SOUTH EAST EUROPE
Jointly for our common future

Co-funded by the EUROPEAN REGIONAL DEVELOPMENT FUND

MONITOR II

Romanian EMIS technical requirements

Work package 4: Technical specification of the Romanian Emergency Management Information System (EMIS)

Monitor II

Romanian EMIS technical requirements

1.1 Business Requirements to Be Met by the System

1.1.1 The Emergency Management Information System (EMIS) must be an integrated computer database, communication and logic system designed to support responders during emergencies by giving them detailed, real-time information, allowing them to graphically integrate it and then transmit their decisions through the chain of command to the appropriate Emergency Responders and other actors involved in the Emergency Management procedures.

1.1.2 The EMIS must select and organize the various data collected and disseminated by a multitude of authorities involved in emergency management, and must process that data to enable the development and implementation of a clear plan of action in response to the emergency.

1.1.3 EMIS must enable the integration and use of real-time data from outside sources, such as meteorological, hydrological, seismologic and radiological information.

1.1.4 The EMIS must be an integrated information system within the National Emergency Management System (NEMS) connecting all the emergency operational centers and other stakeholders for streamline information sharing and decision support for both daily routine and emergency situations response operations, supporting all phases of emergency management: mitigation, preparedness, response, and recovery

1.1.5 The EMIS must map on the operational structures (Emergency Operational Centers - EOCs) of the National Emergency Situations Management System: National Emergency Operational Center[1] (NEOC), County Emergency Operational Center[2] (CEOC) and Bucharest Emergency Operational Center (BEOC), Ministry Operative Centers and emergency operational centers from other central public institutions (MEOC) and on the future operational environment presented in *Appendix 12 - EMIS Operational Model*. Within the EMIS, the emergency operational centers are acting as information hubs: the information is centralized at county level (CEOC and BEOC) or ministry/ agency level (MEOC) and then are replicated at the national level (NEOC). These locations must be interconnected by means of a WAN, built on the existing infrastructure of STS and MAI networks; the necessary equipment is procured, installed and configured through this project.

1.1.6 The EMIS must be a client-server application, allowing users in various locations to use the system, regardless of the core-components location.

1.1.7 For an overview of the overseen architecture of the EMIS please refer to *Appendix 7 - EMIS model and supporting IT environment*.

1.1.8 The main general business requirements to be met by EMIS are as follows:

a. Coordination of preparedness activities by:

- EMIS must allow the definition of the organizational structures of institutions, offices and organizations involved in emergency management.
- EMIS must provide the possibility to change organizations and data flows mapped into the system to reflect future changes of the emergency management system.

[1] Primary NEOC (NEOC1) in Bucharest – used for managing the normal situations; secondary NEOC (NEOC2) in Ciolpani – used for managing the emergency operations. NEOC2 is a replica of NEOC1, fully operational at all times, ready to undertake the role and task for managing the emergency situations at all times. NEOC2 is minimally staffed.
[2] One for each County

- EMIS must be able to assist planning the human resource usage and intervention forces belonging to the organizations involved in emergency management.
- EMIS must be able to maintain an up-to-date inventory and keep track of all material resource capabilities belonging to the government, private institutions, private organizations and/or private persons that can be used on preventive activities.
- EMIS must be able to maintain an up-to-date inventory and keep track of all strategic material resource capabilities that can be used in emergency management, including the planning of their usage.
- EMIS must be able to maintain an up-to-date inventory of all hazardous materials that fall under the scope of emergency management.
- EMIS must provide the ability to simulate emergency management scenarios and assist the corresponding emergency management exercises.
- EMIS must provide the ability to create, track and control the budgets needed for exercises as well as keeping accounts for intervention costs.

b. Coordination of emergency response activities:

- EMIS must be able to manage the assignment and tracking the usage of all required material resources and intervention forces belonging to either public or private sector in case of emergencies.
- EMIS must be able to track and coordinate aid supplies, including receiving, storage and distribution.
- EMIS must be able to provide the necessary data for informing the public/media on emergency situations and current events.
- EMIS must be self-sufficient for individual organizational units (NEOCs, MEOCs and CEOCs (including BEOC)). EMIS must provide continuity in the event of temporary interruption to the communications link between systems involved, using a distributed system architecture and mobile applications
- EMIS must be able to present evacuation options in affected areas

c. Support the mitigation activities:

- EMIS must provide tools for centralizing the information and assessing the casualties (injuries, fatalities).
- EMIS must provide tools for centralizing the information and assessing the damages and material losses
- EMIS must implement extensive documentation features and case logging capabilities, allowing the complete, post-event replay and analysis of the activities of the emergency situations.

d. Other general business requirements

- The EMIS features must be implemented in accordance with Romanian Administration structure and current legal rules.
- EMIS must provide support for the complete process chains, from planning through implementation and execution to the completion of operations.

- EMIS must be able to use emergency management workflows in order to define information routes through the system
- EMIS must have a user interface that provides users with all relevant integrated functions
- EMIS must provide an integrated solution, so that data would be created only once and used where required throughout the system; static data that is common to various modules within the system will be maintained in one central database used by all other application components.
- EMIS must have the option to use predefined contingency plans and alternative scenarios.
- Based on the scenarios, EMIS must allow for planning the deployment of intervention contingents. Based on the stored scenario, EMIS will provide all the necessary information so that these contingents are equipped and staffed from the base with all the pieces of equipment that are required for the scenario.
- Based on contingency plans and alternative scenarios, EMIS must have the options of predefining operation contingents and their deployment.
- EMIS must allow defining the assignment (chain of command) and support relationships between the deployed units. The currently used assignment mapping must be taken into consideration when implementation services are performed.

1.1.9 Legal codes and regulations affecting the implementation of the system. A comprehensive list of the legal documents, along with a list of international legal documents that regulate or have impact on the Romanian national emergency management system can be found in *Appendix 8 - Relevant Romanian and International Laws and Regulations*.

1.2 Functional Performance Requirements of the System

Functionally different components of the system have different performance requirements. These requirements are grouped by the location of the emergency operational center.

1.2.1 NETWORK PERFORMANCE REQUIREMENTS

1.2.1.1 The Local Area Network (LAN) infrastructure connecting the servers at each emergency operational center must support 1Gbps, full duplex network speed for all server machines connected.

1.2.1.2 The LAN infrastructure for emergency operational center workstations must support at least 100Mbps, full duplex network access for all workstations with at least a 1Gbps, full duplex uplink connection to the server switch at the MEOCs and CEOCs (including BEOC) and at least a 2Gbps, full duplex uplink connection to the server switch at the NEOCs.

1.2.1.3 The firewall and IPS/IDS solution must support at least 200Mbps full packet inspection speed at the interface of the emergency operational centers LANs and the EMIS national backbone network.

1.2.2 DATABASE PERFORMANCE REQUIREMENTS

1.2.2.1 The EMIS application and the underlying database infrastructure must be implemented using a fully distributed hierarchy; the databases at NEOC1 being the masters, all mirrored to NEOC2, where the term “mirroring” refers to the database duplication technology used by most major database vendors.

1.2.2.2 The CEOCs (including BEOC) and MEOCs instances of the EMIS application must be fully operable even if the network connection to the NEOCs is permanently broken (for no longer than

30 days, longer outages need not be considered by the implementation). Consequently, all local instances of the EMIS application must be writable, with a carefully designed replication technology to avoid database corruptions when the broken communication lines are restored and data communication towards the NEOCs resumes.

1.2.2.3 The NEOC databases must support at least 250 concurrent users (125 performing queries and 125 performing database updates at the same time) with a design that will allow the scaling up of the database solution for 500 concurrent users.

1.2.2.4 The MEOCs and CEOCs (including BEOC) database instances must each support 25 concurrent users, with a scalability requirement of supporting 50 concurrent users.

1.2.3 EMIS APPLICATION PERFORMANCE REQUIREMENTS AT NEOCS

1.2.3.1 Users working at MEOCs and CEOCs (including BEOC) locations must be able to interface with the corresponding local EMIS application servers instead on the central, NEOC based EMIS application servers. Therefore the core EMIS application at NEOCs must be able to serve 135 concurrent users.

1.2.3.2 Additional components of the system, such as email messaging, file server access, etc, must be sized to accept at least 135 simultaneous user connections.

1.2.3.3 The Directory Services database must be sized to accommodate 25,000 user accounts.

1.2.3.4 The Web server solution that will service public information dissemination must be constructed so that it will be highly and easily scalable (must be able to scale up from a single server to a Web server farm); while at the initial implementation it must be scaled to accept 100.000 visitors per day (aggregate, not individual IP addresses) and 1.000.000 page impressions (PI) per day, it must be scalable up to 2.000.000 visitors (aggregate, not individual IP addresses) per day and 40.000.000 PI per day. This publicly accessible web server architecture must be implemented at both NEOCs.

1.2.3.5 The response time of the EMIS application must not exceed 5 (five) seconds for 95% of all kinds of application-related transactions on the LAN, with the exception of report generation and login operations.

1.2.4 EMIS APPLICATION PERFORMANCE REQUIREMENTS AT MEOCS AND CEOCS (INCLUDING BEOC)

1.2.4.1 The EMIS application at MEOCs and CEOCs (including BEOC) must be able to serve 108 concurrent users. Additional components of the system, such as email messaging, file server access, etc, must be sized to accept at least 108 simultaneous user connections.

1.2.4.2 The response time of the EMIS application must not exceed 5 (five) seconds for 95% of all kinds of application-related transactions on the LAN, with the exception of report generation and login operations.

1.3 Related Information Technology Issues and Initiatives

1.3.1 There is currently no information system used in Romania that would classify as a full featured Emergency Management Information System (EMIS).

1.3.2 There are a number of systems operated by various government agencies/authorities that must be interfaced by the future EMIS application. Some of these systems serve as data input for the EMIS, while others will require a deeper level of integration.

2.0 General Technical Requirements

2.0.1 LANGUAGE SUPPORT

All information technologies must provide support for the Romanian language. Specifically, all display technologies and software must support either of the ISO 8859-2, ISO 8859-16 or UTF-8 character set and perform sorting according to Romanian dictionary order, case-sensitive.

2.0.2 DATES

All information technologies must properly display, calculate, and transmit date data, including, but not restricted to 21st-Century date data.

2.0.3 ELECTRICAL POWER

All active (powered) equipment must operate on 230V +/- 10V, 50Hz +/- 2Hz]. All active equipment must include power plugs standard in Romania.

2.0.4 ENVIRONMENTAL

Unless otherwise specified, all equipment must operate in environments of 10-30 degrees centigrade, 20-80 percent relative humidity, and 0-40 grams per cubic meter of dust.

2.0.5 SAFETY

2.0.5.1 Unless otherwise specified, all equipment must operate at noise levels no greater than 55 decibels.

2.0.5.2 All electronic equipment that emits electromagnetic energy must be certified as meeting EN 55022 and EN 50082-1, or equivalent, emission standards.

2.0.6 PLATFORM REQUIREMENTS

2.0.6.1 The client side of the EMIS application must be operating system independent.

2.0.7 DEVELOPMENT REQUIREMENTS

2.0.7.1 The application software must be developed to utilize the 3-tier (database backend, application logic, client).system architectural model.

2.0.7.2 Application software must be modular, through object-based relations satisfying high cohesion - low coupling rules.

2.0.8 GENERAL SECURITY REQUIREMENTS AGAINST THE EMIS ARCHITECTURE

2.0.8.1 The proposed EMIS Architecture must appropriately implement means to ensure the *confidentiality*, *integrity* and *availability* (CIA) of data transmitted, stored or otherwise processed within the system.

2.0.8.2 All emergency operational centers' LANs, the data and all components of the EMIS application must be protected from unauthorized access. More detailed security requirements will be listed in chapter 2.4.3 of this document.

2.0.8.3 The access to classified information is allowed, with the observance of the need-to-know principle, only to those individuals who have personnel security clearances or access authorizations, valid for the classification level of information required for carrying out their duties (*Appendix 1 - Security Aspects*). Therefore, the Supplier shall obtain a security clearance both for the firm (industrial security clearance) and for individuals, after the contract signing. These clearances are issued by the "The National Registry Office for Classified Information" (www.orniss.ro).

2.0.9 GENERAL RELIABILITY REQUIREMENTS

The EMIS architecture must ensure timely and reliable user access to all functionalities and data. See paragraphs 1.2.3.5 and 1.2.4.2 of this document for details on this requirement

Software Specifications

System software and all corresponding software will be provided by the Supplier, including database, business application, management, etc, software. Besides the EMIS application itself, a complete supporting backoffice infrastructure will be built by the Supplier.

2.1.1 EMIS APPLICATION, GENERAL REQUIREMENTS

General system requirements against the EMIS are the following:

Fit within an enterprise services architecture framework, which supports cross organizations, cross application interoperability, collaboration & integration.

Must support XML data integration & exchange.

Incorporate a business process/ workflow engine/solution.

Incorporate a tool for master data harmonization & management (such as database maintenance functions, dump-load scripting automatization, transaction archiving, database consistency check and fix, automatic save and synchronization, start- stop procedures, logging).

Include analytics & reporting tool set with pre-built content for resource management.

The EMIS solution must have a front-end web server for public information dissemination. The actual contents published on this Website will be defined by responsible GIES/ MAI personnel.

The front-end Website of the EMIS suite must be webserver and operating system independent.

All the contents published on this Webserver must be accessible for everyone.

The front-end Webserver must be separated from the NEOC network by the NEOC firewall – the Webserver must be placed on a dedicated interface of the NEOC firewall cluster.

Dynamic data communication between the front-end Webserver and the EMIS application will be allowed; the exact data to be communicated will be defined by NEOC personnel responsible for public information dissemination.

The front-end webserver's authentication system (for write and administrator-level access) must be integrated with the central Directory solution.

Role based access control must be implemented for editing content on the front-end Webserver.

The EMIS application must be database independent, by supporting more than a single market leader database technologies, such as Microsoft SQL Server, Oracle RDBMS, IBM DB2, Sybase ASE.

The EMIS solution must be customized for the standard operational procedures, informational flow and organizational structure of the Romanian Emergency Management System.

The EMIS application must be web based (for the client side).

User access to the system must be role-based.

It must incorporate tools for creating/customizing flexible & friendly user interfaces.

The aim of the EMIS is to help the work and efforts of emergency professionals in a way that its use does not slow down the emergency management procedures. Since it is a highly specialized application, its functions map very closely to the major task areas of emergency management. The following functions listed here, would be part of the integrated application. The list of essential system functions is presented in the following subchapters.

EMIS application Key Functional Areas

Incident Management

The solution must incorporate incident handling functionality which will enable operators, specialists & key personnel to identify, record, track and trace incidents, action taken and follow up.

The solution must provide standard Customer Relationship Management (CRM) functionality, such as contact management, contact lookup, contact search.

The solution must provide an integrated view, having as the main object the citizens, which supports casualty, missing, deceased, volunteer and other classification information around a core master person record.

The solution must support post emergency case management, for example to cover investigations, follow up reports, lessons learned materials and follow up activities.

The system must provide personnel notification using different means of communications: telephone, SMS (Short Message Service), email and fax.

The incident management function must be integrated with the following functions/modules: Logistics & Supply Chain Management, Task Force Creation, Finance & Procurement, Human Resources.

Risk Management

The solution must incorporate a risk register function for risk identification, registration, classification and effects assessment functions.

This risk register must be accessible for all emergency management personnel.

Hazard/ Emergency Monitoring and Measurement

The solution must be capable of receiving and analyzing key emergency management data such as performance data of emergency actors (reaction time, materials and resources used), readouts of various sensors/controllers (manual data feed only), etc and must be capable of alerting/ triggering activities, responses or broadcasting capabilities based upon pre-determined or ad-hoc distribution lists.

This functionality must be integrated with incident management capabilities so that key responders are notified from within the system.

Emergency Management Alerting & Notification

A key requirement for the Romanian Emergency Management Information System solution is for a national system/network which provides for structured, targeted, tiered& responsive alerting and notification of key threats, vulnerabilities and hazards for emergency personnel.

The solution must enable rapid broadcasting of a change/potential emergency situation.

This capability (broadcast issuing and receiving) must be role-based.

This capability must be workflow – based.

Emergency Preparedness & Mitigation

The solution must provide, for planning and simulation, capabilities which support pre-emergency contingency planning and preparation.

The solution must be capable of supporting the planning, deployment and tracking of personnel, vital supplies, transport, command posts, materials and skills to specific emergency situations.

The solution must support templated/checklisted deployment plans for specific emergency situations

Emergency Management - Response

The solution must be able to manage the creation and assignment of task forces and specialist teams.

Logistics and supply chain management, human resources, finance and procurement, assets and critical infrastructure functions must be integrated as part of the response process, by integration of the corresponding functions/modules.

The solution must incorporate integration with fully functional self-contained GIS software. Although this requirement is listed here, under the Response phase, the GIS must be integrated into the solution in such a way that it can be used in all phases of emergency: mitigation, preparedness, response and recovery.

The following GIS technical requirements must also be met:

GIS must display Tiff format.

GIS must display DTED Level 0, 1 and 2 formats

GIS must load, use and display ESRI-Shape formats

GIS must support Geographical, Mercator and Transverse Mercator projections

GIS must support WGS-84 and ED-50 datum

GIS must support UTM and Lat-Long coordinate systems

GIS must have Pan-Zoom functionality

GIS must have map layer creation, deletion and display capabilities

GIS must have the capability to save any displayed map view including the environment variables (map layers, coordinate system, object groups, datum, scale, dimension etc.)

GIS must provide ability to load a saved map view

GIS must provide the ability to save the current map view as a JPEG file

GIS must provide a customizable drawing tool/palette for creating, modifying, placing shapes and text on map layers and for creating legend for a layer (single symbol, graduate color or unique value).

GIS must support spatial queries with FIND/SEARCH functionality.

GIS must support a JOIN functionality to connect with external sources (CSV, DBF)

GIS must provide an identification tool capable of displaying the information contained within the layer database: ATTRIBUTES.

GIS must support printing functionality on different paper formats from A0 to A4

GIS must support export into ESRI formats.

The solution must incorporate integration with legacy systems and applications listed later in this document (section 2.5.4.)

The solution must be able to present the availability of resources and their ability to be assigned to various tasks.

The solution must incorporate roistering & time management functionality for both emergency operational centers and intervention unit personnel.

Classification of emergency, automatic triggering/alerting & tasking of resources must be capable within initial response capability.

The solution must include the ability to quickly create temporary teams/units.

The solution must include the ability to create and report temporary locations for storing equipment and supplies needed for interventions.

The solution must provide an open Application Programming Interface (API) reference documentation for programmers on all publicly accessible methods/functions, properties, objects, etc.

The solution must support evacuation area planning and management functionality.

The solution must support evacuation route planning.

The solution must support evacuation-related logistics planning.

The solution must support tracking/tracing capabilities for evacuated personnel/communities.

Emergency Management - Recovery

The solution must support program & project management for intermediate and long term post disaster/ recovery management.

The following recovery-phase functions must be provided by the system:

- support the management of reconstruction/sanitation works.
- support financial management for recovery efforts.
- support procurement for recovery efforts.
- support human resources management for recovery efforts.
- support analysis of recovery efforts.
- support the allocation & tasking of police, military & specialist personnel for deployment to maintain/re-establish & sustain public order.

The solution must support/enable NATO/UN/EU master data harmonization for equipment, materials, stock numbers etc.

Functional Modules of the EMIS application

The software technical requirements listed so far must be implemented as standalone EMIS functional modules. The modularity of the software must be demonstrated. The modules altogether must provide the following functionalities:

- Portal
- Business Intelligence
- Citizen Relationship Management
- Human Resources
- Finance & Procurement
- Logistics & Supply Chain Management
- Operational Resources Management (Shifts/Roistering/Scenario Planning)
- Program & Project Management
- Advanced Planning & Optimization for Scenario Simulation
- Task Force Creation

- Asset & Critical Infrastructure Protection
- Master Data Management
- Geographical Information Systems
- Messaging (email, instant messaging)
- Documentation and help system
- System administration (security)
- Personnel notification
- Real-time status board

S44 The EMIS application must be implemented in a way that all the functional needs of the various actors in emergency management are met. A list of these functional needs is found in *Appendix 13 - Data feeds requirements* of this section, which represents the starting point of preparing the Software Requirements Specification.

S45 The Software Requirements Specification must contain a complete description of the behavior of the system to be developed, including a set of use cases describing all of the interactions that the users will have with the System in order to met all the above requirements. Software Requirements Specification documentation must be prepared by the Supplier consulting the Purchaser representatives and will be approved by the Purchaser.

IT supporting environment: Backoffice modules of the EMIS architecture

Apart from providing the core emergency management functionality, the EMIS architecture must provide additional functionality in order to realize a self-contained backoffice software environment for the EMIS users. If the Bidder choose a solution based on Microsoft products, the license cost for these Microsoft products shall be **not** included in the bid price according to **Provisions of the agreement between the Romanian Government and Microsoft presented in Appendix 14.** In this case the Bidder should present a list of the needed Microsoft products and number of licenses for these products to be used in his solution.

In the following paragraphs specifications for these other functions can be found.

Central resource directory

The proposed solution must implement an LDAP directory service.

The LDAP solution must allow for a quick and simple replication and taking off roles in case of servers failures.

User authentication and authorization

Single-sign-on capabilities for users must be provided by LDAP servers (or LDAP connected authentication servers) installed at each emergency operational center.

The implemented system must provide two-factor authentication solution integrated with directory services (supplying token devices is not required).

An access control and rights management system for managing the user access to various modules and functions of the system according to their role and security level access must be implemented.

Auditing

Full user-transaction auditing capabilities with the ability to playback user activities must be implemented.

Central log collection must be implemented locally at the level of each emergency operational center.

Administration and maintenance

Two-level system administration model must be implemented, where local administrators (at MEOC and CEOC (including BEOC) locations) will administer the system from their own workstations while system administrators working at NEOCs will have full, secure remote administrative access to all subsystems installed at the NEOCs and at all (MEOC and CEOC (including BEOC) locations) as well.

The system must implement an automated software distribution solution for software installation, upgrading, updating, patching and removal.

Certificate services

A full, self-contained PKI infrastructure must be implemented as part of the EMIS framework.

Messaging Services

Full email server functionality (SMTP, pop3, pop3s, imap, imaps) must be implemented as part of the EMIS framework.

BO11.1 An instant messaging and collaboration subsystem must be implemented as part of the EMIS framework

The email subsystem must be integrated with the access control and rights management system.

The user database used for the entire messaging services module must be the same as for the LDAP directory.

The emails and instant messages must be archived locally at the emergency operational center server.

Content Management Services (CMS)

The EMIS system must provide CMS functionality. At least the following CMS functions must be provided:

- LDAP Directory integrated user management
- MAC/ RBAC rights management
- Configurable workflows, workflow engine
- WYSIWYG[3] (graphical text) editor for users
- Ability to handle MS Office files, at least Word and Excel
- Events calendar
- UTF-8 support
- Search engine (built-in or external)
- Customizable user views (dashboards)
- Ability to handle zipped files
- Direct (one click) connection to email
- Content scheduling/staging
- Inline administration (from the CMS environment)

[3] WYSIWYG - What You See Is What You Get

- Distributed administration
- Full user – action auditing (audit trail)
- The ability to create and customize sub-sites
- An open API to create additional web parts/widgets
- Drag'n'Drop content
- Undo functionality for users
- FTP protocol support
- Cache-ing support
- Instant messaging support (if not implemented by the messaging server)
- Contact management (if not implemented by the messaging server)
- Help desk/bug reporting

The common content must be published at NEOC and shared among all others MEOCs and CEOCs (including BEOC).

The CMS functionality must be implemented locally in all emergency operational centers.

All CMSes must be logically connected in order to share content among emergency operational centers.

Storage

A multipurpose (file/ print/ antivirus) server must be installed at NEOCs, CEOCs (including BEOC) and MEOCs.

Database Backends

A server configuration must be installed as the database backend with a two-node cluster at both NEOCs.

The NEOC database cluster must have an external expandable SAN solution (see BO27).

A server configuration must be installed as the database backend at the emergency operational centers.

The backend solution must allow for a quick and simple replication and taking off databases in case of servers failures, between all MEOCs, CEOCs (including BEOC) and NEOCs.

Backup Solution

A tape-library based backup solution (with the installation and configuration of the corresponding backup software) must be implemented at each NEOC, CEOC (including BEOC) and MEOC.

A complete backup plan must be elaborated by the Supplier.

SAN device support

A Storage Area Network (SAN) solution must be implemented at both NEOC locations for database and file storage.

System Management, Administration, and Security Specifications

General Requirements: In addition to the management, administration, and security requirements specified in each sections covering the various hardware and software components of the System, the System must also provide for the following management, administration, and security features at the overall system level.

Technical management and troubleshooting: the EMIS must provide tools for the management and troubleshooting of the infrastructure including event monitoring, alerting and management, remote control, hardware and software inventory.

User and usage administration: a complete event auditing subsystem must be provided that is capable of logging all system, application and security events occurring in the system, including the complete user transactions. See requirements BO6 and BO7 for more details.

Security:

Network perimeter security

All connections of the system to public Internet must be protected by deep packet inspection or application proxy firewalls.

At NEOCs a clustered firewall solution capable of hosting IPSec VPN tunnels must be implemented (2.2.3).

CEOCs (including BEOC) and MEOCs connections to the backbone (for EMIS communication) must be protected by at least a deep packet inspection firewall (2.2.4).

Antivirus/ antispam/ antispyware solution

All computers (be it servers or workstations) must have antivirus/antispyware software installed that provides real-time protection from malware.

The messaging servers must be equipped with a separate antispam solution to filter email traffic for unsolicited emails.

The firewall protecting NEOCs must have an embedded antivirus module for filtering HTTP and FTP traffic.

The client antivirus/antispyware solution must be centrally managed at each NEOC, CEOC (BEOC) and MEOC, with the possibility for selected NEOC administrators to access and manage the antivirus subsystems in CEOCs (BEOC) and MEOCs.

An automated antivirus/antispam/antispy software distribution solution for software installation, upgrading, patching and updating must be implemented.

Network Intrusion Detection/ Prevention (IDS/ IPS)

The NEOCs must be equipped with an inline IPS/IDS device, the sensors of which will be placed on (at least) the network segment connecting to the internal interface(s) of the firewall. The IPS/IDS device can not be implemented on the same hardware as the firewall.

IPS/IDS log files must be archived on the device itself onto long-term storage media (CD/DVD-RW, tape) separately from the general backup process and will not be held on the central log management server.

File encryption

Users' files must be encrypted on the fileserver using 3DES or AES encryption.

Users' file decryption keys must be archived and the archives will be stored in a specially secured location within the emergency operational center.

The use of file encryption must be compulsory and transparent for the users.

Network traffic encryption

Network traffic encryption will be provided in two ways. First, where Romanian regulations require, physical level encryption will be provided by the network service provider (typically STS) using its own proprietary devices (no Supplier action required here).

Where regulations do not specifically prescribe the use of given encryption algorithms and techniques but the traffic travels in channels not fully under the control of the emergency operational centers, the use of 128 bit SSL application layer encryption must be enforced.

Devices that are unable to communicate over either secure channel must only be allowed to access public parts of the EMIS system (that is, information for public dissemination).