be built on a modern DBMS.

Built-in DBMS mechanisms must be used to ensure data integrity. DBMS tools, as well as those of the operating systems used, must ensure documentation and logging of information processed within the system. The database structure must support the encoding of stored and processed information. Access to data must be granted only to authorized users, taking into account their official authority and the category of information requested.

The DBMS tools, as well as the tools of the operating systems used, the application server and the web server, must ensure documentation and logging of information circulating in the System, protection of data from destruction during accidents and power failures in the System, control, storage, updating and recovery of data.

- Software requirements.

The application software must meet the following requirements:

high degree of readiness to solve assigned tasks;

compatibility of software products in terms of the technical means used, system software and general system infrastructure within the requirements for technical support, as well as their information compatibility within the requirements for information exchange.

The software must be built as **software modules, standardized for each workstation** . Tasks not needed for a given information system must be inactive or added to the software shell. All modules must fully exchange information without compromising the overall system.

Information must be accessed in a timely manner and presented in the form of tables, reports, forms, and corresponding main and context menus. Data must be transmitted over the network without affecting the functioning of the entire system. The system software must be capable of creating, maintaining, and using reference books.

- User training requirements

At the beginning of the provision of services, the Contractor must conduct testing and assessment of users' knowledge of working with the information system to ensure their readiness to use the system in their daily activities.

The contractor must develop training materials for visitors (public). It is recommended to specify interactive onboarding (Onboarding Tour): When first accessing the site, the system should launch a short visual tour (tooltips) that shows step-by-step, for example: "Here you can select the flood layer," "Here you can see the weather forecast," "Here you can find the

ruler and analytics." It is also necessary to supplement this section with tooltips and an FAQ for online catalog visitors.

The Contractor shall conduct user training in accordance with the requirements below:

User training must be conducted in Russian.

The cost of translation services, if necessary, must be included in the tender proposal.

User training should include theoretical and practical classes.

User training should include monitoring of material acquisition.

In order to conduct user training, the Contractor must:

- develop a detailed user training program;
- prepare handouts and print them in the required quantity (one set for each student);
- conduct in-person user training;

Training of users to work with the information system should at least include the following:

- Users must be trained in the operation of the basic functions and capabilities of the IS, including methods of entering, editing and searching for data, as well as performing basic operations, including navigation through various sections, using menus and tools, and applying filters and sorting data.
- Users must be familiar with security rules when working with the information system, such as password requirements, rules for accessing confidential data, and protection from malicious actions.
- Practical exercises, skill development;
- User training, including theoretical and practical classes, with a total duration of at least 8 academic hours, no more than 4 academic hours per day.
- Practical classes are held in the training classroom (head office of the Ministry of Emergency Situations, Bishkek, Manasa Street 1).
- Number of students: 10-12 people.

Training of users in system administration and maintenance should at least include the following:

- Users should be familiar with the main types of cyber threats and attack methods, such as phishing, malware, DDoS attacks, etc.
- Training in basic information security principles, including password protection, access restrictions, data encryption, and regular software updates.
- Training users in methods of monitoring and analyzing IS logs to identify abnormal activity and unauthorized actions.
- Guidelines for interpreting log entries, including security events.
- Instructions for rapid response to security incidents.
- Training users on how to request support and resolve potential issues when working with the IS, including support contact information and troubleshooting steps.
- Users should be trained in the basics of CMS operation, including adding and editing content, managing users and settings, which will allow them to effectively manage the local version of the site.
- User training, including theoretical and practical classes, with a total duration of at least 8 academic hours, no more than 4 academic hours per day.
- Practical classes are held in the training class (head office of the Ministry of Emergency Situations , Bishkek, Manasa Street 1).
- Number of trainees: 4 people.

- Stages and acceptance

The IS development will proceed in stages, with each stage being documented and approved by the Department of Emergency Management. The Department of Emergency Management may make changes to the development process, including changes to the data structure and module development.

The transition to the next stage must be implemented by the Contractor only after the approval of the previous stage by the DMFE. All actions at each stage (meetings and task implementation) must be documented and signed by the DMFE and the Contractor.

Stages	Result
Stage #1 **Development of primary documentation of the information system** : • Develop a detailed logical diagram of the IS operation. • Conduct a comprehensive analysis of current and planned work. • Draw up a detailed work plan describing all stages of the development and implementation of the information system. • Include timeframes, responsibilities, and resources needed to complete each step. Creation of design and prototype of a web platform and local website: • Develop a design and prototype for the public and local website, ensuring alignment with key stakeholders. • Prepare a design and prototype report including visual mockups (3 options), user scenarios and a description of functionality. • A list of minimum and recommended hardware requirements for the information system, as well as a list of required pre-installed software. •	• A document with recommendations for IS optimization has been prepared, including proposals for improving work processes and resource utilization. • A logical diagram showing the main processes and interactions in the system is attached to the report for the corresponding stage. • A detailed work plan, including a description of all stages, timeframes, responsible persons and resources. • A coordinated design and prototype report for the web platform and local site, including visual mockups and functionality descriptions.
Stage No. 2. **Development of IS software:** • Conduct design and development of software architecture of the information system. • Prepare an architecture testing report agreed with the Department of Emergency Situations. • Develop an API to ensure external interaction and integration with other systems and services. • Prepare an API testing report agreed with the Ministry of Emergency Situations. • Include in the test results an assessment of the API's security, performance, and compatibility with various external systems. Set up web platform integration with at least one of the following analytics tools: Google Analytics 4 or Yandex Metrica, to collect audience statistics.	• Developed by IS • APIs have been developed • Architecture testing report agreed with the Ministry of Emergency Situations. • API testing report agreed with the Ministry of Emergency Situations. • The web platform is successfully integrated with the selected analytics tool (Google Analytics 4 or Yandex Metrica). • The account for the analytics tool is registered on the DMFE. • All pages of the web platform are configured to collect analytics data. • The system successfully collects and displays statistics. • Report on the successful implementation of analytics tools (the system successfully collects and displays statistics).

Stage No. 3 **Commissioning of IS:** • Preparing virtual machines for IS deployment • Place the information system on virtual servers and hosting provided by the Ministry of Emergency Situations. • Configure all necessary system components and parameters to ensure its correct operation. **Launch of IS:** Conduct the launch of the IS, ensuring its readiness for further testing and use.	• The information system has been successfully deployed and configured on virtual servers and hosting provided by the Ministry of Emergency Situations. • The IS has been successfully launched and is functioning in accordance with design requirements.
Stage No. 4 **Experimental (pilot) operation of the IS.** • Transfer of the System to the Customer (MES of the Kyrgyz Republic) for conducting trial operation in real operating conditions on the computing capacities of the MES. • Collection, recording and classification of comments, errors and suggestions for improvement from users on the Customer's side. • Formation of a unified register of defects (Bug Report). • Preparation and signing of the Certificate of Completion of Trial Operation with an attached list of identified deficiencies to be corrected.	• The system operates in trial mode. • A formalized register of identified comments and defects was generated and transferred to the Contractor. • The certificate of completion of the trial operation has been prepared, signed and approved by the Customer
Stage #5 **Acceptance tests and commissioning.** • Elimination by the Contractor of all deficiencies recorded in the Certificate of Completion of Trial Operation. • Conducting comprehensive control (regression) testing of the information system to confirm the fact that defects have been eliminated and that it fully complies with the technical specifications. • Checking the System for compliance with information security requirements. • Transfer of all source codes of the System to the balance sheet of the Ministry of Emergency Situations. • Preparation and execution of the Certificate	• An analysis was carried out and it was confirmed that all the shortcomings of the trial operation were successfully eliminated. • The information system's compliance with the technical specifications and safety requirements has been confirmed. • All source codes of the online catalogue, which are the intellectual property of the DMFE, have been transferred. • The act of acceptance of the information system into industrial operation was signed and approved. •

of Acceptance of the information system into industrial operation.	
Stage No. 6 **Training users on how to work with the information system:** • Conduct training for users, teaching them how to work with the information system. • Prepare and provide a training program that covers the main functions and capabilities of the IS. • Create a training participant list to ensure that all target users are present. • Develop and distribute a user manual containing detailed instructions and examples on how to work with the IS. • Maintain a training record, recording the process and results of the training. User training for IS management: • Organize training for users responsible for the management and administration of the information system. • Prepare a training program covering topics of administration, security and maintenance of information systems. • Create a list of training participants, including all administrators and technical specialists. • Develop and provide an administrator's guide that includes instructions for managing, monitoring, and maintaining the system. Maintain a training record, recording the process and results of the training.	• The training has been conducted, the training program has been completed, the list of participants has been compiled, the user manual has been distributed, and the user training protocol has been prepared. • Administrator training has been conducted, the training program has been completed, a list of participants has been compiled, an administrator's guide has been distributed, and a user training protocol has been prepared.
Stage #7 **Preparation of operational documentation:** • Language of technical documentation: Russian • Prepare technical documentation, including a complete description of the system architecture, all components and modules, as well as the integration capabilities of the IS. • Prepare a flow chart showing all business processes supported by the IS, as well as the infrastructure used. • Prepare a detailed description of the system debugging process, including steps for detecting and resolving errors, as well as procedures for restarting the system with all connections restored. • Prepare a user manual containing instructions and recommendations for working with the IS, including a description of all basic functions and operations. • Prepare an administration guide that includes instructions on system management, monitoring, configuration, and security.	• Technical documentation with a detailed description of the integration capabilities of the IS has been prepared. • A business process and infrastructure map has been prepared. It is documented and includes all necessary elements. • A User Manual has been prepared, containing a full description of the system, its functionality and how to use it. • A description of debugging and restarting the system has been prepared, including all steps for detecting and eliminating errors, as well as procedures for restarting the system with the restoration of all connections. • A User's Guide for Administration has been prepared, containing instructions on system management, monitoring, setting parameters and ensuring security. • Technical and software requirements have been prepared, minimum and recommended requirements for hardware

• Prepare a programmer's manual containing a detailed description of the internal structure of the system, including descriptions of classes, methods, properties, interfaces, and other components. Prepare and provide the source code for the information system in a readable and structured format. The source code must be understandable and documented to facilitate further maintenance and development.	and necessary pre-installed software have been documented. • The Programmer's Guide has been prepared and includes a complete description of the internal structure of the system, classes, methods, properties, interfaces and other components. • The source codes are provided in a readable form, structured and documented, ensuring their clarity and ease of further maintenance and refinement. All necessary documents for operating the information system, including technical documentation, a business process map, a description of debugging and restarting the system, a user manual for working with the information system, and an administration manual, have been developed and prepared.

- Control and reporting procedures.

The contractor shall be provided with a list of requirements and procedures for documenting testing procedures and results, which shall include, but not be limited to, the following subsections: test plan management, documentation of test procedures, and documentation of the system results summary.

Defect Classification. If a test case within a Test fails, a defect report must be generated. To maximize test results and minimize defect-related issues, all defect reports will be classified as follows:

- Category A: major defect;
- Category B: moderate defect;
- Category C: minor defect;
- Category D: test error;
- Category E: Dispute regarding the incident.

All categories are described below:

Category A: Major Defect. Category A defects are defects that adversely affect system components or the active operation of the system, to the point of completely preventing the use of most of the system.

Category B: Moderate defect. Category B defects are localized issues that do not prevent the active operation of system components or the system (minor errors that do not significantly impact the system). Category B defects are not grounds for terminating testing.

Category C: Minor defect. Category C defects are cosmetic and do not seriously affect the system components or the system, and active operation may continue without fixing the defects (such as unclear error messages, errors in reports, and screen formats). Category C defects should not be grounds for terminating testing.

Category D: Test Error. Category D defects arise from errors in the testing method and/or test data, errors occurring during execution of the test case, or errors in the expected results. In the event of a disagreement between the Contractor and the Beneficiary, the parties must discuss the validity of the test case, and if the error occurs, it will be classified as Category E. Category D defects do not constitute grounds for terminating testing.

Category E: Incident Dispute. Category E defects are those for which the Contractor and Beneficiary cannot agree on a classification. If the parties are unable to reach an agreement within five (5) business days, the matter will be referred to an independent person appointed by the parties after due consultation. The appointed person's decision will be final and binding on both parties.

It is emphasized that any defects of categories B, C, D, or E arising during testing shall not result in termination of such testing. In the event of a defect of category A, both parties will have the right to independently decide whether to terminate testing. In this case, a new date agreed upon by both parties will be set for repeating the testing. With the exception of defects of category A, retesting will only include those test cases that have not yet been successfully completed.

Documentation of testing procedures: protocols that state: “Press the button – the email arrived.”

Test Summary Report : A final document that lists the number of defects found and corrected by category (A, B, C, D, E).

Bug Report : A list of all bugs that occurred during development and proof of their correction .

7. Duties of the Ministry of Emergency Situations related to the provision of services

Provide 2 virtual machines with an installed operating system (Linux).

Provide temporary access for the Contractor's personnel to all virtual machines required to perform the work.

Determine by order of the Ministry of Emergency Situations the procedure for acceptance and the composition of acceptance committees (acceptance tests).

Provide educational premises for organizing the educational process

Provide all necessary documentation for the implementation of the IS.

Provide information and data to fill the site content.

8. WARRANTY OBLIGATIONS (GUARANTEE).

- The warranty for the information system is valid for 12 (twelve) months from the earlier date: the date of signing the Act on acceptance of the information system into operation approved by the Director of the Ministry of Emergency Situations (year from the date of putting the information system into commercial operation).
- The warranty applies to all software and services throughout the Kyrgyz Republic.
- The Contractor shall provide warranty service for the supplied products at no additional cost to the Customer. Warranty service means restoring the functionality of the software in the event of its failure due to reasons unrelated to improper operation during the warranty period.
- All licenses for the supplied software must be perpetual, that is, they must not contain any time limits on the licensee's use of these software products.
- During the warranty period, if the DMFE detects a discrepancy in the functional capabilities of the IS (the IS fails to perform any of its functions described in the Technical Specifications, User Guide and User Administration Guide), the Contractor undertakes to eliminate these discrepancies within 20 (twenty) business days, subject to the following conditions:

i. All discrepancies in the functional capabilities of the information system are recorded by the Department of Emergency Management in writing, in the form of an Act, and sent to the Contractor by e-mail and/or fax;

ii. Inconsistencies in the functional capabilities of the IS are identified if they can be repeated (demonstrated) on equipment and a copy of the IS using a working database;
iii. The Contractor, within 10 (ten) business days from the date of receipt of the Act from the Ministry of Emergency Situations, shall provide the Ministry of Emergency Situations with a written response describing the method for eliminating the discrepancy in the functional capabilities of the information system.
iv. If the period of 20 (twenty) business days is exceeded, the Contractor must notify the Emergency Management Department in writing of the delays and also extend the Warranty Period for a period equal to the period for correcting the non-conformities in the functional capabilities of the IS minus 20 (twenty) business days.

- The warranty for the IC does not apply in the following cases:

i. Changes to the IS database and/or settings of the SQL server on which the IS database is located, configuration files or the IS itself by computer viruses and/or as a result of intentional or unintentional actions of employees of the Ministry of Emergency Situations or other third parties;
ii. Unqualified actions of employees of the Ministry of Emergency Situations/other third parties in the administration of servers, computer equipment, LAN and database management systems, such as, but not limited to:
1. Physical removal of IS files, configuration files or databases;
2. The end user of the IS does not have rights to access the IS to folders and/or certain files (ports) that are required for the normal operation of the IS;
3. Installation by employees of the Ministry of Emergency Situations of updates and new versions of system software not certified by the Contractor , for example, from Microsoft;
4. Incorrect administration of virtual servers on which the IS operates or the IS Database is hosted, for example, limiting computing resources;
5. Making changes to the Database, including through the use of external programs from any other third parties, without written permission from the Contractor.

9. Requirements for the qualifications of the Contractor's personnel

The Contractor will provide personnel and methodology that meet the qualification criteria presented in Tables 1 and 2.

Table 1. Evaluation criteria

No.	***Qualification requirements***
1	Proven experience in implementing similar services and supporting information systems At least 2 completed projects over the last 3 years on the development and implementation of a web-oriented information system with the deployment of a geoserver based on OGC standards .

Table 2. Minimum requirements for the Contractor's personnel and their contribution

No.	**Key personnel**	**Qualification**
1	Senior Specialist (Team Leader)	Higher technical education in IT. A Master's degree is an advantage.
		In total, at least 5 years of experience in designing and creating web-oriented systems
		Experience in implementing at least 2 projects over the past 5 years.
		Additional confirmed experience/qualifications
2	Frontend developer	Higher technical education in IT. A Master's degree is an advantage.
		At least 5 years of experience in programming

		Additional confirmed experience/qualifications
3	Backend developer	Master's or higher technical education in IT
		At least 5 years of experience in programming
		Additional confirmed experience/qualifications
4	GIS expert	Master's or higher technical education in the field of GIS.
		Work experience from 5 years;
		Knowledge of GIS applications and how to work with them
		Knowledge and experience with ArcGIS , QGIS , JVSIG , MapInfo , Erdas
		Additional confirmed experience/qualifications
5	Graphic designer/UI designer	3 years of experience in UI/UX;
		Additional confirmed experience/qualifications

The distribution of assessment points will be carried out as follows:

(1) Compliance and quality of the proposed methodology and work plan with the technical specifications:

Total points for criterion (1): 40

(2) Qualifications and competence of key experts to perform the task:

Position K-1: Senior Specialist (Team Leader): 18

Position K-2: Frontend developer : 14

Position K-3: Backend developer : 14

Position K-4: GIS Expert : 9

Position K-5: Graphic Designer/UI Designer : 5

10. Terms and payment

The contract implementation period is **no more than 270 (two hundred and seventy) calendar days** after contract signing. Payment for services will be made by CAREC within 10 business days after the Customer (DMFE) approves the stage's acceptance.

No.	Objectives / Results	Payment	Deadlines (calendar days)
1	First meeting to launch the project		7 days after the contract is concluded

2	**Stage/Result No. 1.** Development of primary documentation for the information system	10%	40 days after signing the contract
3	**Stage/Result No. 2.** Development of IS software	20%	190 days after signing the contract
4	**Stage/Result No. 3.** Commissioning of the IS and launch	15%	220 days after signing the contract
5	**Stage/Result No. 4** Experimental (pilot) operation of the IS	15%	240 days after signing the contract
6	**Stage/Result No. 5:** Acceptance testing and commissioning	10%	260 days after signing the contract
7	**Stage/Result No. 6.** Training users to work with the information system	5%	270 days after signing the contract
8	**Stage/Result No. 7.** Preparation of operational documentation	5%	270 days after signing the contract
9	Provision of a certificate of completion of work signed by three parties (Contractor, DMFE, CAREC)	20%	7 days after submission of the approved act