United Nations Environment Programme

EP

UNEP(DEPI)/MED WG. 316/6
01 June 2007

ENGLISH

MEDITERRANEAN ACTION PLAN
MED POL

Meeting of the MED POL National Coordinators

Hammamet (Tunisia), 25-28 June 2007

MED POL INFORMATION SYSTEM
PROPOSED DATA MANAGEMENT POLICY

(PREPARED BY INFO/RAC)

UNEP/MAP
Athens, 2007

Table of contents

1. MED POL Data Access Policy

2. MED POL Data Access Procedures

3. Glossary of terms

1. MEDPOL data access policy

Chapter 1. of this document proposes an access policy for the MED POL data. An agreed policy would in fact provide Contracting Parties with a structured and consistent process to obtain the necessary access to MED POL data.

1.1 Why the need for a MED POL data policy

MED POL activities generate different kinds of data. There is a spectrum running from “raw data”, as directly observed data or measurements of the environment, through “processed data” to “information” and ultimately “knowledge”.

These data are considered the fundamental results of the MED POL activities; only through them MED POL can in fact help formulate the appropriate pollution assessment and control actions. The management and access to the MED POL data as well as their dissemination to the public audience, is the crucial point of this process. In this context, special importance pertains to raw data. While data may be manipulated by the researcher to obtain material for publication, reports, etc, data are also a resource in their own right. Properly managed and preserved, data can potentially be used and re-used by future researchers, institutions, etc and exploited educationally.

Environmental data are often irreplaceable; they are always unique, if only the timing of collection is considered. They can also be extremely expensive to collect. For these reasons MED POL attaches great importance to ensuring that maximum benefits are derived from data once acquired.

MED POL is therefore proposing a formal policy relating to data. It is essential that this policy and its implications are understood at management level throughout the MAP community. Managers will then need to ensure that appropriate guidance is passed down to all those who need it within their organizations.

The MED POL data policy is intended to serve the following important aims:

- to ensure the fully controlled access and use of the MED POL data
- to ensure the efficient and lawful management of the MED POL data
- to build a durable data foundation for the long-term development of the MED POL programme
- to sustain an integrated approach to data across the Contracting Parties
- to ensure appropriate access to information on the state of the marine and coastal environment within the field of application of the Convention and the Protocols and on activities carried out or measures taken within the implementation of the Convention and the Protocols, in order to give to the public the opportunity, as appropriate, to participate in decision-making processes relevant to the field of application of the Convention and the Protocols.

1.2. Data covered by the policy

The policy described her below covers all MED POL data extending from raw data to “information” and ultimately “knowledge”.

More specifically, MED POL data cover:

- the pollution monitoring data for the Mediterranean basin generated through the f MED POL state and trends monitoring programme, as initially submitted to MED POL
- data regarding pollution sources for the Mediterranean basin measured within the framework of compliance monitoring, as initially submitted to MED POL

- data relevant to reporting on the implementation of LBS, Dumping and Hazardous Wastes Protocols
- Other data and information requested by CPs
- All the processed data, model outputs, plots, documents, etc produced by the MED POL activities

The policy covers all the products of the MED POL activities, from raw data submitted by Contracting Parties to processed data and results of the MED POL activities.

The policy does not apply to notes and records that are the personal property of individuals in the MED POL system.

Only data after submission to MED POL are covered by this policy.

The MED POL data described above will be referred to in this document as “data”.

1.3 User profiles covered by the policy

Any entity (physical person or organization) interested in the data is referred to as a “user”. The data user may or may not be authenticated, and users who are not authenticated are called *anonymous users*. Any user may have one or more user profiles. A user profile is a logical categorization of users that allows definition of different levels of privilege for data access. Anonymous users are the *lowest* level of users in that they usually have the most restrictions.

The definition of user profiles allows correct management of data access. T he user profiles of the data policy are defined in the section “User profiles definition” below. The policy covers the described user profiles.

1.4 Statement of the proposed policy

1.4.1 Guiding principles for data access

Contracting Parties may agree on the following guiding principles governing the access to data:

- Access to data is subject to restrictions described in this document
- Restriction of access to data can be achieved either by means of DBMS or by organizational measures
- Data are delivered according to specified standards
- As much as possible, access to data should be unrestricted in order to facilitate the active involvement of the civil society in the activities of the MED POL Programme;

As it was stated in the document “CONCEPTUAL DESIGN OF THE MED POL PHASE III DATABASE” (ref. Doc. UNEP(DEC)/MED WG.202/2 (revised), MED POL includes trend monitoring of contaminants and loads, biological effects monitoring and compliance monitoring. Collection of data is obtained according to monitoring agreements signed between UNEP/MAP and Mediterranean countries. Monitoring agreements contain a description of the National Monitoring Programme including a list of sampling stations and parameters to be monitored, monitoring frequencies, participating institutes etc. The Agreement stipulates periodical reporting of monitoring data to the MED POL Unit. Basically, reported data consist of:

1) Monitoring data on the following matrices:

a) Biota

b) Sediments
c) Waters
d) Atmosphere

2) Supplementary data:

a) Certified material analysis data
b) Methods used for the analysis
c) Quality Assurance data

3) Compliance Monitoring data: Loads
4) Data and information related to the implementation of LBS, Dumping and Hazardous Waste Protocols

On the basis of these general classifications, MED POL has organized all the data in several subsets called reporting formats, which contain homogeneous measurements. According to the conceptual design of the current MED POL database, the policy of MEDPOL data uses the same classification, adding a further classification index: the data status of public (category I) or restricted use (category II).

Category I – Public data: This information is targeted for general public use. Examples include Internet website contents for general viewing and press releases.

Category II – Restricted data: Information not generally available to all Parties, such as raw data (those provided by Contracting Parties to MED POL), directory listings and internal (Intranet) websites. This category is the default data classification category.

In summary, data are classified accordingly in three indexes:

- Environmental index: the environmental topic to which they refer. The MED POL reporting format to which they refer and/or are contained.
- Country index: the country to which they refer.
- Status index: public or restricted.

Thus, the three indexes define different domains of data among all the data.

For example: a domain of data is made by the restricted data referring to biota measurements in Spain, another domain by the public data referring to sediment measurements in Tunisia, etc. A domain can also have elements.

The Data Stewards, in consultation with the Data Administrators, are responsible for defining which data elements fall into each data domain.

Users may request that the Data Stewards review the restrictions placed on a data element and/or the classification of data. All such requests will be submitted through a Data Administrator to the appropriate Data Steward. The appropriate Data Steward has final governance authority regarding matters of data restrictions and requests for access rights to the Data.

1.4.2. Data access

Data are accessible to users. Any user can have one or more user profiles according to the privileges he receives. The available user profiles are described in the following list.

1.4.3. User profile definition

Each user profile has defined permissions; permissions are the ability to do something. All the permissions of this policy refer to one or many definite domains of the data. According to the conceptual design of the MED POL database the proposed permissions in the data policy are:

- Permission to read data (including downloading), referred to in this document as “read permission”. The read permission refers to some definite domain of data. For example: read Italian atmospheric restricted data, read Syrian sediment public data etc.
- Permission to enter new data, referred to in this document as “enter new data permission”. The entered new data permission refers to some definite domain of data. For example: enter new biota-restricted data for Greece, enter new seawater-restricted data for Turkey etc.
- Permission to write and modify data referred to in this document as “write permission”. The write permission refers to a definite domain of data. For example: write the Egyptian biota trace metal restricted data, etc.
- Permission to manage (enabling/disabling/modifying) user access to a domain of data, referred to in this document as “user management permission”. The user management permission refers to the management of the user access to some definite domain of the data. For example, there can be the permission to manage all the user access to the France domain of restricted and public data, etc.

User profiles for the data are:

- Anonymous
  - Anonymous permissions: read permission data for public domain of data.
- Expert – has the following two attributes:
  - a selected environment topic of expertise
  - a given nationality
  - Expert permissions: read permission data for some definite domain of data.
- Contracting party – has the following attributes:
  - a given nationality
  - Contracting Party permissions: read and enter new data permissions for its own national domain of data
- Data operator
  - operator permissions: read and write all the data domains.
- Data administrator
  - Data administrator permission: user management permission for all the data domains.

1.4.4. Procedures for requesting data access

Detailed procedures and guidelines for requesting data access under this policy are contained in the MED POL Data Access Procedures. These documents shall be updated on an “as needed” basis, reflecting any changes to the process and/or roles involved.

Data steward, in consultation with Data administrators, are responsible for:

• Categorizing and/or re-classifying data elements and views

• Granting selective access to Data

• Educating authorized users on responsibilities associated with data access

• Informing technology specialists about data classifications to determine physical and/or logical controls required

On the other hand, it is the responsibility of authorized users and their respective business units to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.

The access to MED POL public data would be freely granted provided that the user agrees:

- not to use the information for commercial purposes;
- to acknowledge the source and display the link to the data provider (MED POL or any other data provider listed in the Data service). For all freely available MED POL information the acknowledgement should read: “© MED POL, Athens, <production year>”
- to help improve the quality of the data by noting and reporting any errors or omissions discovered;
- to help improve the quality of the Data service by giving feedback on functionalities and data packaging;
- to help improve the co-coordinated use of data by informing MED POL about applications that make use of the information;
- to help improve efficiency of environmental reporting by supplying MED POL with documented digital copies of data/maps/graphs and information derived from MED POL information, so that it can be re-used by MED POL with reference to the source;
- to supply MED POL with a copy of URL to all publications and other products based on products from its information and services.

Neither the MED POL, or the Contracting Parties or MAP, nor any person or company acting on their behalf would be responsible for the use, which may be made of the information in Data service. The contents of the product would not necessarily reflect the official opinions of the MED POL/MAP, its institutions or the international organizations and individual countries involved in preparing the product.

The designations employed and the presentation of material in the publication would not imply the expression of any opinion whatsoever on the part of the MED POL/MAP concerning the legal status of any country, territory, city or area or its authorities.

In no event would MED POL be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortuous action, arising out of or in connection with the use or performance of software, documents, provision of or failure to provide services, or information available from the Data service. The links will allow the user to leave the MED POL website. The linked sites are not under the control of MED POL. MED POL is not responsible for the contents of any linked site or any changes or updates to such sites. MED POL is providing these links only as a convenience.

The access to restricted data would be granted to authorized users, provided they:

- Observe any restrictions that apply to sensitive data;
- Abide by applicable laws, policies, procedures and guidelines with respect to access, use, or disclosure of information.

The unauthorized storage, disclosure or distribution of MED POL Data in any medium, except as required by the user profile assigned would be expressly forbidden, as would be the access or use of any MED POL Data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's personal curiosity or that of others.

Users would be expected to respect the rules described by this policy. Violations of the policy may result in loss of data access privileges and in sanctions as outlined in the MED POL disciplinary procedures.

Upon approval, the proposed policy shall be published on the MED POL website and widely notified among national authorities, the scientific community and other stakeholders.

2. MEDPOL data access procedures

Chapter 2. on data access procedures is in direct support of the *MED POL Data Access Policy* to which reference must be made. Chapter 2. sets forth guidelines and procedures for requesting access to MED POL Data, and in particular to Restricted Data as defined in the MED POL Data Access Policy. The access procedures shall be subject to periodic changes and updates, as necessary, independent of the policy described in Chapter 1.

The request for data access is managed by a two-level structure. The two levels of management are:

- Authorized requesters,
- Data steward.

The implementation of the request to the data access is the responsibility of the Data Administrator.

The procedure for requesting data access involves the following steps/conditions:

a) A user submits a request to the data access. The access request is initiated via email or applicable web form or fax or ordinary mail, and forwarded to the authorized requester.

b) The authorized requester verifies individual access requirements, and forwards access request to the appropriate Data Steward. The authorized requester is responsible to receive the incoming requests and to provide assistance to the requesters to submit an appropriate request.

In order to be processed, the request should be appropriate, i.e. it should fulfill the following requirements. It should:

(i) be complete, containing all the relevant information about the user, as specified below.

(ii) require appropriate permissions, permissions compatible with the role of the requester.

As required, the authorized requesters will provide assistance to the user to submit an

appropriate access request

c) The Data Steward reviews the request and decides to accept or reject the request.

If the request is accepted, Data Stewards in consultation with authorized requesters and data administrators, assign a user profile to the user.

Granted access is notified to Data Administrator to enable the data access.

Data Administrator enables the data access for the user, informs the user the way to access to the data according his/her user profile, notifies to Authorized requesters of the accomplishing of granting access.

Data administrators and authorized requesters will maintain electronic archives of all requests.

Users with national status submit their requests to the corresponding national authorized requesters and are reviewed by the corresponding national data stewards.

Users with international status submit their requests to the authorized requester at the secretariat and are reviewed by the data steward at the secretariat.

The structure of authorized requesters, data administrator and data steward allows to subdivide the work between all the countries and to allow a more efficient way to review and decide for the single request of access inside each single country.

The two levels structure allows subdividing the responsibility of the access management between a technical role (the authorized requesters and the data administrator) and a political one (the data steward).

Each country should have at least an authorized requester. He/She receives the requests from national users.

The secretariat should have an authorized requester. He/She receives the requests from international users

Each country should have at least a Data Steward. He/She decides to accept or reject the requests from national users. National Data stewards can be the MEDPOL National coordinators.

The secretariat should have at least a Data Steward. He/She decides to accept or reject the requests from international users. Data Stewards at the Secretariat can be a Secretariat officer.

It is sufficient to have a single Data Administrator at the Secretariat, who can also be the authorized requester for international users.

The form to access request to data should include the following information:

- Institution/organization name
- User name,
- Job Title
- Phone number
- What Data/Role and Why (national or MED POL data administrator will provide assistance)
- Access End Date

Note: Any change or extension to the original intended use of the data requested (as documented in the original access request), such as a new application being developed using data for which access was previously granted, shall require a new access request explicitly documenting such change or extension.

The submission of the registration form is performed either in the electronic form (online form or e-mail) or in hard copy (fax or ordinary mail). Online form and downloading PDF file would be found at MED POL website. The hard copy would available via ordinary mail upon request to the secretariat.

It should be recalled that when a user submits the registration form he/she enters a legal contract with MED POL, agreeing to abide by all regulations.

3. Glossary of terms

Application Server: The computer hosting the application that the general end-user terminal connects.

Availability: Time during which you can retrieve information when needed. Information can be unavailable due to destruction/erasure, system or network not working, or needed retrieval resources being overused.

Authorized Requesters: Unit heads or individuals with delegated authority to authorize and initiate access requests in accordance with established procedures by unit heads or higher-level management in their organizational reporting chain.

Authorized User (or Users): individuals or organizations authorized to access MED POL Data in the performance of assigned duties.

Computer & Network Usage and Security Policy (CNUSP): The GIT policy governing the behavior of individuals and organizations in the use of MED POL information technology resources.

Confidentiality: Preventing the disclosure of information to any person not authorized to view, copy, or distribute that specific information.

Data Access Policy (DAP): The MED POL policy established, governing the categorization of data and the appropriate access controls required based on that categorization.

Data Administrator: Individuals responsible for documenting and enabling user access to a

domain of MED POL Data.

Data Categorization:
The two categories of MED POL Data defined in the Data Access Policy are:

• Category I – Public Use: This information is targeted for general public use. Examples include Internet website contents for general viewing and press releases.

• Category II – Internal Use: Information not generally available to parties outside the MED POL and MAP, such as raw data (those provided by Contracting Parties to MED POL), directory listings, minutes from non-confidential meetings, and internal (Intranet) websites. Public disclosure of this information would cause minimal trouble or embarrassment to the Institute. This category is the default data classification category.

Data Stewards: individuals responsible to review the request to data access.

Data Views: A logical collection of data elements, possibly from multiple physical databases, that are assembled and presented according to a defined set of rules.

Denial of Service Attack (DoS): A computer attack typically from a single system to take advantage of a remote system vulnerability to deny legitimate system or resource use.

Digital Certificates: A high-security form of authentication - the exchange of short, encrypted files by the programmes that are communicating, which serve to authenticate the client and server processes to each other. There is an entire system of organizations and protocols that work together to create, authenticate, revoke, and use digital certificates. The user of a computer typically allows the programme(s) to use digital certificates by logging in to the system or programme with a user ID/password.

Disaster Planning: Creating, implementing, and testing plans and procedures for the continuation of essential business operations even after a disaster, such as an earthquake, hurricane, flood, extended power outage, terrorist incident, etc. Usually involves duplicated computing facilities, communications facilities, vendor agreements, employee procedures, etc.

Distributed Denial-of-Service Attack (DDoS): A computer attack by malicious code located on multiple systems where the intent is to overload the target computer(s) or network resources prevent legitimate system or resource use.

Encryption: Using programs and measures to encode information such that it cannot be decoded and read without knowing an appropriate key – usually a user-selected key.

Filtered: The process of examining a file or content acquired through the network or from media (e.g. CD or diskette) for harmful or malicious content.

Fingerprinting (of files): Creating a mathematical summary of the file that is usually sufficient to detect any change to the file, but can be stored compactly (e.g. a hash or CRC of the entire file).

Firewall: A device or program designed to control the network traffic allowed to flow to a computer or segment of the network.

Hashing: Generating a unique value for a specific file, program, or communication that provides assurance that the information is complete and has not been tampered with. Part of the goal is providing enough of a signature to confirm that the information is complete without

being able to generate the actual information from the hash.

Information Technology Resources: Computers, storage peripherals, network equipment and wiring, network-attached printers and fax machines.

Integrity: The amount of confidence that the information has not been modified in an unauthorized or incorrect way.

Intrusion Detection System (IDS): A network or workstation based system used to detect and notify critical individuals when an attack is launched.

Intrusion Prevention System (IPS): A network-based IDS that can automatically react and prevent attacks from being successfull. Special care must be taken with IPS to ensure that the system does not prevent communication that should occur, even during attacks.

Instant Messenger: A method for immediate communications between users

IP Spoofing: Providing a network address (IP address) that is not correctly assigned to purposely prevent others from locating the source for certain network traffic or messages.

ISO 17799: The International Standards Organization document defining computer security standards. The credit card vendors may have based their policies on this standard.

Keyboard Logging: Maintaining a file of the information input from the keyboard of a computer. This can be maintained on the computer or in a device attached to the keyboard.

LAWN: The Georgia Tech Local Area Wireless/Walkup Network. This authenticated network access provides wireless access to GIT and provides authentication for wired ports in some public areas.

Limited-access Room: A room that only a limited number of people possess keys to enter the room and authority to manage the IT equipment within the room.

Network Packet Capturing: Capturing information intended for others being transmitted across the network with the purpose of inappropriate examination later.

Newsgroups: Online discussion groups dedicated to specific topics

Phishing: Sending Spam noting an event requiring a person to provide personal information directly or go to a specially crafted website to provide personal information that is used for fraud.

Port Scanning: Using a program or manually examining all computer network ports (65,535 available) or a small subset on one or multiple computers.

Pre-logon banner: A message that is shown to the person attempting to login to a computer or communications facility BEFORE they are prompted to enter any authentication (user ID/password, biometrics, etc).

Spam (or unsolicited bulk e-mail – UBE, or unsolicited commercial e-mail – UCE): E-mail distributed without (and frequently against) the recipient's wishes to promote commercial offerings. This type of e-mail may represent 50%-70% of all e-mail on the Internet in 2004.

Spyware: Software installed on a computer (typically from a website) to monitor and report computer use.

Trojan Horse (programme): A programme which consists of malicious code, but which is promoted as or appears to be a useful program, in order to trick an unsuspecting person into executing the program. This program would not be self-replicating and is normally targeted at an individual or system.

Technical Authority: Individual (internal or external to the unit) designated by unit head with the expertise to certify and sign-off on technical compliance with published standards of all workstations and servers used by the unit for accessing or storing MED POL Data.

Technical Lead: The person designated by the unit head as the primary responsible party for information technology/information systems planning and implementation.

Technical Support Team: The group of people (where appropriate) handling information technology/information systems implementation and maintenance.

Two-factor Authentication: An authentication method requiring two items (beyond a user ID) for authentication. Typically, these items would be something you know (e.g. a password) and something you have (e.g. a number from a token, a fingerprint).

Unit: A fundamental workgroup identified in the official organizational chart.

Unit Head: An individual responsible for direct oversight of a Unit.

Unit-level Servers: Servers that provide critical information services for units, or ancillary systems that interface with centralized services, such as: Web servers, fileservers, print servers, domain name servers, file transfer servers, firewalls, network storage devices, DHCP servers, unit-level remote access solutions and other ancillary systems

Virus: Malicious software that is executed by the user. The virus will spread to other computers and/or programmes.

Voice over IP communications (VoIP): Telephone communications routed over a computer network using IP rather than a traditional telephone network.

Web Development: The design, development, implementation and management of front-end interfaces for web applications.

Wireless Access Point (AP): Any device providing connectivity from one computer or PDA to a network or other computer or PDA via radio frequency transmission.

Worm: A self-contained programme that runs itself on a system, which replicates to other systems without user intervention.

The above definitions may be revised in consultation and agreement with National MED POL Coordinators to reflect the changing nature of technology and the changing regulatory landscape.