Government of India & Government of The Netherlands

Technical Assistance
HYDROLOGY PROJECT

DHV CONSULTANTS &
DELFT HYDRAULICS with
HALCROW, TAHAL, CES,
ORG & JPS

VOLUME 9
DATA TRANSFER, STORAGE AND DISSEMINATION

OPERATION MANUAL

Table of Contents

1 INTRODUCTION 1

1.1 GENERAL 1
1.2 SERVICE, SUPPORT AND MAINTENANCE 1
1.3 SEPARATION OF DATA PROCESSING AND DATA STORAGE FUNCTIONS 2
1.4 STAFF FUNCTIONS DATA STORAGE CENTRE 3
1.5 STORED DATA 5
1.5.1 FIELD DATA 5
1.5.2 AUTHENTICATED DATA 5
1.5.3 TEMPORARY DATA 6
1.5.4 OBJECT DATA 6
1.5.5 META-DATA 6
1.5.6 MIS DATA 6

2 OPERATION 6

2.1 FUNCTIONS 6
2.2 SECURITY 7
2.3 DATABASE ADMINISTRATION 9
2.3.1 SUPPORT FROM OWNER DPCS 11
2.3.2 DATA IMPORT FROM LOCAL DPCS 12
2.3.3 DATA IMPORT FROM CENTRAL HIS SERVER 14
2.3.4 DATA IMPORT FROM HDU 14
2.3.5 DATA EXPORT TO OWNER DPCS 15
2.3.6 DATA EXPORT TO LOCAL DPCS 15
2.3.7 DATA EXPORT TO CENTRAL HIS SERVER 16
2.3.8 DATA EXPORT TO HDU 16
2.3.9 ADMINISTRATION OF DATA FLOWS 16
2.4 META-DATA AND CATALOGUE 16
2.4.1 DRF PROCESSING 17
2.4.2 GATHERING AND MAINTENANCE OF META-DATA 18
2.4.3 CATALOGUE GENERATION 18
2.4.4 SUPPLY OF META-DATA TO THE CENTRAL HIS SERVER 18
2.4.5 INTEGRATION OF META-DATA FILES 19
2.4.6 DISSEMINATION OF THE CENTRAL CATALOGUE 19
2.4.7 DISTRIBUTION OF CATALOGUE TO USERS ON CD AND VIA INTERNET / INTRANET 20
2.4.8 PROVIDE ACCESS TO CATALOGUE ON INTERNET, INTRANET AND CD 21
2.5 MANAGEMENT INFORMATION SYSTEM 21
2.5.1 MONITORING 21
2.5.2 DATA PROCESSING 22
2.5.3 REPORTING 22
2.5.4 MAINTENANCE 22
2.6 INTERACTIONS 23
2.6.1 DSC COOPERATION AT NATIONAL LEVEL 23
2.6.2 ADVISE USERS ON DATABASE CONTENT AND DATA RETRIEVAL OPTIONS 23
2.6.3 LIAISON WITH HDUS 24
2.6.4 USER RIGHTS, ACCESS, SECURITY 24
2.6.5 SUPPORT OF DPC COMPUTER USERS ON IT MATTERS 25
2.6.6 SUPPORT OF HDU ON IT MATTERS 25
2.6.7 MAINTAIN KNOWLEDGE BASE ABOUT DEVELOPMENTS IN IT PROFESSION 26
2.6.8 CONTROL OF ACTIVITIES OF SERVICE AND SYSTEM PROVIDERS 26
2.6.9 COMMUNICATION WITH VENDORS, SUPPLIERS AND SERVICE PROVIDERS 27

2.6.10 REPORTING ON DATABASES AND REPOSITORIES 27
2.6.11 FORMATTING PROCEDURES FOR IMPORT AND EXPORT 28

3 MAINTENANCE 28

3.1 COORDINATION 28
3.1.1 ORGANISING MAINTENANCE 29
3.1.2 LOCAL AND COLLECTIVE CHANGES 29
3.2 CORRECTIVE MAINTENANCE 30
3.2.1 DIAGNOSIS 30
3.2.2 CORRECTION 30
3.2.3 DOCUMENTATION 30
3.2.4 TESTING 30
3.2.5 IMPLEMENTATION 31
3.3 ADAPTIVE MAINTENANCE 31
3.3.1 UPGRADING 31
3.3.2 ENHANCEMENT 32
3.4 HARDWARE MAINTENANCE 33
3.5 ROUTINE MAINTENANCE 34
3.5.1 MAINTENANCE OF DATABASES 35
3.5.2 BACKUP PROTOCOLS, FACILITIES AND IMPLEMENTATION 35
3.5.3 BACKUP POLICY 37
3.5.4 ARCHIVAL PROTOCOLS, FACILITIES AND IMPLEMENTATION 38
3.5.5 FACILITATE ADAPTATION OF DATABASES 39
3.5.6 CONTROL OF COMMUNICATION SYSTEMS 39
3.5.7 MANAGE COMMUNICATION PROCEDURES AND PROTOCOLS 40
3.5.8 VIRUS PROTECTION AND FIREWALL 41
3.5.9 MAINTENANCE OF SOFTWARE 42
3.5.10 REPORTING ON H/W AND S/W STATUS, MAINTENANCE AND REPAIRS 42

4 FIRST LINE MAINTENANCE 44

4.1 MAINTENANCE ASPECTS 45
4.2 DISASTER CONTINGENCY PLAN 47

5 ANNUAL MAINTENANCE CONTRACT 48

5.1 COVERAGE 48
5.2 SERVICES 49
5.3 CHARGES 49
5.4 STANDBY EQUIPMENT 50
5.5 REPLACEMENTS 50
5.6 SOFTWARE 50
5.7 PREVENTIVE MAINTENANCE 50
5.8 NETWORK 50
5.9 RECORDS 50

Glossary

Authenticated data	fully processed data ready for archiving
BLOB	Binary Large OBject
Catalogue	meta-data with search and selection tool
CD-R	Recordable CD-ROM
CD-R/W	Rewritable CD-ROM
CD-ROM	Compact Disk type Read Only Memory for computer use
CGWB	Central Ground Water Board
CGWBDPC	CGWB data processing centre
CSV	Text based data file format with Comma Separated Values
CWC	Central Water Commission
CWCDPC	CWC data processing centre
DAT	Digital Audio Tape
DLT	Digital Linear Tape
DPC	Data Processing Centre
DRF	Data Request File
DSC	Data Storage Centre
DVD	Digital Versatile Disk
Encryption	Coding data to make it accessible to key owners only
FAQ	Frequently Asked Questions
Field data	Observed data entered in GW/SWDES passing data entry tests
FTP	File Transfer Protocol
GIS	Geographical Information System
GW	Groundwater
H/W	Hardware
HDS	Hydrological Data Supplier
HDU	Hydrological Data User
HIS	Hydrological Information System
HLTG	High Level Technical Group
HP	Hydrology Project
IMD	Indian Meteorological Department
ISDN	Integrated Services Digital Network
LAN	Local Area Network
Observed data	Data collected in the field
PDF	Portable Document Format
RAID	Redundant Array of Independent Disks
S/W	Software
S/W	Software
SCSI	Small Computer System Interface
SGWD	State Groundwater Department
SGWDPC	State Groundwater Data Processing Centre
SI	International System of Units
SQL	Structured Query Language
SW	Surface Water
VPN	Virtual Private Network
WAN	Wide Area Network

1 INTRODUCTION

1.1 GENERAL

This section of the Operation Manual is dedicated to the data centres in general and the DSC in particular. The manual addresses the day to day operation and maintenance procedures at a general level. The aim of the manual is to give guidelines to avoid omissions in the operation and to ascertain an operation methodology common to all data centres. It is assumed that the data centre (IT) staff has a professional attitude and is properly trained to perform all the tasks adequately and to organise and execute the minute details of the day to day operations. Hence, no application level details are given here.

With respect to the IT procedures, the DPCs have much in common with the DSCs. Many of the operational procedures as defined here do also apply for the DPCs.

General information about the concept of the DSC can be obtained from Volume 9, Data Transfer, Storage and Dissemination, Design Manual.

The software system was supplied with documents and manuals, required to operate, maintain and configure the system at the user's specific environment. For technical details these documents should be consulted, they include:

- Software system general description and diagrams,
- List of modules included, and a short description for each module,
- User's Guide - containing all the screen and menus, explaining each function and the use of it. The user's guide is in hypertext with printer support,
- Error handling - message list and error handling for each message,
- On line Help is to be supplied as integral part of the software system, to assist the users during operations,
- A FAQ list is available to the Catalogue users, and
- Database maintenance guide.

Further, at professional level, the software system includes specific manuals, required to effectively use the DBMS and tools, which are part of the system. These include:

- Manuals and User Guides for the databases and tools used by the software system,
- Manuals and User Guides to the GIS tools used by the software,
- Manuals and User Guides for development tools and programming languages which are required to operate the system,
- System Maintenance Guide - containing the information required to operate and maintain the system by the Data Centre staff, and

1.2 SERVICE, SUPPORT AND MAINTENANCE

Support Provider

The uniformity of the system, which is of great importance, should be retained. Thus the software system should be centrally maintained. For this a support provider may be appointed. The support provider should be capable to render professional support for all the participating DSCs and to guard the uniformity of the systems. Due to the diversity of organisations, measuring networks and data types, it is unavoidable that differences in the systems emerge, however, the database design, the Catalogue and the data exchange procedures should be kept in compliance with a mutually (between the associated DSCs) agreed standard. Changes, if really required, should be limited to the system implementation; they should not affect the general design.

- **Local support** - an efficient, locally based and well-established Indian company renders support for the system software. The system is designed to be **sustainable** in the **Indian** environment, both hardware and software wise.
- **Software House** - the software supplier is M/s Rolta India Ltd.

The M/S Rolta (or the successor, if any) supplies service and support for all the deliverables. The support and service for the software includes for all the participating DSCs:

- Installation and customisation of the system (all items supplied, or agreed on)
- Installation and customisation of new versions of database and software tools (as supplied, or agreed on)
- Designing, implementation and support on the mechanism of replication, synchronisation and publication of the catalogue
- Development of new features and installation of new software versions in the DSCs
- Adaptation of the software for new versions of software tools and hardware platforms when required
- Removal of all ‘bugs’ and glitches in the software as they surface during implementation and operation
- Software support by phone and off-line support
- Software support in-house when needed, at the DSCs
- Advising the users about working environment and performance issues

1.3 SEPARATION OF DATA PROCESSING AND DATA STORAGE FUNCTIONS

In the HIS, the data processing and the data storage functions are separated. Data processing is done in the Data Processing Centres, whereas the computerised data archives are in the Data Storage Centres. Data processing is a technical task for which hydro(geo)logists are qualified, whereas final data storage, i.e. the library or archive functions, is the domain of database managers. Such a distinction is absolutely necessary:

- since processing and storage are different disciplines, which require different expertise, tools, hardware support, activities and responsibilities,
- to guarantee discipline in building the database and its sustainability on the long term,
- to make sure that for design and decision making valid data , which passed all steps of validation, are being used,
- to avoid mixing of fully processed / authenticated data and data still under processing,
- to register and control receipt and supply of authenticated data to and from the database in a formalised manner,
- to ensure compatible database configuration and protocols by all agencies,
- to maintain a professional data security system under which each organisation maintains its independence for data circulation and user authorisation, and
- for an easier updating / replacement in case of new developments in either data storage or data processing tools.

1.4 STAFF FUNCTIONS DATA STORAGE CENTRE

Activities

The Data Storage Centre (DSC) acts as a data archive. The DSC monitors the regular inflow of field and processed data and controls the dissemination of authenticated meteorological, hydrological and geo-hydrological data. In the DSC no data processing is being done.

In a Data Storage Centre, the following activities take place:

- management of the database, storing the field and processed meteorological, surface and groundwater quantity and quality data,
- updating of the data availability records,
- generation of the meta-data and HIS-Catalogue,
- control of supply of field / laboratory and processed data by the State and Central Organisations in accordance with the procedures agreed upon under the Hydrology Project,
- control of data retrieval by the State and Central Organisations,
- control of data retrieval by the Hydrological Data Users (HDUs),
- communication with other Data Storage Centres, and
- communication with the central HIS server.

While the data retrieval is an in-frequent process, which can hardly be planned by the staff of the DSC, the data transfer and storage is, to a great extent, a routine operation, which can be fitted into a proper schedule. Field data are collected at regular intervals and are transferred monthly / quarterly to the HISDB via the DPC. Less frequent, but with a fixed annual deadline is the entry of processed data.

In order to keep track with changes in communication technology and to make sure that the DSC can meet the user's requirements, professional assistance of data communication specialists is to be obtained. To communicate and interact with such specialist the DSC's IT Expert must have and maintain adequate technical background.

Staffing

Based on above considerations, the following staff is required to operate the Data Storage Centre:

1 Data Centre Manager
1 Database Administrator
1 Information Technology Expert
1 Secretary/Clerical Staff

Their tasks are summarised below:

Tasks of Data Centre Manager/Head of the Hydrological Information System

- overall responsibility for the operation of the Data Storage Centre,
- overall responsibility for the operation of the Hydrological Information System,
- liaison between DSC and the owner DPCs,
- liaison between DSC and the data providers (State and Central Organisations),
- liaison between DSC and the Hydrological Data Users,

- authenticate allotment of data access privileges in accordance with the State regulations,
- initiate preparation and distribution of the Catalogue of the HIS-database, and
- liaison between Hardware and Software service organisations.

Tasks of Database Administrator

- overall responsibility for the operation of the HIS-database,
- administration of data input streams,
- administration of data retrieval and security checks,
- preparation and maintenance of the Catalogue of the HIS-database,
- advise users on data retrieval options and database content,
- maintain the integrity of the HIS-database,
- monitor the timely delivery of data,
- monitor the synchronisation with related databases, e.g. between state and region,
- make backups and archive data,
- control the data communication processes and the applied protocols, and
- communicate with external service organisations (outsource highly specialised tasks).

Tasks of Information Technology Expert

- control of the Centre's computer hardware,
- control of the Centre's computer software,
- control of the Centre's communication systems, and
- maintenance of the Centre's hardware, software, peripherals, etc.
- support to the computer users in the Centre on information technological matters, and
- control of activities by service and system maintenance providers.

Tasks of Secretary/Clerical Staff

- all secretarial work, and
- act as a receptionist and control admittance of visitors to the Data Storage Centre.

Some final remarks

With respect to the staffing, the following remarks are made.

1. In Data Storage Centres, where data have a state strategic value and / or are politically sensitive, a **Security Officer** might be necessary to control the physical access to the database. If required, the layout of the DSC should include a secured area with controlled access.
2. The services of staff (secretarial, information technology and database expertise, security) can be shared with the Data Processing Centre(s) of which at least one will be accommodated in the same building. In some DSCs the task of the Data Centre Manager and the Database Administrator may be executed by a single person.

1.5 STORED DATA

The DSC supports and maintains separate databases for the following data groups, viz.:

- Hydrological data
  - Field data
  - Authenticated data
  - Object data
  - Temporary data
- Meta-data (derived from the hydro(geo)logical databases)
- MIS data

In each of the DSCs, the data structures are identical. This applies to all aspects of the hydro(geo)logical data and the related meta-data.

Any data value (**what**) is well defined in space (**where**) and time (**when**), but also with respect to source, measurement conditions, relationship with other data, owner, status of processing etc. This also applies to static data and semi-static data. All data items have a time label to define its validity in time.

1.5.1 FIELD DATA

The field data are measurement results, which have been corrected for administrative and self-evident errors only. The field data can be of any non-processed type, including:

- Geographical and space oriented data, i.e. static or semi-static data on catchment and hydrogeological features and hydraulic infrastructure
- Location oriented data, including static or semi-static data of the observation stations, wells and laboratories
- Time oriented data, covering equidistant and non-equidistant time series for all types of meteorological, climatic, surface water and groundwater quantity and quality data.

The field data has meta-data linked to it.

1.5.2 AUTHENTICATED DATA

Authenticated or processed data have successfully passed the thorough validation processes and are accepted for hydrological use. The authenticated data comprise the following types:

- Geographical and space oriented data, i.e. static or semi-static data on catchment and hydrogeological features and hydraulic infrastructure
- Location oriented data, including static or semi-static data of the observation stations and wells and laboratories
- Time oriented data, covering equidistant and non-equidistant time series for all types of meteorological, climatic, surface and groundwater quantity and quality data
- Relation oriented (derived) data on two or more variables/parameters used with respect to meteorological, climatic, water quantity, quality data
- Derived data and processing results, and
- Other results like aggregated data and extremes

1.5.3 TEMPORARY DATA

The Temporary data can be of any type or category, i.e. any temporary stored data, e.g. as part of data exchange between DPCs during data validation and processing. The Temporary data group is defined to distinguish from permanently stored data.

For reasons on quality assurance and traceability of processing steps, a log is kept about external data, i.e. data pertaining to owner or local DPCs, used for data validation and processing.

1.5.4 OBJECT DATA

The storage of object data in an administered repository is a service to the owner DPCs. The DSC caters for proper administration, the accessibility, archiving and backup of the objects. Only with the consent of the object proprietor, the existence / availability of objects may be publicised via the Catalogue. Maps, GIS layers, scanned maps, manuals, files, reports and other document types can be accommodated in the object repository.

1.5.5 META-DATA

The meta-data are derived from the data stored in the database and comprise information on the available field and authenticated data, object data and other categories in the DSC. Meta-data primarily identify the data in space and time, the data type(s) and the covered time period(s).

One integrating element of the HIS is the exchange of the meta-data between the DSCs. Each DSC receives the meta-data of the other DSCs and based on that, each DSC and its users can search for data that belong to any HIS station in the project area. However, users that are not involved in the data validation processes, i.e. the HDUs, only get access to the meta-data related to the authenticated data.

The meta-data is to be kept up to date. Each time new field/hydrological data is stored in the hydrological database the meta-data are updated as part of the storage process. As the meta-database also contains meta-data of the associated DSCs, a regular exchange of meta-data between the DSCs is taking place to synchronise and update the mutual meta-databases.

Depending on his authentication level, a HDU may get access to all meta-data or a subset thereof. In particular the field data and the object data have usage restriction, mostly limited to the operational area of the DSC.

1.5.6 MIS DATA

A limited number of key performance indicators have to be monitored by the DSC for MIS use. Incoming data flow (sources, amounts, types, dates of receipt), available data (aggregated) and meta-database status, user interactions (requests, supply destination, amounts, types) are monitored automatically.

2 OPERATION

2.1 FUNCTIONS

In order to maintain system stability, it is of great importance to have adequate and easy-to-use service and management tools for the DSC staff.

- **Loading data** – the software supports loading of data in the database. Part of the loading is a rigorous integrity checking facility.
- **Extracting data** - functions to extract any of the stored data from tables. Next to standard data types, also special structures like time series and map objects are supported efficiently.
- **Database service menus** - the software supports on-line and batch service menus and procedures for the use of the database administrator. These menus have been customised (and are flexible to changes) to implement the specific needs of the DSC. One of the batch services is data extraction based on the Data Request File, which is generated as the result of Catalogue search and selection.
- **On-line services** - the software supports on-line services menus for authorised user's, like owner DPCs
- **Periodic production of database meta-data** – tools to generate the DSC meta-data is part of the software. At regular intervals, a snapshot of the DSC meta-data is set apart for inclusion in the Catalogue. Subsequent changes to the meta-data are set apart for distribution via file transfer to any HDU that requests to update his Catalogue.
- **Activity log** - activity log function which includes the information about users login / logout date and time, data import / export / removal, Catalogue update, user requests, response time on user requests and similar performance indicators.
- **Users accounting** - accounting function module for future commercial purposes (such as: private users billing), enabling data dissemination and recording of data retrieved volume, connection time, special services etc.

The DSC is not authorised to alter any data in its administration on its own accord. However, deletion of data is supported based on user authentication.

2.2 SECURITY

Two main security aspects have to be identified, viz.:

1. protecting the system against damage and data loss

   Damage may be caused by natural disaster, accident, failure or on purpose. The DSC should be set-up, operated and maintained in such a way that damages are avoided. If any damages occur, effective and tested procedures should be in place to mitigate the effects. The damages may include the premises, hardware, software and / or the data.

2. access to the information

   Some of the data in the custody of the DSC may not be available for the general public but restricted to trusted users only. The access to the data is controlled by implementation of security protocols.

Protection of the DSC facilities

- The hardware of the DSC is protected against data loss by various methods.
- Fire extinguishing systems and tools are distributed over the building. They should be kept fully operational by scheduled maintenance and checking.
- The power supply is enhanced by Un-interruptible Power Supply units that are part of the power distribution to the computers to avoid sudden failure during power cuts or brownout. The hardware maintenance schedule should include the UPS units.
- To avoid loss of software and recorded data, regularly backups are made. Copies of the installation files of all software are made. Backups are stored at special places, selected for safety and located off-site, i.e. in separate buildings. The storage height above the ground should be sufficient to avoid damage during severe flooding. The physical access to the DSC should be

controlled in such a way that only DSC staff may be permitted access to the actual storage hardware and the data media.

- Access to servers and the LAN is controlled by a firewall. The firewall functions at IP-level (verifying IP and TCP addresses) and at application level. The settings of the firewall have to be regularly reviewed to ascertain the optimal level of protection.
- An anti-virus system protects data and files against manipulation, damage, loss or theft. The protection should cover individual PCs and also the LAN. The virus protection is stringently applied on all in-coming and out-going files. On the LAN and connected PCs and workstations, a continuous rigorous virus monitoring and scanning system is operated. Anti-virus software and associated data files need frequent upgrading. A properly configured upgrading subscription should be in place.

Limiting access to the information

The DSC implements various levels of a user authorisation system. Requests for data (through DRF) are checked against a User Authorisation Table, and access to data is only permitted after positive identification and authentication of the HDU and his specific privileges. The database design supports multiple security / access levels. HDUs holding a certain permission level may only get access to data belonging to that level and data of lower (less limiting) levels. The owner DPCs specify the data security levels and the user authentication and user permissions. The access to the Catalogue is free. Data is disseminated only after authentication.

The following security checks have been implemented:

Users Authorisation - User login to the system are checked, identified and authenticated, by user-ID and password. The tables containing the related data need to reflect the actual status, hence, they should be immediately updated whenever a change is made in the user’s authorisation / permission level, e.g. when the set of supported users is altered, security levels are changed, etc.

Users Authorisation - User login to the system are checked, identified and authenticated, by user-ID and password. The tables containing the related data need to reflect the actual status, hence, they should be immediately updated whenever a change is made in the user’s authorisation / permission level, e.g. when the set of supported users is altered, security levels are changed, etc.

User Registration – The system supports registration of the user’s data requests and the deliveries.

Data access privileges are follows:

- Database use
  - ❑ search and selection Catalogue access only)
  - ❑ data retrieval (read and retrieve privilege)
  - ❑ database update (read, write, update and delete privilege)
- Database management
  - ❑ Performing of data management and administration tasks (special supervisory privilege)
  - ❑ Privilege for using the standard SQL query generator and report generator option for dynamic production of queries and reports (pre-designed queries and reports are used by all users)

Auditing function: Displaying, logging and reporting of all activities by: date, time, user-ID, updates and deletes from the database. The MIS also uses the Auditing data. The focus may need to be adapted when requirements change.

Gateway: As part of a security scheme the DSCs may communicate with each other via a central gateway. However, this should not impair the data exchange with the local and owner DPCs and the DSCs. The data exchange should not depend on that gateway only, alternative methods of communication should be accessible at any time. The DSC should make proper arrangements with trusted service providers.

Encryption: Where needed and feasible, data may be delivered in encrypted format. A standard encryption system, such as SSL (secure Sockets Layer) or IPSec (IP security protocol), has been implemented. The system to manage the distribution of public and private keys is to be maintained. The distribution of the keys requires meticulous administration by the DSC. Further the information should be protected against unwanted access and / or manipulation.

User Administration Component: User Administration can be performed interactively and off-line by batch file.

The following functions are supported and should be properly administrated:

- create new users
- edit existing users (including password)
- delete users
- create new groups
- edit existing groups
- delete groups
- define/edit user permissions
- define/edit group permissions (as roles)

Presently, user-groups are not supported by the system.

The import tools support:

- data load audit trail (quality assurance reporting), and
- data load reporting. (success / failure on record by record basis).

Note that permissions to perform the above functions are controlled by the user's database access permissions.

2.3 DATABASE ADMINISTRATION

The DSC supports and maintains databases for the following data groups, viz.:

- Hydrological data
  - Field data
  - Authenticated data
  - Object data
  - Temporary data
- Meta-data (derived from the hydro(geo)logical databases)
- MIS data

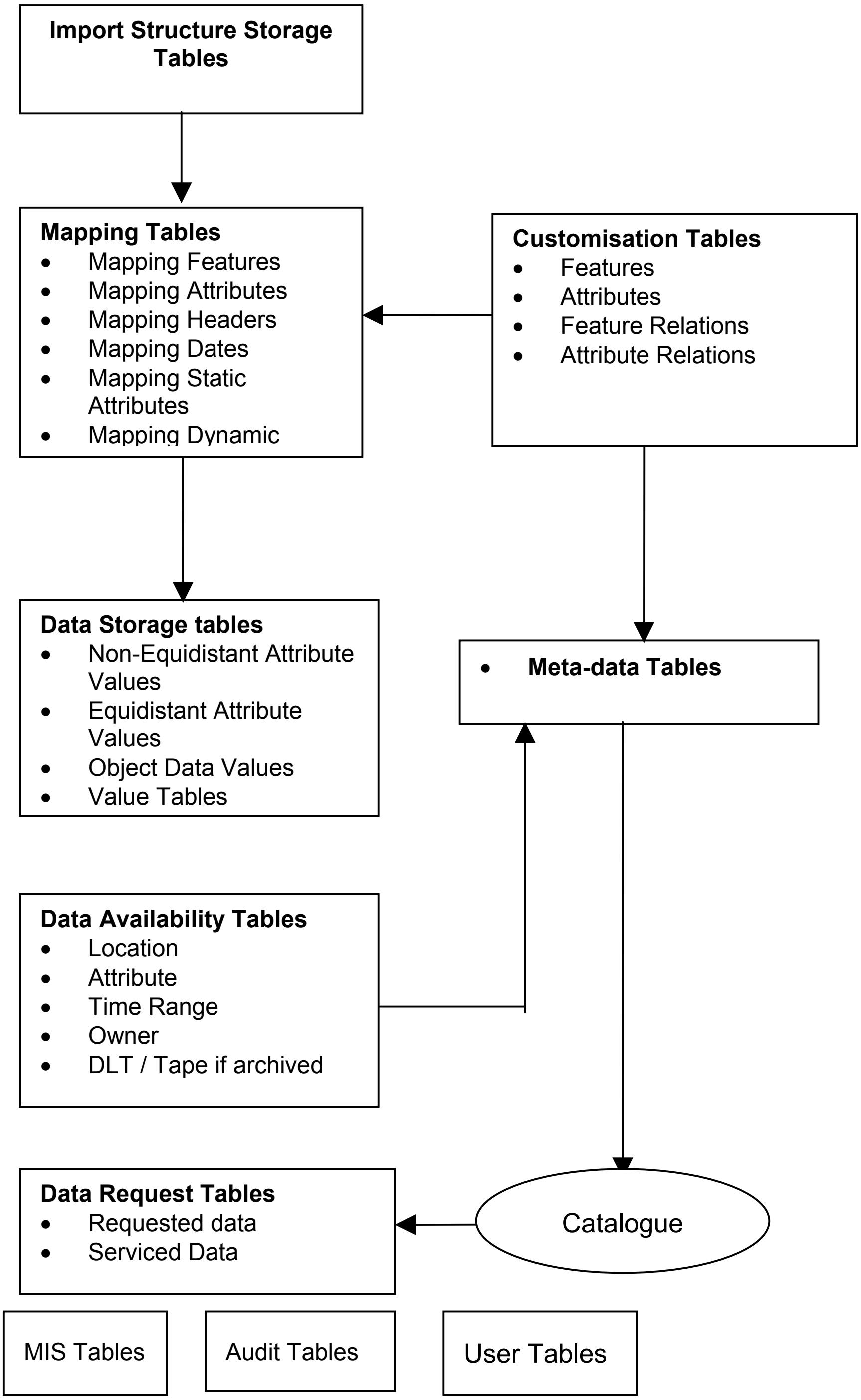


Figure 1.2: Logical database design

A major task of the DSC is control of the data storage in an effective way. This among others implies that the DSC verifies the integrity of the received data, stores the same in a reliable and systematic way, administers the import and export processes and the status of the stored data and safe guards the databases.

The integrity checks imply, among others, verification of the following:

1. the contents of the respective fields comply with the defined properties of these fields
2. time label values fall within the defined period of the data set
3. location identifiers match with the values as defined for the area (basin, aquifer)

4. the data should be complete, i.e. all relevant fields should contain proper values
5. basic access rights

The results of the integrity checks and in particular discrepancies thereof are reported.

All imports, exports, changes and data removals are to be duly reported to the respective owner DPCs. For each data element access rights are to be defined in concert between the owner DPC and the DSC. It is the task of the DSC that proper security measures are in place to prevent any unauthorised access to data in its custody. This applies to all forms of access including, writing, changing, removing, reading, changing of attributes etc.

2.3.1 SUPPORT FROM OWNER DPCS

The DSC basically stores data belonging to the owner DPCs. In addition to that Temporary data obtained from local DPCs is stored for data validation purposes.

For any standard data, the DPCs should deliver that data in compliance with the agreed formatting standard. Data types for which no standard has been defined, should be accompanied with a comprehensive description of the format of delivery.

A non scheduled type of delivery is replacement (up-dating) of existing data which could be necessary after discovery of flaws during data validation and reporting or identified problems with the data collection station.

Another prerogative of the owner DPC is the removal of stored data from the DSC but only if that data belongs to the owner DPC. Proper (safety) procedures have to be implemented to avoid accidental removal of data. These procedures have to be agreed upon between owner DPCs and DSC.

For the delivery of owner DPC data a schedule is to be agreed upon. The DSC monitors the actual progress of data delivery against the delivery schedule. In case any data delivery is overdue, the DSC urges the failing DPC to take appropriate action as required to meet its obligations. Before submitting any data to the database, the DSC checks the integrity of the delivered data. Deviations have to be reported to the owner DPC. For any delivered data the standard access rights should be defined.

Next sections describe the activities and processes in more detail.

Field data

The Field data is collected in a planned fashion according to a time schedule. In particular surface water data can be collected in tune with seasonal schedule; it does not make sense to collect water level data in the lean season in rivers that do not carry water. The data delivery should be linked to that schedule. The actual data delivery schedules depend upon the respective data sources. Groundwater data may be collected at regular intervals, e.g. monthly, irrespective of the season.

Prior to the start of a new hydrological year the DPCs should communicate the data collection and validation schedules with the DSC. Most importantly, the DPCs should inform the associated DSC about the time at which the Field data become available for storage in the database. It is one of the tasks of the DSC to monitor the timely (according to the scheduled milestones) delivery of the data and the completeness thereof. To allow efficient monitoring of the data delivery, for each owner DPC the DSC maintains a list with the details of when what data is to be received from which stations. In case DPCs do not meet the milestones, the DSC should forward alert messages to the related DPCs, e.g. on a weekly basis till the delivery takes place.

The present version of the DSC software does not support this in automatic mode, it is one of the important tasks of the DSC staff to monitor and follow-up the timely delivery of data.

The DPCs execute an initial validation of the Field data, i.e. the data is checked to be free of evident outliers and is unambiguously identified in time, space type and source. The data should include identification of the originating station, type of parameter and other essential particulars as well as a time stamp for each value.

Authenticated data

Much like with the Field data, the Authenticated data is also generated according to a time schedule. The processing generally is executed on data sets that cover an entire season or even a hydrological year. As a result, the Authenticated data comes available after a certain throughput time. The actual throughput time is station dependent. Also for the Authenticated data a delivery schedule should be prepared. The schedule pertaining to each DPC should contain the milestones indicating when what data is to be delivered at the DSC.

Much like with the Field data, the DSC monitors the actual data delivery and urges the failing DPCs in case omissions are detected.

Object data

Storage of Object data is primarily a service to the owner DPC; some of the Objects are published in the Catalogue for external HDUs, though.

The reception of Object data is mostly on ad hoc basis; the DSC does not have a task in monitoring timely delivery. The exception is Object data that is generated on a periodic basis, like yearbooks and station reports. For such Object data a delivery schedule is to be agreed upon and implemented.

The Object data is delivered as files and is stored as such without processing. Groups of files may be packed (zipped) into a single file, e.g. in self-extracting format. As with any data, the particulars of the Object data have to be properly administrated, access rights allocated etc. The delivery of Object data is limited to the owner DPC only.

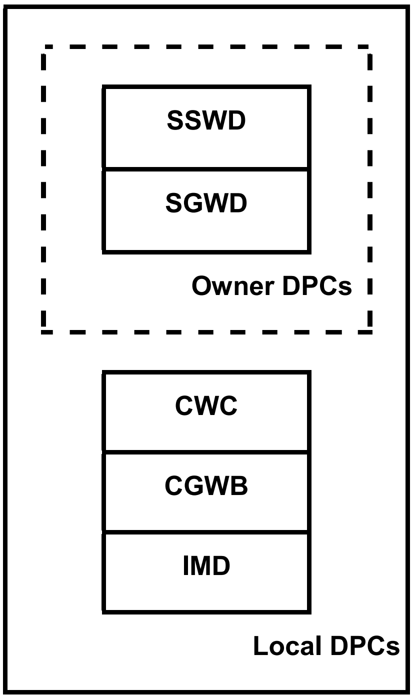
Temporary data

Temporary data is not imported from the owner DPCs but from local DPCs. However, the owner DPC, on request of a local DPC, may identify Field, Authenticated and / or Object data that is to be made available (temporarily) for the local DPC to enhance the data processing. The local “receiving” DPC will store the data in its Temporary data repository.

2.3.2 DATA IMPORT FROM LOCAL DPCS

The data are supplied by:

- owner DPCs
- local DPCs, and
- other sources



Local DPCs are related to the service area of a DSC, e.g. for a state data storage centre all DPCs that are active within the state boundaries are local DPCs.

Owner DPCs form a subset of the local DPCs, they are the suppliers of the hydrological data in the DSC. Each owner DPC has a direct link to the DSC. At state level, owner DPCs are SGWDPC and SSWDPC; they are linked to the state DSC. At national level, a regional SW/GW DPC may be linked to its own DSC.

The users of the data include:

- owner DPCs
- local DPCs, and
- HDUs

HDU is short for Hydrological Data User.

State X

Table 2.1: Local and Owner DPCs

An overview of suppliers and users of the data stored in the DSC distinguished by categories of data is presented in Table 2.2.

Category	**Supplier**	**User**
Field data	Owner DPC	Local DPC
Authenticated data	Owner DPC	HDU
Objects	Any source	Owner DPC
Temporary data	Local DPC	Local DPC

Table 2.2: Data suppliers and users per data category

Local DPCs may deliver data on request of the owner DPC for data processing purposes. Such data will be stored in the repository for Temporary data. The (originating and receiving DPCs define a time frame for completion of the data delivery. Both DPCs should also agree upon the duration of the time frame for use of the Temporary data. The DSC verifies the completeness (in compliance with the data request of the owner DPC) and timeliness of the data transfer and communicates any inconsistencies with both local and owner DPCs. Further, as with all data imports, the DSC verifies the data integrity.

Field data

Field data may be obtained from local DPCs to enhance the data validation. The receiving DSC stores such data as Temporary data on behalf of the requesting owner DPC. The Temporary data is deleted after finishing the data validation. The Field data is not intended for other use, after all, it is not validated data but used for validation purposes only.

Authenticated data

Like with Field data (mentioned above), Authenticated data can be used for validation purposes. In that case it will be kept in the Temporary data repository of the receiving DSC, which subsequently makes the data available to the requesting owner DPC.

Authenticated data may also be delivered for other uses, in such cases the requesting owner DPC is a HDU.

Object data

Like with Authenticated data, an owner DPC may request Object data from other DPCs. Object that is published in the Catalogue may be exchanged on HDU basis, restricted / unpublished data should be handled as Temporary data.

Temporary data

The Temporary data are obtained from other DPCs to enhance the data validation. As mentioned under Field data and Authenticated data, the Temporary data is extracted from the Field data and Authenticated data sets of the supplying DPCs. The Temporary data can be stored in similar structures as applied for the Field and Authenticated data.

Alternatively, the Temporary data can be stored as objects where each object is a data file, e.g. in HYMOS format. In the latter case it is not possible to use the Catalogue to select individual items from the data because they do not feature in the meta-data. The complete file is to be transferred to the DPC for loading in the data processing system. The choice between the two storage methods is to be agreed upon by the DSC and owner DPC staff.

The availability of Temporary data is not published to the external HDUs.

After usage, the custodian DPC orders the DSC to delete the Temporary data, the DSC informs the owner of the deletion of the Temporary data.

The DSC monitors the age of the Temporary data and if the age of the data exceeds a defined time span the custodian DPC is informed accordingly and asked if the data still has to be retained (and if so, for how long) or can be discarded.

2.3.3 DATA IMPORT FROM CENTRAL HIS SERVER

The central HIS server delivers Catalogues and related data to the DSCs. The data exchange with the central HIS server is addressed under the “Meta-data and Catalogue”. No hydrological data is imported from the central HIS server.

The central HIS server caters for the processing of DRF files as they were received from HDUs. The DRFs are processed and sliced into sub-DRFs pertaining to specific DSCs. Subsequently the DRFs are forwarded to the respective DSCs to be executed against the databases.

2.3.4 DATA IMPORT FROM HDU

The HDU delivers Data Request Files (DRFs) to the DSCs. The data exchange with the HDU is addressed under “Meta-data and Catalogue”. No hydrological data is imported from the HDU.

2.3.5 DATA EXPORT TO OWNER DPCS

Any data residing in the databases should be available for its owner DPCs. The owner DPC selects the required data using the Catalogue and submits the DRF to the DSC. The Catalogue should hide no data for the owner DPC and allow selection of any data, also data that is not published for use by others. Upon receipt, the DSC should process the DRF and immediately make the requested data available via the LAN for the owner DPC. The data should be presented in the standard format pertaining to the data types.

No invoicing is required.

2.3.6 DATA EXPORT TO LOCAL DPCS

The local DPC may request the owner DPC for certain hydrological data to enhance the data validation process. The data should be delivered in the standard format pertaining to the data types. The mode of transport is to be agreed upon between the DSC and requesting local DPC.

No invoicing is required.

Field data

Field data may be delivered to local DPCs, on their request, to enhance the data validation. The receiving DSC stores such data as Temporary data on behalf of the requesting local DPC. The Temporary data is deleted after finishing of the data validation. The Field data is not intended for other use, after all, it is not validated data and used for validation purposes only.

Authenticated data

Like with the above-mentioned Field data, Authenticated data can be used for validation purposes. In that case it will be kept in the Temporary data segment of the receiving DSC, which subsequently makes the data available to the requesting local DPC.

Authenticated data may also be delivered for other uses, in such cases the requesting local DPC is treated as an HDU.

Object data

As a rule, standalone Object data, i.e. Objects that do not belong to Field or Authenticated data, are not published in the Catalogue and are not exchanged with other DSCs/DPCs.

Temporary data

The Temporary data are obtained from other (non-owner) DPCs to enhance the data validation. It is the receiving DSC's prerogative to decide how to store the data in the temporary repository. The requesting DPC may have a preference for the data format, e.g. similar to the structures as applied for the Field and Authenticated data or formatted for direct loading into the data processing system. In the latter case the data may be delivered as objects. The data centres involved should agree upon the most convenient format.

The availability of Temporary data is not published to external HDUs.

After usage, the custodian DPC orders the DSC to delete the Temporary data, the DSC informs the owner of the deleted Temporary data as well as the custodian DPC of the execution of the same.

The DSC monitors the age of the Temporary data and if the age of the data exceeds a defined and agreed upon duration the custodian DPC is informed accordingly.

2.3.7 DATA EXPORT TO CENTRAL HIS SERVER

Meta-data updates are dispatched to central HIS server in compliance with a defined and agreed upon time schedule. Details are discussed in the Chapter “Meta-data and Catalogue”.

2.3.8 DATA EXPORT TO HDU

Upon request or automatically, the DSC should make new Catalogues, i.e. updated versions, available to interested HDUs. The local Catalogue, which is online in the DSC, is always up to date for the owner DPCs’ data as administrated by the DSCs but not necessarily for the data residing in the other DSCs.

Based upon the processing of the HDU’s DRF hydrological data can be delivered to the HDU provided he has the proper permission. The mode of transport is to be agreed upon between the DSC and requesting HDU.

The data should be delivered in the standard format for each of the data types. Exceptionally, on request of the HDU, the DSC may deliver the data in a special format to meet the requirements of the HDU.

In case an invoicing system is in place, the necessary information is to be collected and processed. The HDU should be informed in advance about the total costs involved. The payment should be received and verified prior to the actual delivery of the data.

2.3.9 ADMINISTRATION OF DATA FLOWS

Obviously, the incoming and outgoing data flows should be properly administrated. The administration should at least imply the source or destination of the data, the date and time of the interaction, the mode of data transport (like diskette, CD, PSTN / ISDN, LAN), the identification and amounts of data etc. In particular for billed data the administration of both the data delivery as well as the invoicing has to be accurate and unambiguous.

Data flows not only comprise the Field data, Authenticated data, Temporary data and objects but also meta-data, invoices, MIS data and DRFs.

National organisations may keep data duplicates in their national head quarters; proper protocols should be implemented to maintain synchronisation of such data with the originating DSCs.

2.4 META-DATA AND CATALOGUE

For search and selection of the required data the Catalogue is made available for public use. Meta-data and the Catalogue are closely associated; actually, the Catalogue is derived from a public subset of the meta-data. The Catalogue comprises meta-data and a search and selection engine (browser).

The result of a data search and selection session on the Catalogue is a request for data, which is generated in a computer file. This file is dubbed Data Request File (DRF). The DRF can be submitted to the specific data custodian DSC(s) via telecommunication, e.g. email or FTP (if available) or by post/hand carried on physical media. The DSC verifies the HDU's authorisation and permission level to establish if the HDU is entitled to receive the requested data. For authorised HDUs the data request may be run on the database and the results are made available to the HDU. To support all this, adequate procedures and tools have to be implemented.

2.4.1 DRF PROCESSING

DRFs can be generated from different representations of the Catalogue, viz.

1. local Catalogue at a DSC and
2. central Catalogue via the web on the central HIS server,
3. standalone Catalogue offline on the HDU’s PC.

The contents of these Catalogue versions most likely will differ, primarily because each of these Catalogues may cover a different period. The content of the Catalogue is derived from the meta-data files pertaining to the respective DSCs as available at the time of Catalogue generation. It is to be expected that the local Catalogue will best reflect the contents of the databases in the local DSC but may not be that complete with respect to the other DSCs. The central Catalogue will have the best overview of the contents of all the DSCs but probably of some time ago, depending upon the periods covered by the meta-data files as received from the associated DSCs. The standalone Catalogue is a snapshot of the contents of the central Catalogue; it will become outdated quickly, at least as far as the current and latest data are concerned. However, although the standalone Catalogue version may not reflect the present data contents of the DSCs, even older versions of the standalone Catalogue will still be quite useful for search and selection of historical data.

DRFs can be obtained from the local Catalogue, such DRFs are sent to the central HIS server in case they contain requests for data that is not locally available.

The DSC may receive DRFs from each of the various representations of Catalogue

1. **central Catalogue**

   The central HIS server distributes sub-DRFs to the DSCs for further processing. Such sub-DRFs contain data requests for the addressed local DSCs only.

2. **local Catalogue**

   DRFs, as obtained from the local Catalogue, are processed locally. However, if data residing in other DSCs is requested, the DRF has to be forwarded to the central HIS server for distribution to the respective DSCs.

3. **offline Catalogue**

   The handling of “offline DRFs” is similar to the “local DRFs”.

The reception of a DRF is to be properly administrated. Subsequently, the credentials and the authorisation levels of the HDU are obtained and verified. The DRF may be run against the databases then, however, only data for which the HDU is authorised will be retrieved from the databases. For all other cases, the request is rejected. As a result, the HDU may receive all, some or no data at all. Any retrieval and rejection should be duly administrated including the HDU’s particulars, authorisation levels, identification of delivered data, identification of rejected data, date and time of the interaction, mode of data transfer (e.g. email, FTP, CD). In case special formatting is part of the delivery this should also be recorded. In case certain unsupported formatting becomes popular (frequently requested), steps should be taken to include these formats in the standard supported set.

2.4.2 GATHERING AND MAINTENANCE OF META-DATA

Any change in the contents of the database is immediately reflected in the meta-data. Data administration tools supervise the updating of the meta-data. At the end of each day, the pending version of the meta-data is set apart for implementation in the local Catalogue. The local Catalogue is updated on a daily basis.

The changes in other DSCs can only be reflected in the local Catalogue upon reception and processing of the related meta-data.

On a monthly basis, a copy of the meta-data is transferred to the Central HIS server for inclusion in the central Catalogue. The offline Catalogue is derived from the same meta-data.

Changes in the structure of the database, addition / removal of parameters / fields and similar should be reflected in the meta-data and the Catalogue as well.

2.4.3 CATALOGUE GENERATION

A distinction is made between the locally available Catalogue, i.e. the one that is on-line in the DSC and the central version of the Catalogue. The local Catalogue is used by the owner DPC and should reflect the actual state of the databases. Therefore the local Catalogue should be updated on a daily basis, at least at the end of the working day.

The central Catalogue entirely depends upon the delivery of the meta-data by the associated DSCs. It is not feasible to make the central Catalogue reflect the actual database contents in all the DSCs. It is to be accepted that the central Catalogue lags behind, however, to avoid excessive lag, the DSCs should deliver their meta-data at a monthly interval or more often. It is the task of central HIS server to alert any failing DSCs.

Prospective HDUs may browse the Catalogue through the web or download the Catalogue (this may take some time due to the amount of data involved) or request an offline Catalogue on CD.

The Catalogue integrates the separate meta files pertaining to the DSCs. It does not matter what the actual age of the different meta-data sets is. Obviously, a Catalogue based on old meta-data is not up-to-date.

The generation of each Catalogue should be duly administrated. Further the validity of each Catalogue version should be recorded. Each Catalogue is valid from the time of creation up to the moment it is succeeded by a new version.

2.4.4 SUPPLY OF META-DATA TO THE CENTRAL HIS SERVER

Each DSC forwards its local meta-data to the central HIS server for inclusion in the central Catalogue preferably at a weekly interval but not longer than a monthly interval. The central HIS server and the DSCs have to decide the most convenient mode of communication, e.g. email or FTP.

During transport the meta-data may be altered, e.g. due to communication error or tampering. To allow verification of the complete and unaltered transfer of the data a unique signature should be derived from the data. Such signature could be a checksum or a CRC (Cyclic Redundancy Check) code. That signature is also transmitted to the recipient, but separately by other means and / or at another time.

The meta-data could also be encrypted using standard encryption software and the receiving DSC would decrypt the data using the key transmitted separately by the source DSC.

At the receiving end again a signature is calculated from the received data. That signature is compared with the original signature and if identical the data may be accepted, otherwise the transfer has to be redone.

The central HIS server replaces the previous version by the newly received meta-data.

2.4.5 INTEGRATION OF META-DATA FILES

The central HIS server creates an integrated version of the Catalogue at the end of each day that it receives new meta-data of one or more DSCs. The new version is subsequently made accessible for HDUs via Internet, hence, the central Catalogue will reflect the latest version of meta-data as was received by the central HIS server.

After successful merging of the newly received meta-data file(s), the central HIS server discards the replaced meta-data. It is not a task of the central HIS server to maintain a repository with replaced meta-data files.

2.4.6 DISSEMINATION OF THE CENTRAL CATALOGUE

As explained, the central HIS server assembles the Catalogue from the meta-data pertaining to all the associated DSCs. The central HIS server informs the DSCs about the availability of the newly updated Catalogue and makes the same available on the central HIS server’s FTP site for collection by the DSCs. The transfer of the Catalogue is also associated with a signature.

The central Catalogue may be downloaded by the DSCs and HDUs. The DSCs may subsequently update the received Catalogue with the latest version of the local meta-data and make that Catalogue available on the LAN as the local Catalogue.

HDUs may use the central Catalogue for web based search and selection but they may also opt for downloading of a complete central Catalogue, which then becomes a standalone Catalogue on the HDU’s PC.

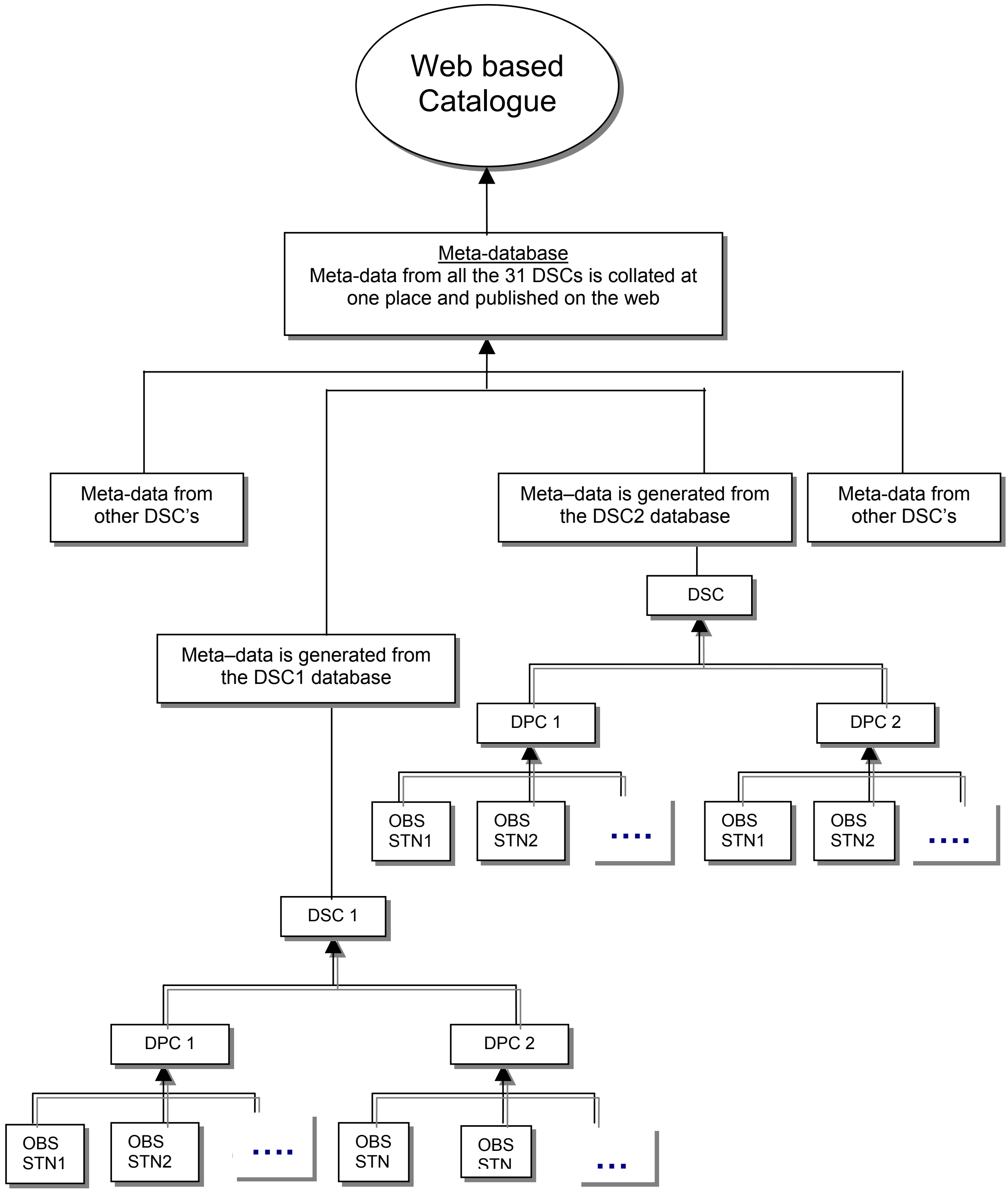

Web based Catalogue
Meta-database
Meta-data from all the 31 DSCs is collated at one place and published on the web
Meta-data from other DSC's
Meta–data is generated from the DSC2 database
Meta-data from other DSC's
DSC
Meta–data is generated from the DSC1 database
DPC 1
DPC 2
OBS STN1
OBS STN2
....
OBS STN1
OBS STN2
....
DSC 1
DPC 1
DPC 2
OBS STN1
OBS STN2
....
OBS STN
OBS STN
...

Figure 2.2: Supply of meta-data

2.4.7 DISTRIBUTION OF CATALOGUE TO USERS ON CD AND VIA INTERNET / INTRANET

The Catalogue at the Central HIS server is primarily accessible via the Internet for search and selection of hydrological data. HDUs may also use the local Catalogue on the Intranet of the local DSC.

HDUs may download the Catalogue from the Central HIS server. Alternatively, HDUs may request the local DSC for direct access to the Catalogue on the DSC's Intranet or to put the Catalogue on CD for offline use.

2.4.8 PROVIDE ACCESS TO CATALOGUE ON INTERNET, INTRANET AND CD

The Catalogue is accessible in various ways, e.g. on-line and from CD on the HDU's PC. On-line there are two varieties, i.e. local on the Intranet and remote through the Internet. The latter two will be normally used. Prospective HDUs may present themselves at the nearest DSC and browse the Catalogue via the DSC's Intranet; this would be the fastest method. The DSC should establish an access point with PC and desk available for use by external HDUs. The staff of the owner DPCs should be allowed and facilitated to use the Catalogue from their own desk. It is the task of the DSC to make this possible by providing access via the DPC's LAN. Proper security measures should be in place to allow access to the Catalogue only and to avoid any unwanted changes to the Catalogue or the databases.

On request by interested HDU, the DSC may put the Catalogue on CD for use on the HDU's own PC.

Remote users may access the central HIS server via the Internet. This is one of the main tasks of the central HIS server. The HDU submits the DRF to the central HIS server, which subsequently distributes the requests to the DSCs.

2.5 MANAGEMENT INFORMATION SYSTEM

The Management Information System (MIS) is intended to collect statistical data about the activities in the DSC, the data flows and the contents of the databases. The information is to be reported routinely in an aggregated form, which is accessible to the agency's management and to the DPC's management. The data gathering is a continuous process, mostly automated.

2.5.1 MONITORING

The basis of the MIS is a monitoring system, which gathers relevant statistical data about activities, status and events related to the databases.

- data imports and exports
- available data / database contents
- data accessed by HDUs
- HDUs' status and activities
- DRF request, status, execution and rejection
- owner DPCs' status and activities
- errors and exceptions

The monitoring should be a continuous process in the sense that the required data is gathered at the time of interaction with DPC or HDU. Although most of the data is gathered automatically, in real time, other data have to be manually logged. Any backlog in the data gathering should be avoided. Therefore proper procedures should be in place to control the manual logging and data entry into the MIS.

2.5.2 DATA PROCESSING

The gathered MIS data is rather detailed and not effective for immediate use; some data processing is required to obtain useful aggregated information. At the start of every new week, the data of the previous week should be processed and the results saved.

2.5.3 REPORTING

Based upon the data processing results, reports are to be generated, also at the same weekly interval. Dedicated reports are distributed to several recipients. For each recipient organisation a dedicated report is made. The reports contain only contains information that is relevant to that organisation. Some of the recipients are the agency's management, the owner DPCs, the local DPCs and central HIS server.

2.5.4 MAINTENANCE

Like any other system, the MIS needs to be properly maintained.

- **adapting functionality**

  During the lifetime of the MIS systems, user requirements change and adaptations will be needed. Change of IT systems, in particular those that are implemented at multiple locations and applied by multiple users, require proper management and tuning to avoid diversion of the systems. Distinction may be made between mutual needs and unique (localised) needs. For the implementation of changes to fulfil mutual needs a change project should be put in place. This to retain the common features of the systems but also to share the development costs.

  Existing documentation, among others, manuals and guidelines, need to be adapted to reflect the changes of the system.

  Unique (localised) changes may be implemented at the local level. However, such changes should be properly documented. When in future the entire MIS system is updated, the unique changes may not be supported anymore. At that time it would be appropriate to thoroughly assess the need of the unique feature, it may not be that important anymore.

- **updating of software**

  However unfortunate it may be, the software systems on which the MIS is based will become obsolete in due time, much like all software systems do. For the replacement of the software the same procedures should be applied as described in Chapter Adaptive Maintenance, under Upgrading.

  Since the MIS is one of the systems that all DSCs have in common, if would be most efficient if the changes were implemented in a concerted manner.

- **retaining data**

  The MIS will generate sizeable amounts of monitoring data whereof the aggregated MIS information is derived. The monitoring data should not be permanently retained forever, it may be discarded one month after publishing of the MIS reports that the data was used for. The MIS aggregated information, from which the reports are generated, should be retained in a historical MIS database.

- **MIS maintenance**

  All MIS related systems should be part of the standard archiving and backup procedures.

- **cross checking of results**

  The accuracy of the gathered data should be verified on a routine basis, e.g. at the standard MIS processing interval. Results should be verified by cross checking against other data collection methods. Such methods could be automatic but also manual. In case of discrepancies, the cause should be established urgently and if possible remedial action should be taken, e.g. by changing procedures or adapting the MIS tools.

2.6 INTERACTIONS

The DSC interacts with a variety of organisations and persons, among others the DPCs, the central HIS server, the HDUs, vendors and service suppliers and the owner organisation. The interactions are related to data exchange, security and access matters, day-to-day operations on the databases, maintenance of hardware and software systems, updating etc.

2.6.1 DSC COOPERATION AT NATIONAL LEVEL

The DSCs interact to exchange the meta-data and the Catalogues, primarily via the central HIS server. This is addressed under “Meta-data and Catalogue” elsewhere in this manual.

Other, essential, interactions should take place to maintain the highest level of standardisation in the databases and the applied formats of data import and export. The DSC management and staff should maintain a cooperative attitude aiming at smooth exchange of data between DPCs and HDUs.

At the national level the DSCs plan how to accommodate new data needs as formulated by the DPCs. To be thought of are the introduction of new data types, adaptation of data attributes etc. Other changes could be due to adaptation of the (re-)definition of catchment areas / aquifers, changes of object naming and others.

Associated with the new data needs as mentioned in the section above, the standard formats of data exchange require adaptation. Further new formats will be needed to accommodate new data collection methods and instruments but also new standard software for data processing.

All these changes and many others not mentioned here should be properly coordinated to maintain a high level of exchangeability of the hydrological data to the benefit of the Indian people.

2.6.2 ADVISE USERS ON DATABASE CONTENT AND DATA RETRIEVAL OPTIONS

One of the tasks of the DSC is to provide the HDU (existing and prospective) about the database content and the data retrieval options. With respect to the database, the HDUs should get information about the time period that is covered by the databases, this in general terms e.g. basin / aquifer related. There is no need to go into the very detail because for that the HDU can assess the Catalogue. Further, the DSC should provide the HDU with information about the types of data that are available.

For the data to become really useful the HDU should know what the accuracy of the various data types is, this should be reported in context with the station and measuring methodology. Obviously the DSC needs the assistance of the DPCs to achieve this. It would be best if they prepare a note to explain all the details. Ideally, the information could be obtained from the data dictionaries, however, some information about the accuracy of the respective data values may need to be added.

Further, the DSC should inform the HDU about the data retrieval options, i.e. on-line via the Intranet of each DSC, on CD-ROM / diskette from the same local DSCs, or via the Web (email / FTP).

Obviously, the HDU should also be informed about pricing and restrictions.

2.6.3 LIAISON WITH HDUS

The DSC is among others a service organisation in support of HDUs; it is one of the reasons of existence of the DSCs.

A task of the DSC is to act as a liaison with the HDUs. This implies that the HDUs may present themselves at the DSC to use the Catalogue via the Intranet and to collect data. The DSC may also assist the HDU in formatting of the requested data to enable the data to be imported by the HDU's application software. This formatting assistance should remain limited, i.e. it should not involve a considerable programming effort that absorbs the manpower capacity of the DSC staff for several days.

Further, the DSC may introduce the HDU to experts of the owner DPCs in case in depth hydrogeological assistance is required.

2.6.4 USER RIGHTS, ACCESS, SECURITY

Physical access to the DSC should be limited to office space only; external HDUs should have no access to the database hardware. For visiting HDUs one or more access points should be established in a separate place; there the HDU can use the Catalogue and prepare a DRF. The access point(s) could be in one of the DPCs or in the DSC area.

The user rights are allocated according to the table below.

interfaces with:	**owner DPC**	**local DPC**	**other DPC**	**other DSC**	**national DSC**	**HDU**
field data	read all write own	read all	none	exchange on request	none	none
authenticated data	read all write own	read all	read if permitted	exchange on request	exchange on request	read if permitted
public domain data	freely distributed	freely distributed	freely distributed	freely distributed	freely distributed	freely distributed
meta-data	read all	read all	read all	up-date and read all scheduled exchange	read all scheduled exchange	read all
object database	read all write own	read if permitted	read if permitted	exchange on request	exchange on request	read if permitted
temporary storage	exchange	exchange	none	none	none	none

Table 2.3: Allocation of data access rights

Read rights imply reading and copying of data including the receipt of data in electronic file format upon processing of the DRF as generated by a HDU (or owner DPC).

Write rights imply writing of new data, change of existing data and deletion of existing data.

Exchange rights do not affect the hydrological data in the DSC, they merely imply transferring data for temporary storage to a DSC on request of one of DSC's owner DPCs.

Read all rights of the meta-data are executed at several levels, the owner DPC can read any meta-data, the HDUs can read meta-data about validated authenticated data (and related objects) only.

The DSC executes the actual security control; no user, (HDU or DPC) should be permitted direct access to any data in the DSC. The Read and Write rights listed in the table above are executed by the DSC on request of the DPC or HDU. In case of the owner DPC, the required actions should be executed immediately, without delay.

2.6.5 SUPPORT OF DPC COMPUTER USERS ON IT MATTERS

One of the tasks of the DSC staff is to support the DPC and other departments of the parent agency with IT matters, both hardware and software related. This implies among others assistance with installation, configuration and removal of hardware and software.

The target area comprises virtually all elements as found in the data centres and office environment like PCs, servers, peripherals, network incl. cabling, and software (PC standalone, client, server).

Support activities rendered to the owner DPCs and offices departments are:

- configuration and tuning of hardware and software systems
- testing trouble shooting and fault finding of all hardware and software
- designing, building, testing and implementation of software utilities and tools for own use and on user demand
- execution of complex non-standardised data processing in assistance of DPC experts
- immediate user assistance in case of software / hardware difficulties and / or failure in the DPC(s)

The DSC staff should appreciate their position as a service organisation, which renders its services to internal clients. It requires a professional attitude to act accordingly.

For all the support fields a proper level of knowledge is to be obtained and maintained.

2.6.6 SUPPORT OF HDU ON IT MATTERS

The DSC staff also gives IT support, both hardware and software related, to HDUs if requested.

Support activities rendered to the owner DPCs and office departments are:

- advice on configuration of hardware and software systems
- execution of special data formatting

Some of the major support services by the DSC are described below.

1. The Catalogue CD contains tools like File Transfer Protocol, Internet Explorer, security tools, etc.
2. Data format conversions

   On specific request the DSC assists with conversion of the requested hydrological data to a format required by a specific application. Very complicated conversion, in particular one-time conversion, may not be fully supported. The DSC prepares proper software documentation for the conversion programs to make reuse possible. In particular for common applications / data processing tools it might be considered to make and support specific conversion programs.

3. Version control and upgrade programs

A record is kept about what software, including the version, has been made to available to the individual HDUs. Upgrades, when they are released for distribution, are to be made available to the HDUs. The availability is published on the central HIS server. Interested HDUs can download the software from their local DSC or form the central HIS server. The downloading is to be recorded including the HDU's particulars and the software identification with its version code.

4. Help in creation of task forces and insisting on nomination of single point of contact from HDU.
5. Knowledge base creation
   - the knowledge base should support retrieval of specific information from the HDU's system
   - complete documentation about the HIS, the data structures, types and attributes, manuals about the tools and the Catalogue and similar specific information is to be made available for interested HDUs on CD and on-line
   - FAQ's containing a compilation of the most often asked questions as well as information that the HDU may expect to find in the FAQ is to be published on CD and the web.
   - Helpdesk for answering and resolving queries.
   - The Helpdesk should be online but also allow the HDU to submit HIS related questions. The response should be fast and formulated in a clear-cut unambiguous way. Although HDUs may have a profound IT expertise, in general the HDU will be computer literate but not an IT expert. The advice by the Helpdesk should assume a limited IT knowledge on the HDU's end.

2.6.7 MAINTAIN KNOWLEDGE BASE ABOUT DEVELOPMENTS IN IT PROFESSION

The DSC monitors hardware and software developments related to the PC platform and the peripherals in use under the HIS. Developments that could become of interest in the near future should be monitored as well, e.g. development related to data storage methods and devices, communication by optical cable, real-time telemetry, other operating systems etc. The activities in this respect should be kept practical in particular the balance between effort and urgency of implementation should be kept in mind.

The knowledge of the primary systems (data processing and storage related to the hydrological data) and the office systems should be properly maintained. The office systems comprise word processing, spread sheets, local data bases, presentation software, internet tools, graphical tools, generic data processing, GIS, etc.

The above may be implemented by subscribing to one or two relevant magazines, attending courses, participation in workshops and doing self-study. The efforts (material and personnel) should be kept balanced. The Internet should also be used in a focused manner for keeping abreast of advances in technology the world over.

Create a knowledge base for storing the paper based and electronic information in an orderly manner. The knowledge base should provide a classification under categories (broad and specific) and topics for storing and retrieving the information. Also the relevance of the topics shall be part of the knowledge base to allow a more focussed retrieval. There should be a provision to gather updates on the information and to maintain particulars on organisations, publishers and people who update the information.

2.6.8 CONTROL OF ACTIVITIES OF SERVICE AND SYSTEM PROVIDERS

In their capacity as IT experts, the staff of the DSC controls the activities of the service and system providers, also for the DPCs and related offices.

This involves:

- the formulation of requirements and tasks
- monitoring of execution of activities
- verification and acceptance of hardware, software and services deliverables
- providing the service providers with required information to execute their tasks
- assistance to the service providers with fault finding and trouble shooting of the systems in DPC and DSC

2.6.9 COMMUNICATION WITH VENDORS, SUPPLIERS AND SERVICE PROVIDERS

Of the agency's departments, the DSC staff have received the most comprehensive education and training in the IT field. As a result, the DSC is the most suitable department to communicate at an appropriate IT level with the IT vendors, suppliers and service providers.

The DSC should organise, in an appropriate way, a regular exchange of information about the current state of affairs and developments in the IT field. This might be achieved through discussions with selected counterparts in the IT field, e.g. on a quarterly basis.

Further the DSC staff should participate in workshops / seminars to improve knowledge and maintain sufficient authority as consultant for the DPCs and management of the agency. Both generic and dedicated workshops and seminars should be selected. Some subjects for the generic level are PC operating systems, Internet, data communication, security, office environment and similar. At dedicated level subjects could be related to databases, security, data warehousing and storage techniques, Web based data dissemination etc.

As a result of ongoing developments in the IT field new and improved solutions for the existing operational systems will emerge. Knowledge of the present state of technology and at a more abstract level, towards a future that is a few years away, should be maintained to have a good insight when the need for adaptation arises.

Also new and / or emerging requirements as defined by the DPCs and the DSC proper should be discussed with IT experts. The discussions should include assessment of the technical and financial feasibility of the envisaged solutions.

2.6.10 REPORTING ON DATABASES AND REPOSITORIES

status

The DSC keeps the respective owner DPCs informed by reporting about the amounts and status of the data residing in the databases and repositories. The reports are prepared and submitted at a fixed monthly reporting interval.

actions

Further all actions and events on databases and repositories are reported. The reports cover all abnormal events like problems encountered, changes of the data storage structures, attacks by virus and / or hackers, hardware failure, software and hardware enhancements and changes, repairs and similar activities.

Further, all routine activities are reported, of which at least the following should be included. Backup and archiving, defragmenting of disks, update of anti virus software and firewall systems.

2.6.11 FORMATTING PROCEDURES FOR IMPORT AND EXPORT

For the standard data types / sources standardised formatting procedures should be applied. All the DSCs should use these standard procedures.

For new data types and / or to support new instruments special formatting procedures may be developed. Such procedures should be thoroughly tested and documented to avoid loss of data and / or introduction of errors.

Data loss can occur due to many reasons e.g. not reading of all data, skipping of lines containing data exceptions like error codes, mixing of text and numerical data, skipping of first and last lines, too large input files.

Data errors can be introduced by mixing up of time labels and / or data fields, losing of digits, losing of sign, mixing up of column sequence, misinterpretation of floating point data and so on. Many errors may be evident but to detect some errors a meticulous mind and domain knowledge is required. For any change proper verification procedures should be implemented.

For export of retrieved data, reverse formatting will be needed, e.g. to allow easy loading of data in the SW and GW data processing systems. Also for export standard formatting should be applied.

As a service to HDUs, the DSC may prepare dedicated formatting functions to support specific HDU requirements, e.g. to enable the data to be loaded directly in the HDU’s data processing software. However, this formatting should be limited in effort and the formatting function should be carefully designed and tested thoroughly.

3 MAINTENANCE

Maintenance in the context of this manual volume involves the activities as to keep the systems in optimum working condition. This includes rectification of errors, bugs and malfunctions but also adaptations towards new hardware, software and operational environments and modification at the functional level, e.g. by adding new facilities and removing obsolete functions.

The throughput time required for solving software problems and modifying the DSC systems and the quality of the solutions largely depends upon the quality of the available documentation at systems and software level. To safeguard the maintainability of the DSCs in the future effective documentation standards should be maintained also for modifications during the operational phase. Further, it is of great importance that the in depth knowledge that was accumulated during the development and implementation of the DSCs is preserved by keeping the key staff of the developer organisation available for consultation and assistance during maintenance.

3.1 COORDINATION

Standardisation and data exchange are essential for an effective management and utilisation of the water resources. Data exchange within the data collecting agencies proper will be most intensive and few problems are to be expected with respect to internal data exchange as all offices within the same organisation will use the same software and database designs. However, as soon as data have to be imported from or exported to other agencies an HDUs standardisation is essential. There is a great risk that different agencies develop their own software and database versions to accommodate specific requirements unless proper cooperation and coordination is maintained.

To manage the standardisation a coordinating body is to be established. Each DSC should cooperate with that body. Major tasks of the coordinating body are maintaining the standardisation of:

- data definition
- database structures
- DSC software
- data exchange formats and protocols
- meta-data and Catalogue

Further, cooperation in the maintenance would allow the sharing of development costs. The DSC management and staff should maintain a cooperative attitude aiming at smooth exchange of data between DPCs and HDUs.

During the lifetime of the Hydrological Information System new needs with respect to the DSCs will emerge. Such needs could be manifold, to be thought of are the introduction of new data types, adaptation of data attributes etc. Other changes could be due to changes in the hydrological organisations, re-definition of catchment areas / aquifers like splitting and merging of existing ones, establishment of new types of data collection stations

Associated with the new data needs, the standard formats of data exchange require adaptation. Further, new formats will be needed to accommodate new data collection methods and instruments on the import end and new standard software for data processing on the export end. New data communication methods and system will also require adaptations.

All these changes and many others not mentioned here should be properly coordinated to maintain a high level of exchangeability of the hydrological data to the benefit of the Indian people.

3.1.1 ORGANISING MAINTENANCE

A single maintenance provider should maintain the software systems and databases of all DSCs, primarily to maintain standardisation and to share the maintenance costs. Development of adaptations and new features of software and the databases should be the task of a single service provider.

The local maintenance of the contents of the databases and the operation of the DSC is entirely the task of the DSC staff.

3.1.2 LOCAL AND COLLECTIVE CHANGES

Unavoidably, agencies will develop new applications. As long as such applications do not interfere with the HIS standards no coordination is required. Other agencies might also be interested to participate in the development of applications, hence, it is recommended to share ideas and plans with the other agencies and DSCs for mutual benefit.

Adaptations for local use only should not affect the standardised software and databases. It should also be possible to install new versions of the DSC software and database structures without having to redevelop the original adaptations. Further the data exchange with other DSCs and HDU at national level should in no way be hampered by local changes.

On the other hand, collective changes of the software and databases are permitted provided that new software and / or data structures are installed at all DSCs in a coordinated manner. Further also the all HDUs should get access to new Catalogue data and tools. It is essential to maintain backward compatibility in all adaptations.

To accommodate new requirements and to adapt to changes in the external world, adaptive maintenance must be executed. The adaptive maintenance should be planned and coordinated at the national level.

3.2 CORRECTIVE MAINTENANCE

Corrective maintenance will be required to remedy system deficiencies, bugs and other flaws. Corrective maintenance is typically responding upon flaws in the existing system and to a great extent erratic in nature.

3.2.1 DIAGNOSIS

The problem should be properly diagnosed to assess its extent and to identify the affected areas. Further the cause should established. The findings should be duly reported giving all the details for unambiguous analyses and design of the remedy.

3.2.2 CORRECTION

A plan for the correction should be defined. It should also include the documentation of the problem, required changes in the system and user's documentation. Further the plan should include required resources, tools to be used, milestones, testing including pass criteria, implementation plan, time frame, estimated costs and documentation.

The correction should be meticulously designed considering all implications.

3.2.3 DOCUMENTATION

All changes should be properly documented. The technical documentation should include changes at functional level, in the source code, data exchange within the software, variable types, etc.

All system and user manuals, guidelines, help desk contents and other documentation should be adapted if affected by the correction.

3.2.4 TESTING

The correction should be tested to establish the complete remedying of the reported problem. Unfortunately, changes may have side effects introducing new bugs in the system functions and / or the data. Rigorous and properly designed tests need to be executed. These tests should not only address the problem proper but also the areas that might be affected by the remedy.

The test plan, the test methodology, the pass criteria, the test results and other findings and observations have to be duly reported. The input and output data of each test run should be retained. It should be possible to repeat the tests at a later stage, for this the relevant information, data, tools and settings should be retained.

Flaws in the databases should be tackled and reported in a similar way: identify, locate and diagnose the problem; design corrective measures, test the same and report all aspects. Further manuals should be properly updated.

3.2.5 IMPLEMENTATION

The implementation of the corrected software should be planned. The implementation should not jeopardise the existing data. If needed (or in doubt) the data should be safeguarded by making a full backup. Further, the interference with the normal day-to-day operations caused by the implementation activities should be kept to a minimum.

If the problem was common to more DSCs, the update should be implemented at all the DSCs in a concerted way.

It is to be decided if the implementation is essential for the normal operation or that it may be delayed for some time. In the latter case, the implementation may be delayed so that other corrective repairs can be accommodated in a single implementation action. The implementation should also involve the updating of the documentation and the manuals in each of the affected DSCs. In severe cases staff might have to undergo additional (focussed) training to properly understand the new systems and their implications.

3.3 ADAPTIVE MAINTENANCE

Adaptive maintenance is executed for two main reasons:

1. upgrading the system with new releases,
2. introducing enhancements of the systems.

As mentioned elsewhere, the maintenance of the systems should be closely coordinated, therefore it is recommended to centralise the same.

3.3.1 UPGRADING

Upgrading is typically supply driven and in some cases even forced upon the owners and users of computer hardware and software.

The systems in the DSCs were centrally purchased; the same applies to the AMC. Hence, under these contracts it is the task of the system supplier to distribute and implement any upgrades.

Some upgrades may affect the databases or may result in changed functionality. In such cases the need for upgrading should be thoroughly assessed and its implications identified. Implications could be the risk of system instability or even data loss, the need to develop new tools and interfaces, redesign of the database structure, incompatibility with existing data and many more. The costs should also be assessed, both the initial costs for the upgrades proper and the costs of the required modifications of the existing systems to accommodate the upgrades. The risk involved in rejecting the upgrading can be great, especially in case the existing systems are not supported anymore. Based on the complete information, a decision is to be taken at the national coordinating level.

It should be avoided that the DSC becomes unavailable due to malfunctioning, unfinished development, ongoing debugging etc. It is strongly recommended to thoroughly test each upgrade before it replaces the incumbent version. Obviously, the same applies to any other changes as required for the updated DSC.

If it is decided to implement the upgrades a project has to be defined to properly manage the execution. Like with any change to the system several aspects have to be taken care of:

- budget allocation,
- time plan with milestones,
- test plan with defined pass criteria,
- adaptation or replacement of technical documentation,
- adaptation or replacement of manuals and guidelines,
- contingency plan in case the implementation fails,
- implementation plan.

To limit the risk of disaster, the following aspects deserve close attention, not only when the installation of an upgrade is imminent but also during normal operation of the data centre.

- A complete record of installed software, the configuration thereof and any customisation should be maintained for each computer as part of the day-to-day procedures.
- The configuration, set-up and changes to be preserved.
- Copies of the installation software, patches, initialisation codes, manuals and other essentials for installation need to be made available.
- Installation procedure and prerequisites for each software to be documented along with version numbers.
- All stored data should be saved on double backups. The backups should be tested for possible corruption.
- The upgrade should be compatible with the retained hardware and software systems.
- Before an upgrade is installed on the life system, it should be thoroughly tested on a separate system. If possible, both systems should be operated in parallel for some time.

Generally, upgrading involves the following:

- uninstalling of the affected incumbent software / system while retaining other software (the software that is not to be upgraded),
- installation of the new software / system,
- development and implementation of new tools and functions,
- adaptation and customisation of configurations and data repositories,
- information of users, if needed.

For systems that the DSCs have in common, if would be most efficient if the upgrades were implemented in a concerted manner.

3.3.2 ENHANCEMENT

Enhancement is typically demand driven, i.e. the system users / operators propose modifications to improve performance, ease of use or to accommodate new requirements. Modifications that affect standardisation in any sense should be proposed via the coordinating body. Some enhancement proposals may not be accepted e.g. due to excessive cost, lack of common interest, complexity, poorly formulated reasoning. The DSCs may accept other proposals.

Documentation, testing and implementation should be given the same attentions as described under corrective maintenance.

3.4 HARDWARE MAINTENANCE

The hardware can be broadly classified into four categories :

1. computer hardware
2. storage devices
3. peripherals like printers
4. line conditioning equipment like UPS and CVT
5. communication and networking equipment like hubs, switches, gateways, modems, cables etc.

All of these are required for the normal operation of the DSC. Although the hardware can be operated directly from the mains supply, it is recommended to avoid this because power fluctuations may damage the equipment and a power cut would bring the whole system to a sudden halt. Brown outs may result in data corruption and system failure. Restarting the systems would take a lot of time and most likely data will be lost and / or corrupted. It is therefore of great importance that the UPSs be kept in optimal condition by proper maintenance. Although the networking and communication equipment is rather robust, there is also vulnerability, in particular with the connectors and cables. Cables hanging loose from sockets, connectors lying on the floor are all indicators of poorly managed maintenance. Dust and mechanical wear and tear are the main failure causes of printers, modern printers normally having a long service life if kept clean. The working environment also affects the performance of the computer systems. Dust corrupts connections, hinders cooling by settling in PCBs and clogging fan and air intake. Moist dust may even result in short circuiting. In particular mass storage devices, among others due to the small mechanical tolerances, are sensitive to high temperature. There is no need to keep the office temperature at 20°C, but in the hot season A/C will be needed to control the temperature within safe limits. Hence, the A/C is to be properly maintained, not only for the comfort of the staff, which obviously is important, but also to protect the data.

It is also important to ensure that all the equipment is kept properly covered when not is use. All openings for insertion of additional cards and devices should be kept closed so as to prevent the ingress of rodents, insects etc. into the system.

Initially, after termination of the warranty period, the hardware maintenance of the DPCs and DSCs will be executed by the hardware supplier under the AMC support.

Hardware maintenance may involve replacement, repair, upgrading of hardware components and reloading of system software The replacement / installation of PCBs usually requires (re-)installation of associated software drivers as well.

Servicing

A schedule for preventive maintenance needs to be agreed upon with the service provider. Strict adherence to the committed schedule from both sides is important to ensure longevity of the computers.

Servicing is part of the first line maintenance, it involves among others cleaning of keyboard, display, PC interior, floppy disk drive, CD device, UPS batteries and fans. Accumulated dust should be removed by vacuum cleaner, surfaces like keyboard and display should be cleaned with a proper cleansing fluid as recommended by the manufacturer or with a damp (not soaking wet) cloth.

Proper safety rules should be adhered to. Do not open live equipment to avoid electrical shock; always disconnect the power cord before opening electrical equipment.

When PCBs have to be handled, adequate anti-static measures have to be implemented. In particular in dry environments there is a high risk of damage by static discharge. Any accumulation of static charge should be removed by connecting the electrical component to ground. The engineer should also be connected to ground through a wrist strap or ankle strap. PCBs should be kept on conductive rubber mats. Always store PCBs and other hardware in appropriate boxes, preferably the original ones.

Repairs

The IT staff should be capable and have the facilities to repair and / or replace cables and connectors, pertaining to power supply, local area network and interface cables of devices, e.g. to connect to the PCs.

For such first line repairs, spare parts and tools should be available in office. If defects are identified, they should be remedied at the earliest.

Complicated repairs and repairs that are covered by an AMC contract should be executed by the AMC contractor only.

All parts or products given as permanent replacement by the AMC party have to be properly administrated and will automatically assume the warranty of the defective product. Replacement parts of different type or model than the original should be accompanied with the documentation, manuals and guidelines for installation, operation and maintenance, both for hardware and software, as applicable.

Certain parts may be defined as critical components for larger centres (DPC / DSC) and these can be stored on site for the supplier so that the service turnaround is faster. This may include certain storage space for diagnostic disks, power cords, cables, power supplies etc. Other logistic support to the supplier may also be required and should be agreed upon during contract preparation.

Communication

Communication is of great importance to maintain an efficient flow of data, both for the collection, validation and processing of the data as well as for the exchange and distribution of data.

Although the communication systems are also part of the hardware and software AMC support, they need special attention because they link with the external world. Changes in the external world would affect the data communication links forcing adaptation and / or updating of the communication facilities. A shift from analogue modem to ISDN or ADSL might be desirable to improve the data transfer rate.

For telephone based communication, the set of dial-up numbers to related offices (e.g. subordinate, other DPCs/DSCs), Internet Service Providers (ISPs), users, etc. may need frequent updating. The particulars should be properly administrated and kept up-to-date.

3.5 ROUTINE MAINTENANCE

Routine maintenance includes the normal operational maintenance of the hardware, software and databases. It is primarily executed by the DSC staff.

3.5.1 MAINTENANCE OF DATABASES

The database administrator on a scheduled basis has to examine the sizes of the data tables, which store the actual values of the various parameters in the DSC software. These are defined in the documentation of the software. In case performance is being affected by the size of the table; the administrator should use the program to break up the larger tables into smaller tables. Similarly, in case of large tables storing deleted data, purging through the appropriate menu options is required to be done.

Backup of the database is essential before any of these operations is carried out. These operations should also be conducted in single user mode, that is, no other user is allowed to log onto the server when this is being processed. It should also be ensured that the UPS is adequately charged when carrying out this operation.

Integrity checks on the database and general statistics generated by the RDBMS should be scrutinised and the DBA should apply his experience and knowledge to identify areas that require attention.

Housekeeping and deletion of Temporary data should also be performed on a scheduled basis.

Further, the databases should be compacted periodically.

Maintenance of Temporary data

The Temporary data, i.e. the data that pertains to local DPCs and that is only used for data validation purposes should be loaded in the Temporary databases in compliance with similar rules as applied to the normal (pertaining to the owner DPCs) Field and Authenticated hydrogeological data. Similar integrity checks as executed on the normal data should be implemented, however, the Temporary data may not have been fully validated and it should not be expected that all entries meet the full integrity requirements.

The availability of Temporary data should be properly administrated. In order to avoid the clogging of the repositories with obsolete Temporary data, the DPC, which requested for the data should inform the DSC about the status of the Temporary data, i.e. if the data is still required or obsolete after using it for the data validation and processing. If the age of the Temporary data exceeds more than two seasons the should DSC inform the user DPC that the data are about to be removed from the Temporary data base due to being obsolete. The custodian DPC may be given one month to respond before the data are actually removed.

Annually, the DSC reports to the respective DPCs about what of their data resides in the Temporary data repository. The report is accompanied by the meta-data of the Temporary data.

3.5.2 BACKUP PROTOCOLS, FACILITIES AND IMPLEMENTATION

Any information stored on the computer or on a disk is vulnerable to damage or loss due to a variety of causes like theft, sabotage, fire, wear and tear, computer viruses, power failure, magnetic fields etc. One of the major threats is the user himself – a single wrong command can destroy months of effort. Therefore, backup of data is critical and has to be performed regularly on a scheduled basis.

Various levels of backup are:

Local backup: The first level of backup can be kept on the same computer, preferably in a different partition.

On-line backup: The second level of backup can be kept on the hard disk of another computer, if connected on a network, e.g. a file server.

Off-line backup: This is the most important backup. This could be on CD's, magnetic tapes or other devices, depending on the hardware configuration of the computer and the facilities available in the DSC.

Off-line incremental backup: This option is useful for very large volumes of periodic data. In this procedure only that information which has changed after the last backup is backed up and thus saves lot of space and backup time. Restoring of incremental backups is a bit tricky because when one of the increments cannot be restored e.g. due to failing media, the chain is broken and data are lost.

Off-line backup can be taken on CDs or tape e.g. DAT or DLT. Typically, the capacity of CDs is 650 MB and of DAT cartridges is between 2 and 40 GB.

CDs and tapes have substantial storage space and are preferred methods for backing up large amounts of data.

Backup on CD's or tapes is done using the special software supporting the backup device. Procedures for CD-R drives and tape drives may be different and equipment specific, and thus would not be conducive to a system based backup protocol. However, backup on tapes using ArcServe software, which is part of the DSC System software, is easy to use and with some training the administrator can configure the system for scheduled incremental backups.

It is self-defeating to take backups on the same piece of physical removable media cycle after cycle. This leads to the following problems:

- corruption of data because of media failure: loss of previous backup also
- loss of backup in case undetected virus in current backup
- all corruption, errors in previous data made in the current cycle transmitted to the backup

To safeguard against these problems, it is suggested that the Monday, Tuesday, Wednesday … Sunday technique is used, whereby backups are taken cyclically on different sets of media. This ensures that at any point of time, different secure backups are always available. It also provides for some redundancy in the backup system and for checking on data sanctity and validity. On a monthly basis, one of the CDs or tapes should be stored for one year, acting as a long-term backup. The slot of the stored data carrier in the weekly backup cycle is to be replaced by a new one.

Alternatively a Grandfather - Father - Son sequence may be adopted

It is essential to ensure that every six months, a complete backup tape is created. Too many sequential incremental backups are not advisable, and the complete backup becomes a new reference point for future restoration of data.

For any backup, the integrity needs to be tested before accepting it as a valid backup. On a monthly basis, restoring the backup should be tested. For this a separate computer should be used. An officer responsible for test-restoring is to be appointed. The results of the restoring test should be reported to the DSC manager and entered into the DSC software, which generates a report on the status of the restoring test.

Restoring Data: The backup system will always have a corresponding restore utility. In case a restore is required it must be ensured that it is done such that no existing valid data is over-written.

Compaction and compression before backing up of data

A database grows each time data is added. However, it is important to note that when data is deleted, the database does not necessarily become smaller automatically. This is a standard feature in most DBMSs and other databases to provide faster response times. Thus, it becomes important to 'compact' the database periodically as the database keeps deleting its own temporary and work data leaving gaps in the data files. Compaction reduces the size of the database and will help in creating smaller backups. It is therefore recommended that the databases be compacted frequently, especially prior to a backup process, e.g. once a day.

Another method commonly available is data compression. Compression reduces file sizes for the purpose of storage by "packing" the data in a smaller space. Since a compression process reduces the size of storage required for backup it is always useful when the amount of data to be backed up is larger and at the same time the receiving media is having relatively lesser space.

There are several utilities available for compressing the files. Most of these utilities also support simultaneous processes of compression and backup functions (with backup spanning on multiple data carriers). A copy of the decompressing software program should be also stored with the backups if they have to be retained for a long time to guard against version changes and / or obsolescence. Compacted data is accessible for normal use by the DBMS, compressed data first has to be decompressed though.

3.5.3 BACKUP POLICY

On-line backup: As all the computers at DSC are connected with the network it would be useful and easy to take a daily backup of important data on all the computers on the server computer. The backup data should comprise the databases and "pending-files" (files under processing)

Off-line backup: As the data at DSC is very important, it is essential to keep an off-line backup on CDs or (DAT) tape drives as well. As a regular activity after the on-line backup is taken it is appropriate to ensure the off-line backups as well. The frequency of the off-line backups must be at least weekly.

Duly record any manual change to the database in such a way that the changes can be redone by any database administrator using the records only, i.e. without oral assistance or knowledge of the history of the DSC.

Use separate backup tapes for each working day of the week, i.e. a Monday tape, Tuesday tape etc. Each Monday, the backup data of the previous Monday are overwritten bay the backup data of the actual Monday.

It is recommended to always make full backups unless performance is too low.

Backups should be stored at a safe place, preferably off-site. It should be noted that the backups contain sensitive data that may not be freely distributed. Hence, proper procedures and physical measures have to be implemented to avoid the backups falling into the wrong hands.

It should be clear at all times which officer is responsible to execute and supervise the backup activities. Further it should be clear to whom responsibility will be shifted in case the primary responsible officer is not available.

It is important to note that backups taken on floppy disks are not safe. They may be corrupted on account of mutilation, sunlight or other physical reasons. While taking the backup, it is also important to check the backup by restoring on another computer or on the same computer after ejecting and reinserting the backup disk.

3.5.4 ARCHIVAL PROTOCOLS, FACILITIES AND IMPLEMENTATION

Archiving in this context implies permanent storage of data. This can be anything like older sets (years) of hydrological data, finished products, one out-of-many backups, e.g. quarterly, yearbooks etc. The local DPCs may also submit data for archiving, by LAN or on physical media.

Media could be CD-R or DAT/DLT tape. The tape is more appropriate for larger amounts, up to 20 GB in uncompressed mode will fit on a single DDS-4 tape. For smaller amounts, up to a few GB CD-R may be used provided that the can be spanned across different CDs. CDs have the advantage that they support random access and can be used in any PC.

The storage life of CDs is not really known. The manufacturer's guidelines for storage and handling should be followed. Further, it is recommended to copy the data to new media, e.g. every 5 years.

Tapes (like DAT and DLT) in the custody of the DSC have to be rewound (re-tensioned) regularly which is to be scheduled accordingly. The manufacturer's recommendations should be adhered to.

Archive of all data belonging to a hydrological year, at least one original and a copy, should be kept on separate media. All relevant data and support files should be included to make it possible to use the archived data even if the databases and / or supporting software (DBMS, OS) have been changed (which is likely to happen). In case the DBMS and / or OS change it is recommended to convert all archived databases to the new platform and put the archived databases on new archive.

Products like Yearbooks should be archived on dedicated media, if possible together with full access software.

Long time (several decades) archiving is not as trivial as it seems at first sight. As mentioned above, the physical media need some scheduled maintenance and / or rewriting. But there is another aspect that requires due attention. The IT industry is still evolving rapidly and pushes new products, new technology and new systems to the market. As a result, systems presently in use will become obsolete soon. Two essential aspects have to be considered.

1. **hardware compatibility**

   It is to be expected that new versions of physical media will replace the incumbent ones. In the recent past this happened to the 5¼" diskette which is now fully replaced by the 3½" form factor. It is already difficult to purchase a new 5¼" disk drive. In a few years time, it will be very difficult to read data from a 5¼" diskette (it is nearly impossible to read from 8" disks, which were the standard in the early 80's). The same may happen with tapes and / or CDs. It is recommended that in case a physical data carrier, as used in the DSC, becomes obsolete, the data of the archived media should be transferred to the most appropriate media of that time. It is important to ensure that the transfer be done in a manner which allows for restoration of data without the need of the intermediate media, for example, in case multiple volumes were made on separate tapes, the new media should store a fresh backup created from a restored file rather than just images of the tape backups, which may not restore directly onto on-line media.

2. **software compatibility**

   Similar issues as described under hardware compatibility apply to the OS, software and the database systems.

   The following is recommended: archive the software tools that are required to access the data and to bring it online in the data storage system. This is to be repeated each time the software update / replacement also implies a change in data storage technology that is not compatible with the previous technology. Before archives become inaccessible, they should be "upgraded" to the software and hardware platforms and data formats of that time.

3.5.5 FACILITATE ADAPTATION OF DATABASES

Adaptation of the databases requires adequate knowledge and capabilities. During the lifetime of the databases and in particular of the database management systems and tools, changes will have to be implemented to adapt the systems to new requirements but also to cope with changing conditions. Similar aspects are discussed in the chapters on backup and archiving.

It is to be expected that the technology of the hardware and software platforms will continue changing which eventually will result in certain components becoming obsolete. It is the task of the DSC to envisage such events and take timely action by informing and advising the management.

Also the demand for services will change. The DPC may want more direct and faster access or remote access from sub-divisions, e.g. to deliver field data or retrieve authenticated data, objects etc.

In the SW and GW agencies the applied technology and methodology will be adapted to meet the user's requirements in the most efficient and effective way. Introduction of new data collection technologies may result in new data types and objects. In SW the ADCP (Acoustic Doppler Current Profiler) will gain more and more acceptance and will become a commonly used instrument. The ADCP for example does not only produce a large amount of velocity profile data but also signal intensity data, which is a presently not supported by the DSC. Other new types may be related to water quality or GPS coordinates in WGS84.

Although presently no on-line data retrieval is permitted for HDUs with the exception of very limited public domain data, it is to be expected that much like in other parts of the world, more and more data will be made available for public use, i.e. without restriction. This obviously would involve adaptation of the implemented security systems and separation of restricted and public data. Further HDUs may require new data formats to be developed and support of new physical media like DVD.

Popular DSCs will attract a lot of traffic and to avoid choking of the communication channels their capacity may need to be increased, possibly by adopting other communication technologies like ADSL or fibre. Related to that the hardware should also be adapted including the server configuration.

All in all for many reasons it is to be expected that the systems and services of the DSC need adaptation, this will actually be an ongoing process. It is one of the essential tasks of the DSC to keep its systems and services up to date.

3.5.6 CONTROL OF COMMUNICATION SYSTEMS

Initially, the HIS communication infrastructure relies on classic land based communication lines viz. PSTN, ISDN and Leased Line, further at some locations VSAT connectivity has been implemented.

The costing is channel dependent, an overview is given in the table below.

channel	hardware	availability cost	usage cost
PSTN	purchased	rented	pro rata
ISDN	purchased	rented	pro rata
Leased line	rented	purchased	annual cost
VSAT	purchased	purchased	annual cost

Table 3.1: Overview of communication costing

It is envisaged that in the near future new communication requirements will be defined. In particular web server connectivity will be introduced in more and more DSCs. The requirements of web server connectivity have to be assessed before deciding on the actual implementation.

Aspects that need consideration are:

1. Total hours of connectivity required
2. Speed and quality of connectivity
3. Value added services and other aspects with the connectivity
   - e-mail accounts
   - redirection and distribution facilities
   - information and patterns of usage
   - security issues (Shiva Certificate server for user login authentication and data transfer)
   - encryption features (PGP encryption presently supported)
   - compression
4. choice of communication with remote systems like
   - Peer-to-peer
   - Internet
   - Virtual Private Network on the Internet

The maintenance of the system entails:

1. AMC on hardware in case procured by the agency
2. renewal of access charges and rental charges as applicable
3. maintaining proper documentation and records for setting up the communication system

   The documentation should comprise all relevant particulars about the communication channels as administrated by the DSC. The administration of these particulars should be meticulously organised and frequent updates have to be carried out to cope with the continuous changes. Further, data may be security related and has to be administrated accordingly.
4. documentation specifying the standards and protocols to be followed for communication procedures and protocols have to be kept up-to-date.

3.5.7 MANAGE COMMUNICATION PROCEDURES AND PROTOCOLS

Also the protocols supported by other nodes may change and adaptations will have to be implemented to sustain normal communication.

Communication technology is developing rapidly as new capabilities become available. When new communication technology is implemented in the data centres, then the staff responsible for the communication infrastructure and systems should be trained in the management and operation thereof.

The DSC administrates the user rights of each employee and HDU, part of it is the control and monitoring of the permissions and limitations of each individual.

A firewall is part of the protection against hackers and other external hazards.

All procedures and protocols should be properly documented. Work copies should be kept readily available for the DSC's staff. The security related documents and the associated data require special attention. Access to such information is to be restricted to concerned staff only.

Adaptation / modification of hardware / software systems may affect the procedures and protocols, the latter have to be updated accordingly. The staff responsible for the communication infrastructure and systems may need refresher training.

The synchronisation of protocols with other participating DSC's is to be agreed upon at the national coordination level and adhered to. Scheduled meetings are needed for fine-tuning and modifications.

The schedule of data flow between DSC and DPCs is to be maintained and adapted if needed. Also the feedback in case of omissions has to be defined.

The same applies to data transfers and maintenance related to the Temporary data. The DSC, the local and owner DPCs are the parties involved.

The exchange of meta-data and Catalogues is essential for the HIS. The related protocols need strict adherence with a positive attitude towards servicing the HDUs. The processing of DRFs requires the same positive attitude. In particular the quick (immediate) follow-up of DRF should be pursued. The DRFs are the counterpart of the meta-data. The communication protocols for servicing the HDUs should be intuitive and open for use. The protocols and interfaces for HDU communication need regular adaptation to the latest common practice on the web, in particular to maintain a high standard of accessibility.

3.5.8 VIRUS PROTECTION AND FIREWALL

It is the task of the DSC to maintain and safeguard the databases and the contents thereof. Like with any other PC system where interaction with external systems is permitted, protection against virus attack is to be implemented. The DSC should subscribe to an update scheme of a virus protection system. The update services should include updating of new data files and virus protection software. That subscription should be maintained and an annual budget should be accommodated. Part of the subscription should be an immediate notification by the supplier of the virus scan system in case a new aggressive virus is detected to which the system does not offer protection, at the same time updates should be made available.

Check daily for the latest updates of the virus protection software and / or virus data files; load and implement the updates immediately, if any.

Regularly, e.g. daily, execute a virus scan on the entire network.

Regularly, e.g. weekly execute a virus scan on all individual PCs.

The scans should access all files including the various types of packed files.

Any new file on the network should be scanned before acceptance.

Any accessed file on network or PC should be automatically scanned for virus.

The virus protection software and updating subscription should be obtained at the national coordinating level primarily to reduce costs based on the scale advantage.

An effective firewall should be set-up to limit the external access to the network to the very minimum.

Demilitarised zones should be defined and maintained.

Do not admit unknown originators to the network.

Limit rights for reading, writing, changing and deleting to a practical minimum.

3.5.9 MAINTENANCE OF SOFTWARE

Initially, maintenance of software like (re)installation, patching, configuring and tuning, debugging will be covered by the AMC. Before the AMC expires, a new annual maintenance contract may be agreed upon or an alternative maintenance service could be implemented.

The DSC experts may take care of the first line maintenance. In that case some additional measures have to be taken. First of all it should be avoided that only one person is capable to properly maintain the software. Secondly, the DSC experts should be adequately trained in all relevant aspects (from the maintenance perspective). In case one or more of the trained experts are transferred new IT staff has to be allocated and trained.

Funds for IT staff, training and software updates should be allocated in the annual budget.

The maintenance should include:

- installation of software updates
- remedying of bugs, supply of work-arounds, patches
- configuration and tuning of software to specific application
- user support by helpdesk

The DSC administrates various software packages including the user rights. User rights define among others the users of the software, the user rights like plain use, change of configuration, save data, etc. Further the DSC staff should also distribute and administrate the distribution of hardware keys for operation of software.

3.5.10 REPORTING ON H/W AND S/W STATUS, MAINTENANCE AND REPAIRS

The reporting comprises two main types, i.e. reports and logs. Reports are intended for management and contain aggregated information. Logs are supported primarily by automated procedures and system functions. They are for technical use and to monitor the follow-up of problems. Typically logs have a sequential content, i.e. new data is appended to the logs tagged with appropriate time stamps.

Reports

The status of distributed hardware should be closely monitored, down to the detail of individual devices. The whereabouts (user and place of use, storeroom, under repair) of any device should be known at all times. The status of hardware implies aspects like: working condition, in use, reported problems and pending actions, expected time of return to normal operation, defective, damaged, beyond repair, obsolete.

The software status report covers similar aspects as hardware status report. Status is described by aspects like: operational, in use, reported problems / bugs and pending actions, expected time of return to normal operation, corrupt, beyond repair, obsolete. Software failure may also affect the integrity of the stored data and the administration thereof. The software failure can be localised in a single program or function but can also be caused be a chain of interactions between the operating system, the operational software, data and hardware. The software status report should address the likelihood and the estimated extent / complexity of such interactions.

In case of repairs or debugging, the problem, the assessment of its cause, the remedying action (including activities and required material / tools / resources), estimated time to implementation, costs, executing agency) have to be reported. The report should also include an action plan, which is to be pursued, and the progress monitored. If a repair order is given, then priorities and proper deadlines should be defined, in case a deadline is not met the cause should be identified and appropriate action is to be taken. The follow-up of repairs should also be monitored and reported upon. Simple cases can be covered by a simple report, e.g. just stating the fact of pending repair (when repair is expected to be finalised, by whom) or the successful re-deployment of the repaired component. More complex repairs must be executed as a project, part of which proper reporting should be scheduled.

Aggregated versions of the hardware and software status, maintenance and repair reports should be forwarded to the national coordination level in-charge of co-ordinating with the concerned vendor. By analysing the reports of all the DSCs, common patterns could be identified and tackled in a concerted way. Cooperation would save a lot of resources and keep the standardisation of software and data at a high level.

Logs

Two main log types are implemented, viz.:

1. Machine-wise Log
2. Data Centre Log

In support of the logging activities, log forms and databases should be implemented. Entries should be identified in time, place, machine and staff.

The machine wise log will be maintained for each computer and will keep track of the following aspects as presented in the list below. Both hardware and software problems pertaining to the individual machine appear in the same log.

- Call Number (if applicable) attributed to the problem
- description of the nature of the problem
- date and time the problem was reported and by whom
- previously reported on date / time / previous Call Number(s) if any
- engineer name, date, time and diagnosis
- estimated repair cost, if any
- parts / deliverables required, if any
- planned date and time to fix the problem
- rectified – Yes / No / Observation / remedial action
- finally rectified – Y/N, date if so, else date the problem was discarded
- parts replaced with serial number, new drivers: particulars

The machine log will also have a monthly summary of the following:

- backup and restore information
- scandisk
- virus scan
- disk defragmenting

The summary comprises dates of the concerned activity, the result (like successful or failed) and additional information related to the activity. In case of failure its major aspects should be entered in the log. Further a problem report should be made and submitted to the officer / section responsible for repair and maintenance.

The summary should fully identify the machine, elements and aspects involved.

Please note that all logs have to be on hard copy as they cannot be on the computer itself in case it becomes defective

The Data Centre Logs will contain the following information:

- scheduled and unscheduled backup and archival of data
- virus checks on the network, beyond machine checks
- inventory of equipment, software, manuals, communication lines, data
- snapshot of status on pending calls

4 FIRST LINE MAINTENANCE

Proper routine maintenance is necessary to remove dust and to ensure proper functioning. The cabinet needs to be closed properly, both from front and behind, so as to prevent the entry of dust and rodents. Waste and obsolete paper should not be kept lying idle but collected for other use or disposal instead.

Old and outdated files, like temporary files should be deleted regularly. Hard disk scans and defragmenting should be performed routinely, e.g. at weekly intervals.

Installation of unnecessary or private software should not be permitted

- to limit the risk of virus attack
- to avoid incompatibility problems with the DSC's software systems
- to avoid wasting of computer resources
- to maintain maximum performance

The power supply should be properly stabilised and on a separate phase from the air-conditioners.

Corrective maintenance is also performed when required as certain electronic components and mechanical components are subject to failure. These are normally covered under a comprehensive AMC (Annual Maintenance Contract).

Inkjet and Laser printers are susceptible to dust induced problems. Long periods of inactivity also cause problems in these devices as their printing and paper movement mechanisms are purely mechanical.

UPS batteries, if not maintenance free, require standard procedures as prescribed for automotive batteries, like topping up with water, to be carried out at regular intervals.

Regular checks need to be performed on all communication media and networking products.

One additional reason for concern is the mishandling of magnetic media like floppies. If left in the sun, the surface coating may melt and when used, sticks to the head of the floppy drive. This drive will now scratch all floppies inserted into the drive, and the problem will spread to other computers. It is therefore extremely important to handle the media in a proper manner and to take immediate corrective action in case such a problem develops.

Virus attacks can occur through removable media and the Internet (or any other communication medium). The virus attacks can range from simple irritating messages and slower performance to total loss of data. Data being the most valuable resource of the Data Centre, frequent backups taken in a proper manner are a must. Also, all virus scanners must be current and care must be exercised while handling external media.

The computers in the Data Centres are run off the Windows family Operating System. It is an established fact that the Windows family in general provides a very easy and intuitive interface to the user, however, it is not as stable as may be desired. The performance of a Windows computer also degrades with time; for which it is required that a periodic reinitialising of the entire OS be carried out. To reduce the risk of loss of data or installed software precautions have to be taken. A complete log if installed software and the configuration thereof should be maintained. The installation software, drivers, initialisation codes and other essentials for installation need to be available. All stored data should be save on double backups. The latter should be tested for possible corruption. Only if all precautions are taken and verified, the OS should reinitialised.

4.1 MAINTENANCE ASPECTS

Electrical Supply

All points for mains and UPS need to be checked for sparking and worn out plugs and sockets should be replaced. Loose sockets should be securely and permanently fixed. It is also essential to ensure that no loose wires are lying on the floor, adequate extension boards are available and that the boards are equipped with fuses. MCBs should be checked and cleaned regularly. Proper safety measures should be in place though. Fire extinguishers should be handy in compliance with local regulations.

The computers should be on a different phase from the air-conditioning. Proper earth-neutral and earth-live voltage should be ensured. This is especially important in the monsoon season. No cables should be lying on the floor and water ingress, e.g. due to rain or floor mopping, should be avoided.

UPS points should be distinct from the main power supply points. This can be achieved through proper labelling, different coloured plates or by using different pin configurations for UPS and mains. Another method could be to have UPS and mains points at different heights in the room.

The conduits carrying electrical wire should be separated from network wiring, preferably by 1m or more.

Lighting

For each computer station adequate lighting should installed and maintained operational. Care should be taken that light does not directly reflect off the screen into the user's eyes.

Air conditioning

Proper air-conditioning has to be ensured. It should be on a different phase from the computers and the stabiliser should be equipped with a time delay circuit.

Room coolers are never to be installed. The increased humidity, which they cause, is very harmful for the electronic circuits.

In case of emergency, a normal pedestal fan may be mounted directly behind the computer to facilitate air-circulation.

Furniture & Storage

The tables for the computers should be maintained well. The keyboard drawer should be functional and the keyboard and CPU covers kept properly. Printer tables and the chairs have also be checked for proper levels and for all castors installed.

Storage locks should be checked regularly and an extra key kept in a safe location.

Flooring

The floor has to be kept clean at all times and any damages repaired immediately as dust will affect the computers' performance. Carpets are not recommended in the Data centre.

Hardware

The hardware comprise among others:

- computers
- printers
- scanners
- plotter
- network components
- mass storage and backup devices
- communication components
- other peripherals
- UPS

The hardware should be kept clean and all housing should be kept closed. For the equipment an Annual Maintenance Contract should be entered into.

System software

The system software comprise among others:

- Windows 95 / 98 / NT / 2000 / XP
- MS-Office
- virus scanners
- device drivers
- backup software
- connectivity pack
- firewall
- other software

Application Software

The application software comprise among others:

- database administration software

- data storage software
- software tools

All the installation software for the OS and the various application software packages (old and new) should be kept in a locked enclosure. Copies should be kept in a separate location for safety. All software on magnetic media (tapes, floppies etc.) should be refreshed onto new media every year.

Hardware keys belonging of certain application software should be properly administrated. At all times the responsible user should be known and in the possession of the hardware key.

Consumables

- floppies, CD-R,CD-RW, tapes etc.
- stationery
- cartridges, toners, ribbons etc.
- printer paper
- print heads
- batteries

All media and backups are to be kept in a locked enclosure in a dust free and low moisture environment.

The cartridges and toners should not be stocked for too long as they have a short shelf life and in case of prolonged disuse, should be cleaned properly before printing.

The recording surface of the CD and the magnetic portions of tapes and floppies should never be touched by hand.

Every used media should be properly labelled and stored. Diskettes should always be kept in protective boxes, away from moisture, heat and magnetic materials / fields. It is strongly advised against to keep diskettes lying on a desk or in drawer.

Batteries that are not maintenance free should be regularly (at least once a month) topped up with battery water.

4.2 DISASTER CONTINGENCY PLAN

A contingency plan to limit the damages of any disaster should be prepared and implemented. The contingency plan should address the procedures to cope with partial or complete loss of:

1. hardware,
2. software,
3. data and
4. office space.

The plan should define the responsibility of each staff member.

An overview of required hardware, interfaces, peripherals and drivers should be maintained. The overview should also include the configuration details. The overview should be stored at a safe and separate location, e.g. together with the software originals. A copy of the overview is to be stored with the software copies.

Same arrangement should be made on how / where to obtain replacement hardware. Possibly this is from the hardware AMC provider or from other offices in the agency. However, it is quite likely that in case of a major disaster like fire, earthquake or flooding the other offices in the same building including the hardware will also be damaged.

As mentioned elsewhere in this manual, originals and copies of all installed software should be installed at different places, preferably at least one of the two at an off-site location. The major systems are assumed to be available from the AMC provider as well.

Also the installation record, i.e. a list of installed software, installation sequence, patches, configuration and other required information should be kept together with the software originals and copies. Based on that information a detailed installation plan can be defined and executed. The software not only includes the application software but also the operating system, tools and auxiliary software.

For the safe guarding of the data routinely backups are made and stored.

Contact details of offices and persons that might be required for assistance should be maintained. Assistance may be obtained from the AMC providers, other DSCs, vendors and developers.

The contingency plan should also define who is to do what and when.

5 ANNUAL MAINTENANCE CONTRACT

In the IT context, Annual Maintenance Contracts (AMCs) have to be implemented to arrange for the required support to keep all systems and functions operational. Separate AMCs have to be in place for hardware and software. Initially, the AMCs will be engaged with the original vendors, at the time of termination of a contract, possibly a new service provider may be contracted; depending upon the performance of the original one, the offered rates and the capabilities of the various bidders. For separate, i.e. unrelated software systems, different service providers may be selected. The standard software for normal office use like word processing, project management, spreadsheet and the like may be contracted to a local service provider or supported by in-house experts. For the HIS related systems the contracting should be coordinated with the other DSCs this to maintain the HIS standards and to benefit from reduced cost because of the larger scale.

The hardware AMCs may also be broken up between different vendors depending upon the original supplier or the type of equipment. UPS maintenance may, for example, be contracted to a UPS specialist rather than to an IT services provider.

In this chapter some guidelines for the implementation of Annual Maintenance Contracts (AMCs) are given.

5.1 COVERAGE

It is desirable that the hardware is under a comprehensive maintenance contract covering all parts and on-site service support with well defined parameters on fault rectification. The contract should have provision for standby arrangement and escalation of problems in case of delay. Adequate protection in terms of penalty clauses needs to be defined. All parts exempted from the AMC coverage should be clearly defined by the vendor.

For hardware the AMC would cover all hardware related to the computer, peripherals and auxiliary systems for a defined period for scheduled preventive maintenance and as-and-when required corrective maintenance. The AMC is on-site, which means that the vendor is responsible for repair or replacement of the defective parts at the client site, in this case, the Data Centre.

Hardware AMCs generally cover all parts except consumables like printer cartridges, toner cartridges, print heads and batteries. All other parts are normally covered for free replacement. It is also important to realise that also consumables are covered by warranties, so any defects in the workmanship or the quality has to be rectified by the vendor. It may be noted that in the specifications for the procurement of DSC hardware, the batteries of the UPS have been covered for warranty.

Software AMC would cover the installation of updates, new releases and upgrading. Further the remedying of malfunctions, bugs and flaws has to be covered.

If any of the remedies or updates impact on the data, also data conversion would be required. The manuals should be updated and / or replaced to completely reflect the actual software and systems.

In case any part is not covered under the comprehensive contract on account of product obsolescence, it would be necessary to have coverage under an insurance policy for the same.

5.2 SERVICES

AMC requires coverage from the vendor on all normal working days within regular office hours. The contract lays out the exact details; however, it is expected that in case the engineer does not visit within 24 to 48 elapsed hours of the call being reported, a penalty will be imposed on the vendor. In case the problem is not rectified within a specific time frame (4 hours to 24 hours); the vendor has to provide an ‘equivalent’ (functionally equivalent standby). Failure to do so calls for a more severe penalty. The rectified part / replacement has to be finally put in within a pre-specified time frame.

It is important to finalise with the vendor as to whether a temporary or a permanent replacement has been provided. In case a permanent replacement has been provided, especially in the case of a complete item like a printer or monitor, records will have to preserved for future warranty references and insurance claims.

A complete paper trail of request for assistance, AMC provider’s response, remedy and report should be maintained.

It is essential to remember that almost no AMC covers data. It is therefore of the utmost importance to ensure that proper and adequate backups of all data are maintained at all times.

5.3 CHARGES

The majority of contracts specify AMCs with quarterly payments. Six monthly and annual payment modes are also preferred for lower value contracts. Individual AMC can differ from this depending upon the location and the situation. There is also the provision of a performance guarantee being provided by the bidder in the form of a Bank Guarantee.

Penalties accrued in the previous period can be adjusted in the next period’s payment. No charges are allowed for any replacement whatsoever except for deliverables excluded in the AMC. No charges are payable on any account like freight, courier etc. and the entire cost has to be borne by the vendor except for the purchase of consumables.

It is recommended that the vendor be asked to provide the market (not list) prices of all consumables at the time of signing of the contract. In case any of these have to be procured, the local market conditions can then be examined. In case the contract is renewed from year to year automatically, it is desirable that the price list be updated periodically. In some situations it may be wise to obtain a no-objection letter from the vendor for procurement of consumable items from a third party.

5.4 STANDBY EQUIPMENT

For remote locations and for larger installations, the vendor may choose or stipulate the availability of standby equipment at site. No extra charges are payable for the standby as it has been furnished for the vendors’ convenience. However, it has to be kept in a secure area and a proper record maintained of its components.

5.5 REPLACEMENTS

With the rapid development in IT, it is possible that some parts of computers are not available and better or more advanced parts have to be provided. It may also be possible that some normally working parts are to be changed to get the computer operational. This is the vendors’ responsibility as he has signed the AMC on the premise that he can repair the computer when required. This provision is anyway built into all Hydrology Project procurement for a period of six years.

5.6 SOFTWARE

The AMC provider, initially the software supplier, is responsible for its working under the AMC. The AMC provider can be called upon to reload the software as and when required. However, maintaining backups remains the DSC’s responsibility, though help from the AMC provider can be requested for. The latest version of all software should be made available, however, the decision to actually install the upgrade or replacement software is to be taken in concert with the DSC management, this to avoid any unnecessary risk with respect to system performance and stability.

The same holds true for virus scanning software. However, any new data files or software upgrades should be installed immediately.

5.7 PREVENTIVE MAINTENANCE

A regular schedule for preventive maintenance has to be worked out in consultation with the AMC provider and included in the AMC, which has to be adhered to by AMC provider.

5.8 NETWORK

In Data Centres that have networking installed, the networking components should all be covered under AMC. It is also recommended that standby networking equipment – hubs and wires should be provided by the vendor to prevent downtime.

5.9 RECORDS

Complete records for the entire process of corrective maintenance needs to be adhered to for proper reporting on downtime and AMC effectiveness.

A complete inventory of the hardware and system software has to be maintained with the help of the vendor. The system software should be backed up on separate CD’s (unless specifically forbidden by the terms of the software agreement). The hardware record should have the complete details with part number down to the major component level (like Hard disks, monitors etc.). It would be the duty of the vendor to provide standard do's and don'ts for all the equipment to be maintained.

In case of problems that are repeated, the vendor may ask for a record to be maintained for diagnostic purposes. Complete co-operation has to be extended on this account.

Multiple AMC vendors in a single installation tend to blame the product of the other(s) for any fault. To prevent this, proper records have to be maintained.

Logistic support and storage space may be required to be provided to the vendor depending upon the terms of the contract. The resources for this should be set aside to ensure smooth functioning of the data centre.