TERMS OF REFERENCE
FOR PURCHASING
ENVIRONMENTAL DATA MANAGEMENT SYSTEMS

BISHKEK 2025

Content

ABBREVIATIONS AND NOTATIONS

Term	Definition
DRC	A Data Processing Center is a specialized dedicated room for the placement of server and network equipment, which ensures the uninterrupted operation of the company's IT Systems.
DB	Data Backup is a consistent copy of data on removable media (hard disk, floppy disk, etc.) designed to restore data to its original or new location in case of damage or destruction.
LIMS	Laboratory Information Management System

1. General information

1.1. Name

The full name is “Terms of Reference for purchasing Environmental Data Management and Monitoring Systems”.

1.2. Supplier and Contractor

Customer: The “Kumtor Gold Company” CJSC

Software Provider: the organization selected by the Customer to supply the software under this ToR.

2. Basis, purpose and objectives of the acquisition of an environmental data management system

2.1. Basis

The basis for the acquisition of an environmental data management system is the maintenance of the existing system and/or improvement of the existing system with subsequent modernization (development of new templates for reports with the possibility of automatic download in the form of ready-made state reports, statistical reports.

2.2. Assignment

The environmental data management system should:

1. Ensure the automation of the Company's technological processes in terms of monitoring and management of environmental data (automatic and manual collection of data from various sources, validation of entered data, planning of work schedules, use of calculation formulas, verification of data for compliance with regulatory requirements, notifications and reporting);
2. Provide environmental monitoring data management combined with interpretation tools to quickly and efficiently process and analyze large amounts of monitoring data over long periods of time.

2.3. Project objectives

Project objectives:

1. Continuous improvement of technological processes.
2. Improving the quality of strategic and operational decision-making.
3. Optimization of the work of the Environmental Protection Department in order to increase labor productivity and the reliability of decisions made.
4. Reducing the impact of the “human factor” due to the automation of technological processes in the field of environmental protection.
5. Improving the quality of control and analysis of monitoring data.
6. Improve efficiency in all areas of data management by quickly finding the information you need and making every monitoring event available.
7. Reducing the costs of untimely decision-making.
8. Timely identification of risks.
9. Reduce operating costs by automating processes.

3. Requirements for an environmental data management system

3.1. Requirements for software functionality

The system should contain the following modules:

1. Data collection
2. Validate data import results
3. Work schedules, daily tasks
4. Notifications and warnings
5. Regulatory Compliance
6. Application of formulas, counting functions
7. Reporting

The list of requirements for the functionality of the software is given below.

3.1.1. Data collection
When working in the field, possibility to measure indicators from devices and enter them into the system manually. Data import wizard.
Division of work into current, when the data is entered directly into the field at a given time, and historical (the employee returns to the office and enters the captured data later).
Ability to use mobile devices to collect data.
Ability to enter data offline mode and synchronize with the server when a connection is available.
Ability to set up a scheduled data import scheduler.
Ability to create templates for data entry with descriptions of the following object parameters: Date, Sample Point, Variable / Measure, Data Source, Site/Location, Sample type Comment, Lab reference, Data Qualifier, Test method, Uncertainty, Sample Reference, Detection limit, Analysis date.
3.1.2. Validation of the data import results
Checking the quality of the data entered, whether the data is imported automatically or manually entered.
When uploading data, you need a primary filter for errors (by notification in the application and by e-mail): typos, violation of limits, duplicates, incorrect dates, etc.
Quality and integrity checks include: • Spelling mistakes • Violation of physical limitations • Threshold violations • Duplicate values • Invalid dates • “Unusual” data
3.1.3. Work schedules, daily tasks
Ability to divide work into planned ones based on created work schedules; and unplanned (if deviations are detected during monitoring and work is needed to eliminate problems). Work schedules must be synchronized with the monitoring scheduler.
Ability to monitor visits by multiple users.

Monitoring graphs can be managed automatically, with email notifications when the monitoring time and date arrives, details of the data received, the data to be collected, and what data is missing according to the data status and settings.
Once the schedules are created, they automatically generate visits. Such events require visiting certain locations and measuring variables. When the data arrives in the database, it is marked as complete and the percentage of completion is updated.
By default, visits should be marked as complete if the database has 100% of their data. However, for some schedules, not all data is always available, it should be possible to mark the visit as complete with a lower percentage.
Ability to make the monitoring schedule inactive. This will pause the monitoring schedule until further notice, preventing unnecessary alerts from being sent.
Ability to schedule the frequency of visits according to the schedule and start date. The default date of the next visit is the start date. The ability to change the date of the next visit (and therefore the date of future visits according to this schedule).
In addition to the required data source, it should be possible to specify the employee or department responsible for sampling in the schedule and visit management forms.
Ability to create and edit one-time visits without affecting its parent. For example, a visit can be scheduled for the 1st of each month to collect data. However, after some time, a change may occur, and the visit will be postponed to the 14th. If only this visit is edited, then the next one will be on the 1st day of the next month according to the schedule.
Ability to create special visits. Sampling events do not always fit into the schedule. Sometimes they are unplanned or one-time. These events also need to be tracked to ensure that samples/readings have been taken and that the data has subsequently entered the database.
The ability to send samples for testing anonymously, i.e. with reference to the sample and without information about the place from which the sample was taken.
3.1.4. Notifications and warnings
Warnings when exceeding the set limits (in color in the application and by email notification).
Ability to adjust color coding in case of violation of regulatory requirements.
If the work schedule is violated, a sample is not taken, a notification is sent to the responsible persons, depending on the rules set for the degree of response.
Ability to send notifications to primary, secondary and tertiary contacts depending on the rules set.
Ability to send alerts to email addresses based on the location of sample collection. That is, recipients will only need to receive alerts related to specific locations for which they are responsible. Other contacts can also be alerted if necessary.
Ability to filter email alerts using the selection system. For example, some people may only receive notifications about lab data, while others are interested in field data. A tool is needed to allow only certain types of data that apply to a specific email alert.
A global setting to copy all notifications to a single address for all email alerts.
Alerts for “unusual” data (e.g., future dates).
Ability to track the following notifications: • The data calendar shows you how to import, export, run the calculator, and enter data. • The violation calendar shows where violations have occurred. They appear on the actual date of sampling. Violations are based on threshold levels. • The monitoring schedule calendar shows the scheduled visits and the % complete of each visit.

• The calendar of scheduled tasks shows when scheduled tasks are due to be completed.
3.1.5. Regulatory Compliance
Ability to create compliance packages (baselines) for use in single-tier, multi-sampling point situations. For example, the water quality standard. The levels are fixed and are not added separately for each well. A level is entered once and all relevant wells are applied to that level.
Compliance grids are designed to be used where different levels are applied to different sampling points and/or where multiple types of levels are applied (e.g., warning, compliance) and/or where they change over time.
Configure different types of match levels. A compliance level refers to a specific upper or lower limit set for a variable, such as a CO upper limit of 10 ppm. A level can refer to a mandatory regulatory limit. The level may refer to a limit set by the company. The levels can be internal, warning, license violation, required urgent actions, etc.
Logically group levels and determine which sampling points are subject to threshold levels.
Ability to create a package with multiple levels for variables and application to all sampling points.
The ability to determine whether data from all or selected sources is evaluated for compliance.
The ability to insert text, such as instructions to follow in the event of a level violation.
Ability to set the level to either the upper limit, the lower limit, or both. There may also be dates up to which the level has not been applied, and therefore data identified as collected before that date will not be evaluated. For example, if the license permission is changed to include new limits against which historical data should not be evaluated.
Ability to set different levels for different sampling points for the same variable. For example, well 1 may have pH limits of 5 and 8, well 2 may have limits of 4.8 and 8.2.
Ability to revise the specified levels while preserving the history of changes.
The ability to create a single, multidimensional mapping grid for each data type. New sheets are created for each type of level. Within each level type, you can create new tiles for different date ranges. Each sheet in the grid takes both the upper and lower levels for each variable.
Match types allow you to set several different levels so that a single item can be evaluated at multiple levels.
3.1.6. Application of formulas, counting functions
The ability to apply formulas to data as it enters the database.
The ability to apply a single calculation to multiple locations, sites, and sampling points.
Ability to compare the same variable from different locations.
The ability to filter based on time, allowing you to define one calculation for working time, for example, and another for non-working time.
Ability to filter data by sources.
Ability to create calculation rules. For example, only compute records that have the same date/time. Or take into account only data within certain dates or times for calculation, for example, received from 9:00 to 17:00. Other options are fixed ranges, day of the week, or month of the year.
The presence of the “Recalculate” function. The ability to determine that calculations work only with new data. To reverse calculate the data, it must be marked as “calculable”. The Recalculate feature allows you to specify which (or all) of the sampling points to use, as well as a date range.
A way is needed to manage values that are normally static but may change from time to time, such as carbon conversion factors or the height of a groundwater shaft.

Ability to apply coefficients to sampling points so that they can work in calculations. Each factor table can be constructed differently: either to apply a single factor to each sampling point, or to apply a single factor to multiple sample points using different groupings.
Constants can either be entered directly into the calculation or created and reused.
Aggregations take a dataset from a specific variable and data source and perform one of the following functions with it: •Sum •Average • Maximum value • Minimum value • Standard deviation Aggregations are updated each time data is imported into them. At the end of the period for which they are set, they save the final data point and start the next period.
Configurable whether the aggregated calculation will be performed on all data from all sources or only on a specific source.
Ability to save an audit trail (history) of aggregate recalculations.
Ability to set the number of standard deviations/percentages. For example, creating calculated limits to alert users when any new groundwater data entering the database is compared to the mean plus 4 standard deviations for historical data that have been entered into the database over the past year. Data series with less than three readings are not included in this calculation.
Ability to set a minimum number of data points to set the minimum number of reads that are considered reasonably necessary for a data series to provide meaningful statistics. Below this number, the function will not create a value for the cell in the grid. For example, if a value of 5 is set and the calculation detects that there are only 3 readings within the specified date range for chloride for well 1, then the restriction will not be created.
Ability to set the number of decimal places for the created limits.
A calibration tool that is designed to correct data over a period when the accuracy of the instrument deviates from the calibration point.
3.1.7. Other
An integrated mapping interface (GIS) that allows you to visualize sampling points and data on maps, aerial imagery, and more.
The ability to add hyperlinks and files (such as PDFs and photos) to database data and objects. Hyperlinks and embedded files can be attached to database objects, such as data points, sample points, sites, variables, and data sources.
Approval and pre-approval system. Quarantine option to store even verified data from the database for any import until approved according to the rules you have made.
Accreditation ISO9000, 14001.

3.2. Non-functional software requirements

3.2.1. Data Residency

The solution must be On-Premise in accordance with the Customer's policies and the legislation of the Kyrgyz Republic. The system must be deployed in data processing centers and at the Customer's server facilities.

3.2.2. Operating System Requirements

The Customer’s side of the application must be cross-platform. The web client must be fully compatible with all the following current versions of browsers: Google Chrome, MS Edge, Mozilla Firefox, Opera, Safari. The marked versions of browsers must support Windows (versions 10 and higher), Android

(versions 10 and higher), iOS (versions 16 and higher), Mac OS (versions 10 and higher). The backend should be able to publish through a web server using REST API requests and support the function of encrypting the data transmitted between the client and the server.

The backend must be deployed using a virtual infrastructure (VMWare).

The server part of the system must also be cross-platform, i.e. support the following operating systems:

• Windows Server 2019 or later.

• Linux

3.2.3. System reliability requirements

The system must be able to operate around the clock on a daily basis. A temporary suspension of the system is allowed for no more than 1 day 19 hours 50 minutes per year or 99.5% of the system availability per year for preventive maintenance of the software and hardware of the server on which the system is located.

3.2.4. System Recovery Requirements and Technical Support

According to the Customer's requirements, the system must ensure the restoration of the system operability from data backups no more than 8 hours. The terms of service and technical warranty support will be determined and agreed upon during the conclusion of the service contract.

3.2.5. Performance requirements

№	Parameter	Meaning
1.	Number of users simultaneously working with the system per unit of time	-
2.	Average Response Time for Screen Form Navigation Operations	<= 8s
3.	Average response time for data search/filter operations	<= 60 sec.

3.2.6. Requirements for integration with existing systems

3.2.6.1.Automatic data upload from equipment

1. The PLS membrane level sensor is connected via Campbell Scientific CR1000 datalogger. Sensor data is recorded at 5-minute intervals and must be entered into the system database every hour.
2. Radar Level Sensor OTT RLS connected via Campbell Scientific CR1000 datalogger, real-time integration.
3. Flow meters, connected to the system via Campbell Scientific CR100 datalogger, real-time integration.
4. The flow meter will be connected to the system via Campbell Scientific's CR100 datalogger, real-time integration.
5. Radar Level Sensor OTT RLS connected via Campbell Scientific CR1000 datalogger, real-time integration.
6. Campbell Scientific CR100 Datalogger Main Weather Station, real-time integration.

3.2.6.2. Integration with Leica GeoMoS

Leica GeoMoS 24/7 system - automatic monitoring software (MS SQL database, coordinates of 12 points in the local coordinate system, data transmission interval 2 hours).

3.2.6.3. Integration with LIMS Archimedes Technologies

Data exchange between the Environmental Data Management System and the Laboratory Management System:

1. Registration Date
2. Delivery date

3. Sample Quantity
4. Name of the design
5. Sample Type
6. Defined parameters
7. Sample storage (return/disposal)

Event-based integration, as trials or trial results occur.

3.2.7. System Reporting Requirements

Trends to detect equipment failure and maintenance needs.
Ability to send reports by email.
Daily task reports are automatically sent via email.
Site visit reports can be printed either before the visit for use in the field or as a report showing the data once it has entered the database.
Task Scheduler automatically generates output in the form of files and reports and can either save it in a specific location or send it via email according to defined rules.

3.2.8. System documentation requirements

Based on the results of the project, the Contractor must develop, agree and submit to the Customer the following documents:

- Terms of reference
- Specification (composition and description of the program, information about the logical structure and functioning of the program, technical architecture, description of application: Information about the purpose of the program, scope of application, methods used, class of tasks to be solved, restrictions for application).
- Test program and methodology (test object; test objective; requirements for the program; requirements for program documentation; composition and procedure of tests with an indication of the hardware and software used during the tests, as well as the procedure for conducting tests; test methods with an indication of the test results (lists of test examples)).
- Testing protocols (unit, integration, performance, stress tests, vulnerability tests).
- Developer's Guide (Information for testing, ensuring the functioning and configuration of the program, API library of classes and functions with a description of signatures, semantics of functions).
- Application Administrator Guide.
- User’s guide.

3.2.9. Requirements for the role model of the system

During the implementation of the project, the CRUD (Create, Read, Update, Delete) matrix must be implemented in the system.

Action / Role	Creating user directories	Management Access	Creating work schedules	Reporting
Environmental Protection Manager			R	RU
Head of the Joint Forces Operation			CRU	CRU
Environmental Protection Engineer			R	R
Heads of CB			R	R
OS Operators			R	R
ISPS operators			R	R
Administrator	CRU			
Information Security Officer		CRU		

3.2.10. Information security requirements

The system should provide automatic logging and logging of all changes and events on the server side, as well as record all user operations. Logging settings should provide for the following areas:

- Administrative changes
- Custom Changes
- System Changes

It is necessary to ensure that it is possible to send security events, information system integrity events and other information to the log aggregator and/or information security event management and monitoring system. Sending must be able to transmit all or only certain types of events.

The system should include an administrative application or a module for managing and administering accesses, roles and user groups in the context of functions, applications and software modules. End-user access to system modules and applications should be based on a role-based model. The roles and rights of users should be configured in accordance with their job duties. All data about employees (personal and financial) must be protected from unauthorized access.

Data transmission between the server and the client, as well as between server applications and the DBMS, must be encrypted. Encryption algorithms and keys must be as secure as possible, and the key must be at least 1024 bits long.

User authentication in the system should support integration with the company's Active Directory (AD) and provide SSO authentication capability.

User authorization should be centralized in the user and access rights administration module.

You should provide a function to automatically block a client session or application when there is no user activity. The time for automatic blocking should be configurable in the range from 10 minutes to 1 hour in accordance with the requirements and policies of the KGC information security.

The system must be able to send security events to the SIEM system and/or log aggregator. The format of sending events must comply with standards, LEEF, CEF, or Syslog, to be compatible with your existing SIEM system.

The system should support connecting and interacting with IDM via API.

The system must support multi-factor authentication (MFA) for users who have access to critical data.

3.2.10.1. Control (analysis) of information security

Control of the installation of software updates, including software updates of information security tools.

Monitoring the performance, configuration parameters and correct functioning of software and information security tools.

Control of the composition of hardware, software and information security tools.

3.2.10.2. Ensuring the integrity of the information system and information

Software integrity control.

Restriction of users' rights to enter information into the information system.

Control of the accuracy, completeness and correctness of data entered into the information system.

Control of erroneous actions of users to enter and (or) transmit information and warn users about erroneous actions.