AWS Tender Specifications:MIPS

# General

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | WMO Tag | Functionality | Requirement Heading | Requirement | Test | Importance |
| 296 | G.IT.1 | IT Security | Access security method | Access authorisation should be based on user identification in combination with a personal password. | Demonstration | Very Important (Regional Input) |

# AWS Network Management

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | WMO Tag | Functionality | Requirement Heading | Requirement | Test | Importance |
| 129 | ANM.AWL.1 | Alarms/Warnings/Logging | All exceptions shall be reported | A system component or system part reports all operational and technical exceptions (e.g. failures) to the AWS Network Controller. An operational exception is a situation, which is unusual for the system component or system part | Demonstration | Very Important |

# Network Metadata Management

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | WMO Tag | Functionality | Requirement Heading | Requirement | Test | Importance |
| 163 | NMM.MS.1 | Metadata Storage | Management of configuration parameters for the generation of metadata | It may be possible to manage the data necessary to generate metadata information. These data may include • A table containing data types and classes with the companion properties• The default values for all existing metadata fields | Demonstration | Important |

# Measurement Data Archive

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | WMO Tag | Functionality | Requirement Heading | Requirement | Test | Importance |
| 168 | MDA.AWL.1 | Alarms/Warnings/Logging | Logging of data use | It should be possible to record the requests for data, for example::• Regarding requests for data: which users, what data, time of request• Regarding requests for metadata: which users, what data, time of request | Demonstration | Very Important |

# National Message Generation

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | WMO Tag | Functionality | Requirement Heading | Requirement | Test | Importance |
| 208 | NMG.RMG.1 | Message/Report Generation | Generation of meteorological reports | The NMG should generate meteorological reports and store them for a configurable period of time. The contents and layout of reports should be configurable via templates that should be managed by the system operator. At least the standard reports SYNOP, METAR, and SPECI should be included, with the internationally and nationally defined groups. The National Message Generation System (NMG) should automatically generate CORs for the SYNOP or METAR if conditions require this.It should also be possible to define reports of own composition consisting of arbitrary data that can be chosen freely from the available data. The NMG should have a user friendly tool to define such report templates. This tool should include but is not limited to the following functionality:• Definition of a report name.• Definition of the structure of a report.• The elements from the database.• The format of the elements to be included.• The order in which report elements are placed in a report.The following report elements are required:• Fixed text. All ASCII characters (also characters such as a carriage return and line feed) can be entered• Date and time• Meteorological data• Visual observations.A limited amount of computation capacity may be required to generate reports from the database. The location in the NMG (map, directory) where the reports should be stored is configurable.The NMG should at least be able to generate the alphanumeric FM-12-XIV SYNOP and FM 15–XV METAR codes as described in [WMO\_306, Vol I.1, PART A \_ Alphanumeric Codes]. [[If other formats are required (BUFR, CREX), they should be specifically requested.]] | Demonstration | Very Important |
| 210 | NMG.RMG.2 | Message/Report Generation | Distribution and storage of meteorological reports | The NMG should distribute meteorological reports. It should be configurable if the report is distributed automatically or manually, although ‘automatic’ should be the default. Every report is stored separately. If, for example, an original report has been distributed followed by a COR, both reports should be stored.• Automatic distribution.When it is time to distribute a report and it is available, it is distributed automatically.• Manual distributionWhen it is time to distribute a report and it is available, it should be distributed by human intervention.The destination of the reports is configurable. In general, the destination is a message switch (MSS). Disseminated reports cannot be changed anymore. If a corrected report has to be sent after the original report (for example, if data that was missing in the original report has become available), NMG should automatically generate and disseminate the corrected report. Both the original report and corrected report should be stored. | Demonstration | Very Important |

# IT Infrastructure

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | WMO Tag | Functionality | Requirement Heading | Requirement | Test | Importance |
| 294 | IT.IT.1 | IT Security | Strict access control | Strict access control procedures will be implemented. | Demonstration | Essential (Regional Input) |

# Communications

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | WMO Tag | Functionality | Requirement Heading | Requirement | Test | Importance |
| 1113 | C.DCA.1 | Data Communications-AWS | Communication protection | Communication between all system components shall be protected against unauthorized access. This especially applies to dial up connections and mobile data communications such as GPRS/4G. | Demonstration | Essential |
| 1114 | C.DCA.2 | Data Communications-AWS | Communication equipment for communication with MIPS | Data communication should at least be possible via fixed data communication cables (serial, Ethernet), dial up connections, GPRS or the most recent versions of mobile data communication, radio modems, satellite modems, wifi. In case of wireless data communication, the connection should be protected, i.e. unauthorized access should not be possible. | Demonstration | Very Important |
| 173 | C.DCO.1 | Data Communications Other | Communication equipment for communication with MIPS | Data communication should at least be possible via fixed data communication cables (serial, Ethernet), dial up connections, GPRS or the most recent versions of mobile data communication, radio modems, satellite modems, wifi. In case of wireless data communication, the connection should be protected, i.e. unauthorized access should not be possible. | Demonstration | Very Important |
| 316 | C.DCO.2 | Data Communications Other | Communication protection | Communication between all system components shall be protected against unauthorized access. This especially applies to dial up connections and mobile data communications such as GPRS/4G.[The NMHS may specify additional Communications security protections including logging of AWS/Smart Sensor Access, encryption,] | Demonstration | Essential |

# AWS/Smart Sensors

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | WMO Tag | Functionality | Requirement Heading | Requirement | Test | Importance |
| 187 | AS.AWL.1 | Alarms/Warnings/Logging | The AWS/Sensor shall notify the AWS Network Control if an alarm situation occurs | The AWS/Sensor should have the capability to notify the AWS Network Control if an alarm situation (defined in the AWS NC) occurs. It should be possible for the AWS/Sensor to actively initiate contact with the AWS NC to send the alarm immediately when the alarm occurs. Alternatively, alarm may be included in the regular data communication cycle if this cycle is based on, for example, 10 minute communication.[NMHS to determine method to silence the alarm] | Demonstration | Very Important |

# MIPS All

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | WMO Tag | Functionality | Requirement Heading | Requirement | Test | Importance |
| 169 | MIPS.AWL.1 | Alarms/Warnings/Logging | Logging of system information | Logging of system process and error correction, as provided by the computer operating systems, should be possible. It should be possible to turn this logging on or off by a system administrator. The system administrator can select the relevant system information to be logged (when logging is switched on). | Demonstration | Very Important (Regional Input) |
| 220 | MIPS.AWL.2 | Alarms/Warnings/Logging | Exceptions | “Exceptions” are states outside the scope of the “normal operational state” of the instruments, AWS’, computers, data communication equipment and connections, the MIPS, software, algorithms, etc. Each exception should be assigned an ID and a description, and each should be time stamped and logged. | Demonstration | Very Important |
| 221 | MIPS.AWL.3 | Alarms/Warnings/Logging | Alarm list | All exceptions should generate an alarm that should be presented in an “alarm list”, that should be visible for all MIPS users. | Demonstration | Very Important (Regional Input) |
| 222 | MIPS.AWL.4 | Alarms/Warnings/Logging | Exception filtering | The MIPS should have a tool to filter exceptions from the alarm list. It should at least be possible to filter on station, meteorological parameters, housekeeping data, start date/time, end date/time, alarm ID, unacknowledged alarms, acknowledged alarms. Filtering should be possible per single filter criterion and for all possible combinations of the filter criteria. A screen in which all possible filter criteria can be selected, should be used to initiate a filter based search in the alarm list. | Demonstration | Very Important (Regional Input) |
| 223 | MIPS.AWL.5 | Alarms/Warnings/Logging | Exception grouping | It should be possible to group and/or sort exceptions in a logical way (for example, per AWS, per meteorological parameter) and to display the exceptions per these groups. | Demonstration | Very Important |
| 224 | MIPS.AWL.6 | Alarms/Warnings/Logging | Notifications to user | It should be possible to configure the MIPS to send notifications to users in case exceptions, all notifications or for particular groups of notifications, occur. At least notifications per email should be possible.There are no specific requirements on how the data will be stored. However, for many reasons it would be convenient if data is stored in a relational database, which provides many of the data management tools as standard features. Storage in files is possible, bur many of the required tools will have to be provided separately.Disk space should be dimensioned so that at most 50% of the capacity is used during normal operation. Storage structure should be defined in detail by the supplier. | Demonstration | Very Important |
| 225 | MIPS.AWL.7 | Alarms/Warnings/Logging | Acknowledgement of exceptions | Each exception should have an “owner” group: the technician group, the meteorological administrator group or the system administrator group. Individuals from the groups can acknowledge only the alarms that are owned by their group. Acknowledgement should be done when a problem is solved or when the reason for the exception does not exist anymore. | Demonstration | Very Important |
| 226 | MIPS.AWL.8 | Alarms/Warnings/Logging | Smart presentation of exception | The MIPS may not present spurious exceptions. Repeated and duplicate exceptions from the incoming exception stream in a smart manner. For example, if an instrument is not operational, this may only be presented once every hour (configurable) and not every 10 seconds of the sampling cycle, and if the status of the alarm changes (instrument status from “non-operational” to “repaired”), it may be presented. Note that this requirement is relevant for presentation of alarms only, all alarms may be logged in the alarm log file.s, it may still be possible to see and read all the information. | Demonstration | Important |
| 228 | MIPS.AWL.9 | Alarms/Warnings/Logging | Access to log data | In the access to log data it should be possible to show the data of the complete observation network and/or of a selected sub-system. The presentation should be able to show the log data sorted or by using filters such as time (most recent or last first), error ID, alphabetical, etc. It should be possible to scroll back and forward in the data.Headers should show all relevant information, such as the name of a selected sub-system, time, date. Every line shows date/time and log message, flags, error ID, etc. For the complete observation network overview, every line also should show the sub-system name. | Demonstration | Very Important |
| 297 | MIPS.AWL.10 | Alarms/Warnings/Logging | Logging of information updates | The system should, whenever information is updated or deleted, log the following information:• account [related to a person or group of people]• terminal• date and time• the modifications made. | Demonstration | Very Important |
| 340 | MIPS.AWL.11 | Alarms/Warnings/Logging | Logging general configurability | The system may offer the possibility to specify for all logging facilities (without having to shut down the system or a part of the system):• whether logging is turned on or off• how long the log should be retained• where the log should be stored. | Demonstration | Important |
| 342 | MIPS.AWL.12 | Alarms/Warnings/Logging | Logging of diagnostics | The system should log a diagnostic message for each unusual event within the system that could affect the proper functioning of the system. | Demonstration | Very Important |
| 344 | MIPS.AWL.13 | Alarms/Warnings/Logging | Classification of diagnostics | The system may subdivide diagnostic messages into classes, based on the severity of the malfunction the diagnostic relates to. | Demonstration | Important |
| 345 | MIPS.AWL.14 | Alarms/Warnings/Logging | Logging of diagnostics configurability | Apart from logging general configurability, the system should offer facilities to specify for each diagnostic message (without having to shut down the system or part of the system):• whether information should be logged• what message types, including unrecognisable incoming data, should be logged. | Demonstration | Very Important |
| 971 | MIPS.AWL.15 | Alarms/Warnings/Logging | Logging retention period | The system shall retain logged data for a period of [[Time period to be determined by Customer, at least 7 days is recommended]]. The retention period shall be configurable. | Demonstration | Essential (Regional Input) |
| 293 | MIPS.IT.1 | IT Security | Data access restricted by authorisation | In order to prevent unauthorised personnel from access or damaging information it is required that authorisation take place. Access to security and privacy sensitive information shall be by login procedure. Access authorisation is to be provided by the supplier, the customer shall decide which systems shall require login access. | Demonstration | Essential (Regional Input) |
| 295 | MIPS.IT.2 | IT Security | Access rights | The system administrator should be able to define and control the following access rights for each logical user:• the applications, or application functions, that can be executed by the account• the read and/or write access rights to system internal data. | Demonstration | Very Important |
| 161 | MIPS.CMS.1 | Configuration Management for MIPS | Management of the configuration parameters for data reception | It may be possible to configure and to manage the access and function of the storage system, database or files, using the following parameters:• Back-up location • Access (i.e. who has access to provide data, buffer limitation authorisation) | Demonstration | Important |
| 162 | MIPS.CMS.2 | Configuration Management for MIPS | Management of configuration parameters for data processing | It may be possible to configure the process of data transactions and processing of the received data sets and/or data reports. Parameters that may be configurable are, for example:• Control data to check the supplied data (files),• Adjustment of the default-priorities• Overview of the waiting queue• Changing manually the default priority settings concerning data processing | Demonstration | Important |