SOCIB Data Repository Preservation Plan

DCF and CIT

Version 1.0
20/11/2021

List of Acronyms

AIP   Archival Information Package
CIT   Computing and IT Service
DCF   Data Center Facility
DIP   Dissemination Information Package
DMM   Data Management Maturity model
DMP   Data Management Plan
SIP   Submission Information Package

Index of Content

This page intentionally left blank

Document type:	Strategic Plan
Date:	2021-11-20

Description:	This document describes the Preservation Plan of SOCIB Data Repository.
Authors:	M.À. Rújula, J.G. Fernández, S. Gómara
Supervision:	J. Tintoré, J.G. Fernández
URI:	https://repository.socib.es/repository/entry/show?entryid=504dd999-0e5e-49c0-b2e1-790559055fd0
Access:	Public

DOCUMENT DISTRIBUTION LIST

Date:	Distribution to:

CHANGE RECORD

#	Date	Description	Author	Checked by
1.0	20/11/2021	1st version of the document	M.À. Rújula, J.G. Fernández, S. Gómara	J.G. Fernández, J. Tintoré

This page intentionally left blank

1. Purpose

This document defines SOCIB policy on preservation, including for the designated community of users. This policy generally conforms to the OAIS Reference Model, with additions and alterations that are specific to the materials held within SOCIB.

The SOCIB Data Repository is hosted by SOCIB (Sistema d'Observació i predicció Costaner de les Illes Balears), which is a national marine research infrastructure included in the Spanish Large Scale Infrastructures (ICTS, Infraestructuras Científicas y Técnicas Singulares) Map, updated in November 2018.

It contains data on the domain of oceanographic and coastal sciences. The data collection comes from different observing platforms (e.g., High Frequency radar, gliders, drifters, buoys, etc.) and forecasting services (numerical models). Main roadmap and objectives of the repository are driven by the ocean and coastal communities, national or European marine directives.

It also includes data coming not only from the SOCIB's observation programs and projects, but also from different research projects within the Spanish National Research Plan (MOCCA, MUSA, Pre-SWOT, etc.), European (Jerico-S3, EuroSea, Euro Argo RISE, etc.) and International research projects (eg. Calypso_ONR). The metadata included in the different files has the specific information. SOCIB repository is used in these projects as an archiving tool, from which research can be done in a different phase.

SOCIB detected ten ocean and coastal sectors and associated communities that use SOCIB's repository: marine and coastal research, maritime safety, marine sports, beach and coastal communities, coastal protection and planning governance, sustainable marine ecosystems, ports and shippings, ocean management, sustainability of islands and climate change, and educational.

A preservation policy helps SOCIB meet legislative and accountability requirements and its user communities' expectations. SOCIB ensures that it is at the leading edge of technical advances by taking a strategic approach to long-term digital preservation, and by monitoring hardware and software developments and migrating its collections accordingly.

SOCIB also aims continually to improve all aspects of the preservation-related workflow by embedding an awareness of quality in all processes.

2. Scope

The scope of this policy is limited to SOCIB's data collections, which include raw data files, as well as the resulting processed data. It also includes supporting databases that contain metadata used to perform the processing step. It deals with all aspects of preservation and applies to all materials held for long-term digital preservation by SOCIB.

This policy only covers the preservation of data collections for which SOCIB is the primary custodian. It does not consider preservation of other materials such as SOCIB web pages, internal administrative documents and correspondence. Some of these materials including third-party standards, legislation, policies and procedures have a direct impact on the preservation process, but are out of the scope of this document.

SOCIB's preservation strategy is not formulated in a single document but rather is embedded across a range of business information related to data curation and preservation.

2.1.   Objectives of the plan

SOCIB is also responsible for ensuring the authenticity and integrity of the data. Any strategy for the long-term preservation of any digital information must address the issue of software dependence. For most digital information and in particular research data it is generally possible to eliminate software dependency. Thus the primary goal of SOCIB's preservation plan is to ensure the long-term accessibility of data collections while ensuring the highest level of authenticity possible.

The specific aims of the preservation plan are to:

- provide authentic and reliable instances of datasets to researchers;
- maintain the integrity and quality of the datasets;
- ensure that digital resources are managed throughout their lifecycle (e.g. when migrations or changes in metadata are carried out) in the medium that is most appropriate for the task they perform;
- ensure that the relevant level of information security is applied to each dataset;
- and so to be a "trustworthy digital repository".

3. Requirements

3.1.   SOCIB's requirements

SOCIB has developed a series of requirements which it strives to ensure as closely as possible:

- the datasets are checked and validated according to strict data ingest procedures (see section 5.2);
- the data are professionally catalogued according to appropriate metadata standards;
- the data, documentation, metadata and other representation information are preserved for the long-term;
- the authenticity, integrity and reliability of datasets preserved for future use are retained;

3.2.   Legal and regulatory framework

The mission of the ICTS SOCIB is to operate a coastal ocean observing and forecasting system, a scientific and technological infrastructure that provides free, open, quality controlled, and timely streams of oceanographic data, as well as data stewardship and long-term preservation.

The ICTS SOCIB follows the European Union recommendations that promote the creation of a more open, transparent, collaborative and sustainable global system of scientific communication, pursuing a greater impact and scope of research results and the exploitation of research data. In this context, following the Spanish State Plan for Scientific, Technical and Innovation research for the period 2021-2023, SOCIB provides open access to the scientific results and the data derived from its activities as an ICTS, through the storage in its repository, in compliance with Article 37 of the Law 14/2011, of June 1, of Science, Technology and Innovation, and the recommendations related to the European agenda on open access and open science, among which data preservation stands out.

Open Data is one of the pillars of Open Science, a movement that promotes free access to open research data to facilitate its use, reuse and distribution. Moreover, its publication guarantees the free access and its correct preservation, reproduction, diffusion, visibility and impact. The correct preservation of data permits a faster replication and verification of studies.

In addition, as a consortium with the participation of CSIC, SOCIB aligns with the institutional mandate of open access at CSIC that emphasizes the research data management following the FAIR principles. This mandate connects with SOCIB's institutional commitment to provide free access through its data repository, in line with the good practices and research data policies of DIGITAL.CSIC.

4. Roles and responsibilities

Most data managed by SOCIB comes from its own observation platforms (e.g., High Frequency radar, gliders, drifters, buoys) and the operational models. The responsibilities and roles are specified in the Data Management Plans which serve as meeting points between the facilities and the Data Center.

Some observing platforms belong to national institutions (like PortsIB). In this case although no formal agreements are signed, a kindly collaboration is ongoing that allows working on defining the actions needed.

Concerning external projects, a Data Management Plan (DMP) is written beforehand.

All IC&T department staff, assisted by the Data Center department, are responsible for implementing the policy contained in this preservation plan as appropriate to their roles and responsibilities. The head of the Data Center department is responsible for maintaining this policy.

5. Model

The following chapters are structured around the main functional concepts of the Open Archival Information System (OAIS) reference model for digital preservation environments as well as the FAIR principles. The OAIS reference model is an international standard which proposes common terms and concepts and a framework for entities and relationships between entities in digital preservation environments.

Preservation decisions at SOCIB are made within the context of SOCIB's mission and strategy, balancing the constraints of costs, scholarly value, user accessibility, and legal admissibility. SOCIB's processes are organised according to this model.
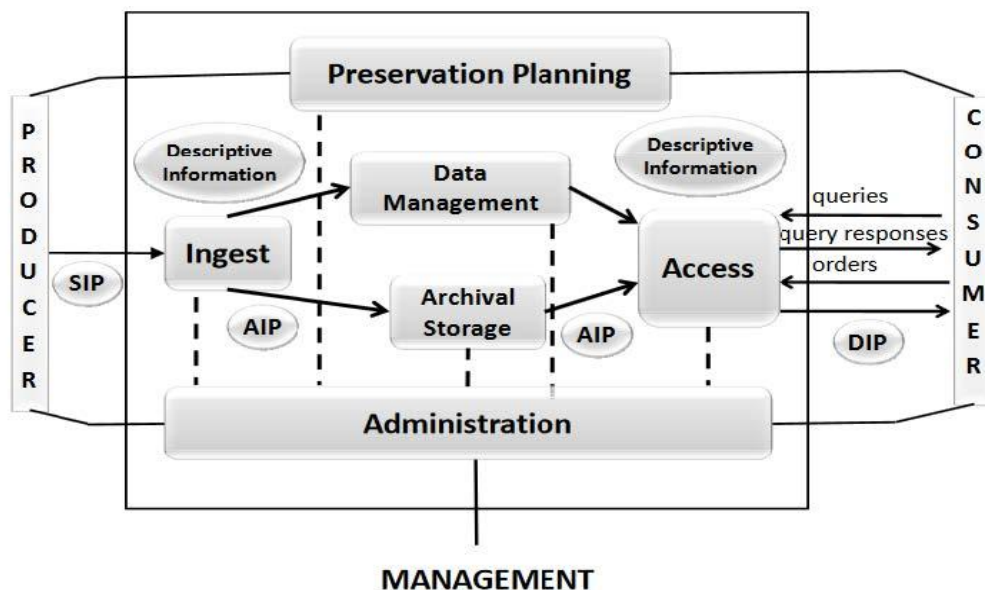
Figure 1. The OAIS model.

5.1. Pre-ingest function

Officially, the pre-ingest function is not part of the OAIS model. However, SOCIB strongly believes that documented pre-ingest procedures help to reduce costs, minimize errors during the ingest process and ensure that data and metadata are well defined.

The selection of the data to be placed in the repository is done by qualified technicians or scientists based on the Global Ocean Observing System (GOOS) and scientific objectives, SOCIB is adopting common standards and is focussing on the Essential Ocean Variables.

The pre-ingest function also includes the introduction of proper metadata in an internal database. This metadata is later used in the ingest function for the creation of Dissemination Information Packages (DIPs) in OAIS terminology.

5.2. Ingest function

Ingest is the first functional component of the OAIS reference model. It includes the receipt of information from a *producer* and the validation that the information supplied is uncorrupted and complete. This process also identifies the specific properties of the information to be preserved; it authenticates that the information is what it purports to be.

The supplied version, which comes from the different instruments and sensors, is known within SOCIB as the "raw file". This original version is retained for preservation in its original

format and stored in the appropriate directory within the preservation system. This supplied version has a close correspondence to the OAIS Submission Information Package (SIP).

The ingest function also transforms all elements of the deposited files into a valid preservation format, which is always NetCDF, as it is the "de facto" standard in the Designated Community (oceanography). This transformation is performed by in-house developed applications and toolboxes (processing application, glider toolbox, radar toolbox). In some cases, they can be adapted to ingest new data formats (creating a new parsing function), but in some cases this is not trivial to do and this fact is taken into account. In particular, the maintenance of the processing applications, and their backwards compatibility (reprocessing), plays a key role in preserving SOCIB's ability to ingest data.

It's also important to note that the information in a resulting DIP may come from a collection of SIPs. So, there's not always a one-to-one relationship between SIPs and DIPs.

All changes in the metadata and configuration databases, which are used by the transformation tools, are tracked. The ingestion process is also monitored automatically, and the results reviewed by technical and scientific staff to ensure the authenticity and integrity of any data collection. Moreover, a software tool is executed in the background to validate the metadata included in the resulting DIPs (NetCDF files), as well as the metadata used during the processing.

The ingest function uses the corresponding metadata introduced in the pre-ingest function in order to process the SIPs and produce DIPs in the main archiving format (NetCDF).

The version resulting from the ingest process is an Archival Information Package (AIP). All actions related to the preservation of the data are documented in the corresponding Data Management Plan (DMP).

5.3. Archival storage function

In essence, the purpose of archival storage is to ensure that what is passed to it from the ingest process remains identical and accessible. In SOCIB this function receives AIPs and DIPs from the ingest function and stores them in their corresponding directories. This function is also responsible for ensuring that AIPs can be retrieved.

SOCIB does not follow the OAIS model fully. In the model there is a "Provide Data Function" whereby the Access function of an Archive can request AIP transfer from the storage area. In the reference model this process ensures that the end users receive an authentic version of the data collection. However, this is not applicable to SOCIB's model and operations as the SIPs contain raw data coming directly from the sensors network, which need to be processed to be usable.

Additionally, in some cases, certain data from the SIPs is not published for security reasons or because it's not relevant to the end users. SOCIB has elected to prepare DIPs (NetCDF files) as part of the ingest process. These DIPs are accessible to users via a 'Provide Data Function' and identical copies are also stored alongside the AIPs in the preservation system. Thus, for any data collection there are always at least three information packages residing on each of the different preservation systems: the original SIPs, the ingested AIPs and the resulting DIP. When a new version of a DIP is created it must be created from the AIPs (or possibly the SIPs if they are understood to be a de facto subset of the AIPs) but not from an earlier recension of a DIP.

5.4. Data management function

Data Management is the third major function of the OAIS reference model. It maintains databases of descriptive metadata; supports external finding aids; and manages administrative metadata which support internal operations, including change control.

Ensuring that any alteration to the preserved version of any part of a data collection is accurately documented is integral to the authenticity of any data collection.

SOCIB uses an internal database, called "*management*", to store the metadata associated with each data set, and the configuration to process the raw data files during the ingestion. This database is not modified directly, but through an internal web application called "*instrumentation*" that keeps track of any change (who, what and when). The access to *instrumentation* is restricted to SOCIB staff through user and password.

SOCIB distinguishes between two forms of alteration post ingest:

- update (Definition: when new data is appended to a data set)
- new version (Definition: when a data set has been re-processed due to changes in the metadata or the processing configuration)

The repository always publishes the best version of a data set. This means that, in general, when a new version is generated, it replaces the previous one, which is not preserved.

On the other hand, a Digital Object Identifier (DOI) managed by DataCite is assigned to a data product, only once SOCIB's scientific and technical staff consider that the level of curation and quality are adequate. The metadata scheme offered by DataCite (see R7-D5) is followed to manage the data products metadata.

Data products with a DOI have a strict semantic versioning policy and an archiving system to guarantee reproducibility any time the data product is requested. The data product is always

served in a compressed file that contains the corresponding datasets (NetCDF files). The compressed file that represents a data product is periodically updated, replacing the previous one. In addition, the versioning policy indicates if a copy of the previous version needs to be archived to maintain reproducibility. The different versions of a data product include the time range in which such a version is valid. In addition, each version includes a change-log file with appropriate information about the changes that were applied respecting the previous version. Every time a new version is generated, regardless of its importance or relevance, the metadata in DataCite is updated. The DOI assigned to a data product never changes.

Only the latest version of the product is available directly. Older versions are archived and available under request.

5.4.1.   Data objects identification

SOCIB data objects with Persistent Identifiers (PID) can be divided in 3 categories:

- The first category is composed of high level data products and they are identified by means of the DOI system.

- The second category is composed of data collections belonging to the high level data products. These data collections are identified by a unique local hash ID within the SOCIB data category (eg. space name), and it is managed by an automatic system and a relational database.

- The third category are the NetCDF files that comprise the data collections. In this case the PID is the unique id attribute in the global metadata. Additionally, the file name is unique within SOCIB. These file names are managed by an automatic system and follow a documented naming convention.

It's important to note that, ultimately, all the data in the SOCIB Repository are contained in NetCDF files (third category above) that are easily accessible through the Thredds server individually, regardless of the high level data product they belong to.

5.5.   Access function

This OAIS function contains the services and functions that make the archival collection and related services visible to consumers. In this function end users interact with SOCIB to find, request and receive data collections. These three separate, but interrelated operations are:

- finding data collections;
- requesting data collections;
- delivering data collections.

The access function must also implement the security relating to access; all access management failures are logged and processes reviewed periodically.

SOCIB provides three main interfaces to access the data collections:

- The Data Catalog is a user-friendly web page that allows users to find data collections using several filters (name, dates, status, variables, platform types, instrument types, feature types and gps coordinates).
- The Thredds Data Server is a web server that provides metadata and data access for scientific datasets, using OPeNDAP, OGC WMS and WCS, HTTP, and other remote data access protocols.
- The Data API, for machine-to-machine communication.

5.6. Administration function

In the OAIS model the 'administration function' manages the day-to-day operations of the repository. In SOCIB the roles of this function are spread across different internal documents in the Data Management Program, based on the Data Management Maturity (DMM) model of the CMMI Institute, although the designated Data Steward has a key role in it.

6. Preservation planning and strategy

Several services and processes in SOCIB's organisation relate to what is known as "Preservation Planning" in the OAIS reference model.
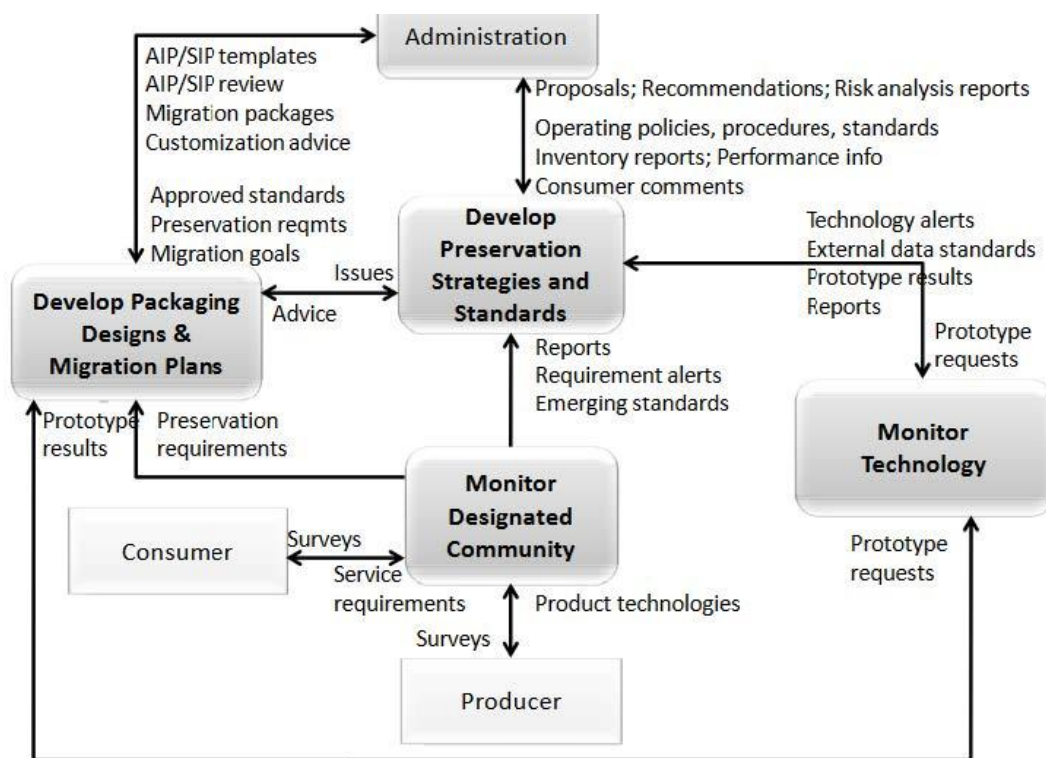
Figure 2. *Functions of the Preservation Planning Functional Entity in the OAIS model (Reference Model for an Open Archival Information System (OAIS), Recommended Practice, CCSDS 650.0-M-2 (Magenta Book) Issue 2, June 2012. Figure taken from page 4-14).*

6.1.   Preservation strategy overview

SOCIB has chosen to implement a preservation strategy based upon open and available file formats and data migration.

SOCIB's preservation strategy is predicated on two basic principles: first, that digital storage media are inherently untrustworthy unless stored appropriately; second, that all file formats and physical storage media will ultimately become obsolete.

The Data Center Facility has developed a general Data Management System that is continually being improved to guarantee international standards, quality assurance and interoperability. The combination of different sources and types of information requires appropriate methods to ingest, catalogue, display, distribute and preserve this information.

The Computing & IT Service team is responsible for providing the major computing infrastructure to support SOCIB Observing Facilities, Data Centre, Modelling and Forecasting, and general operations. Importantly, the Computing & IT Service also ensures that the SOCIB Data Repository, a key asset, is protected and that SOCIB complies fully with the requirements of Data Protection and Data Storage regulations. All technical processes such as security, changes, hardware upgrades and service-desk are managed and operated by Computing & IT Service employees.

Thus, the SOCIB Data Repository is mainly managed by two teams: the Data Center Facility and the Computing & IT Service, each of them having their own duties and staff. They jointly provide the IT infrastructure and computing services to acquire, maintain, access, distribute and preserve data of interest and develop visualization tools. Both teams are ensured with long-term sustainability and stability. Specific achievements per team are described in the SOCIB Strategic Plan 2017-2020.

The data is published in the NetCDF format, which is a well-established, de-facto standard in the scientific community, with long-term support. The generation of metadata follows interoperable and international standards in order to facilitate data discovery, while adopting the European Directive INSPIRE (European Commission 2007). In addition, CF vocabularies (standard names, feature type) are part of the metadata being offered by the repository. Following these standards and best practices facilitates the maintenance and evolution of the data in the repository.

The Data Center Facility and the Computing and IT Service constantly improve their services to meet the requirements of long-term access and availability of data in the repository. The latest developments and technological progress to stay informed of the best practices for long-term preservation are followed.

The funding for the two departments in charge of the repository is sufficient to maintain core operations and activities (data archiving and dissemination, information service).

In the case of a potential risk, a remote backup stored in the secondary Data Center (further explanation in the Security section) eventually will provide continuity of access to the data, meaning that the backup would be restored in the primary Data Center as soon as possible.

Additionally, the SOCIB Strategic Plan for the period 2021-2024 (publicly available soon), describes the continuity business plan and the disaster recovery plan in two phases:

- Phase I (approximate start date Dec. 2021): Deploy a secondary backup environment over a cloud infrastructure, to ensure data availability.
- Phase II (approximate start date Nov. 2022): Deploy a fully replicated on-cloud datacenter infrastructure.

Once Phase II is complete, SOCIB Data Center will be able to resume the service quickly in the cloud infrastructure, while fixing any disaster in the main Data Center infrastructure.

Several data collections managed by SOCIB Data Repository are already ingested or replicated by other international-level repositories; with the master copy of data collections kept at SOCIB. This allows users to potentially keep accessing the same data sets in case SOCIB Data Repository discontinues its service, whether it's temporary or definitively. Some of these portals are:

- CMEMS: In Situ data from SOCIB platforms
- EMODnet Physics: In situ data for SOCIB platforms
- EMODnet Chemistry (SeaDataNet): Analysis from laboratory samples data obtained from scientific cruises.
- EGO: Glider Near Real Time and Delayed Time (recovered) data
- Coriolis Argo GDAC: Profiler floats data in the Argo Program.
- ERDDAP NOAA: Surface drifters data (SVP) through the Global Drifter Program.
- European HF-Radar node: data from the Ibiza radar network.

SOCIB is a member of some of the institutions that manage these repositories.

CSIC, the Spanish Council for Scientific Research, entered the SOCIB Consortium partnership in December 2020 and this will be a major step forward to guarantee sustainability of both SOCIB and SOCIB data holdings.

In the unlikely case of a SOCIB closing and according to Spanish regulation, all information and scientific data will be transferred to the most appropriate partner institution as well as any economic obligations (e.g. DIGITAL.CSIC is the institutional repository of the Spanish National Research Council, CSIC).

Every data collection within the preservation system follows a consistent directory structure for storage. This has many benefits, such as the ability to find set types of information and also to allow automated tasks (e.g. migration of file formats) to be run without the need for complicated locator scripts.

6.2.   Integrity measures

In SOCIB, the whole data lifecycle is automated. This is, from the sensors sending their data, to the final introduction into the repository made by the corresponding processing application. When a new instrument or sensor is added to SOCIB's sensors network, Data Center technicians add the new configuration to the databases, set up the necessary QC

automated tests, develop new parsing functions (if needed) and, finally, make sure that the data is arriving correctly into the repository.

As mentioned above in section 5.4 (Data management function), SOCIB keeps track of any change in the metadata and configuration databases, which are used by the processing tools. The ingestion process is also monitored automatically, and the results reviewed by technical and scientific staff to ensure the authenticity and integrity of any data collection. Moreover, a software tool is executed in the background to validate the metadata included in the resulting NetCDF files, as well as the metadata used during the processing. When an error is found, it is properly registered and notified. After the evaluation, the data asset is reprocessed to maintain the quality requirements predefined.

The processing applications that create the NetCDF files during ingestion ensure that all the metadata fields are set.

6.3.   Monitoring, review and feedback

This is an overview of processes in SOCIB's organisation which contribute to Preservation Planning, because they monitor community, technology, legal or strategic developments or risks.

Nr.	Process	Frequency	Responsible
1	Monitor SOCIB's designated communities for developments that may affect the repository, such as changes in the technology or the file formats that communities use. This is done in substantial – not always plannable – contacts with the communities, applied research projects, membership of European Research Infrastructures and training & consultancy. Furthermore, SOCIB observation and modelling facilities and, especially, their scientific staff are aware of the state-of-the-art in operational oceanography, and	Once a year (in preparation for yearly planning)	Data Center + observing and modelling facilities

	provide feedback to SOCIB Data Center in order to improve the repository.		
2	Check whether all the SOCIB Data repository's preferred file formats should still be preferred and whether the list is complete (given mission and scope of SOCIB). If not: Analyse alternative formats and select a new preferred format; Migrate all relevant files from the no longer preferred format to the successor format. Update the relevant internal & external documents	Once a year (in preparation for yearly planning)	Data Steward + heads of facilities
3	The SOCIB systems are monitored. The monitoring is done by the Computing & IT service, and the Data Center. When a malfunction is noticed the corresponding action will be executed.	Continuously	Head of C&IT service + head of Data Center
4	Monitor potential external threats to the IT network. External network access is controlled, at first level, by the University of the Balearic Islands (UIB) IT and Network Department, and a second level, by SOCIB C&IT Service	Continuously	Head of C&IT + UIB IT and Network Department

5	Revise this Preservation Plan: still up to date or is there reason to change (either of) it? Are there any unintended consequences of revision that must be taken care of?	Biannually	Head of Data Center
6	Update the SOCIB Strategic Plan, including the services, strategic goals and designated communities	Every four years	Director of SOCIB

7. IT Architecture

The preservation of SOCIB's collections relies on an IT infrastructure that is fit for purpose and is continually monitored and periodically reviewed to ensure timely upgrades in both hardware and software.

In order to ensure resilience and provide an adequate level of redundancy, the preservation system consists of on-site, near-site and off-site storage. For the same reasons, mirror versions of on-site systems are provided.

Adequate storage capacity for all holdings is maintained.

SOCIB provides necessary secure networking and communications equipment, providing adequate connectivity, the ability to restrict access to valid Mac addresses and a facility to segment the network for switched separated firewall connectivity.

All servers in SOCIB are protected by power surge protection systems.

Disaster recovery procedures are in place.

8. Security

Data holdings are stored in two different Data Centers, separated by more than 10 kilometers; the main Data Center is located at the ParcBit IT Campus (Palma, Mallorca) and the secondary Data Center at IMEDEA (Esporles, Mallorca). Access to both campuses is controlled by gatekeepers and security services.

These two Data Centers are secured areas with access limited to authorized personnel (Computing & IT Service staff). Access to these areas is only possible by keys that are kept in a secure and safe place, only accessible to IT staff. Occasionally accesses of external personnel is only permitted under supervision of one of the members of the Computing & IT Service.

Both facilities are equipped with security and environmental monitoring systems over the network. A camera system allows video surveillance and monitoring to record human activity, while integrated sensors monitor variables such as temperature, humidity or air flow. These active network monitoring systems protect data holdings from security or environmental threats, providing an automatic alert notification system to ensure immediate detection and enabling rapid response. In addition, SOCIB Data Center is equipped with an automatic fire detection and suppression system, specifically designed to operate within data centers facilities.

Access to the internal network (LAN) is only granted to SOCIB personnel or to authorized guest users, always under the supervision of SOCIB staff. Access to IT resources is granted through a user-password authorization policy, mainly based on an LDAP directory service.

Both facilities provide secured wireless networks (WPA2), protected by password and isolated from the wired local network. SOCIB personnel and guest users access segregated networks (with different identifiers SSIDs), to control their access to network resources.

When one member leaves the organization the user account is immediately disabled. During the following month, the former member maintains access to their personal data; after this time, that data is erased. The work related content is kept in a proper location under the organization storage resources.

External network access is controlled, at first level, by the University of the Balearic Islands (UIB) IT and Network Department, and a second level, by SOCIB C&IT Service. Most of the data are open data, accessible to the general public, but for special purposes some network access control policies are applied to ensure private access to protected resources. Access control is provided by different mechanisms such as hardware firewalls (under UIB supervision), software firewalls or intrusion prevention software (prevent DDoS attacks). All network access is monitored and accesses are logged and monitored; any suspicious requests are blacklisted and access prohibited.

Access to some of the services and applications are restricted only to authenticated users. Typically the authorization part relies on the LDAP service described above. In some circumstances, external users with granted access to specific restricted resources are managed by means of a hidden (access protected within the organization) configuration file or database record containing their credentials. The later method will be overridden when

the new SOCIB corporate website is deployed (early next year), since it will contain a new Authentication and Authorization system.

All IT equipment connected to the SOCIB network is fully protected with complete, updated and trustable software (antivirus, firewall, anti-malware software, ...). E-mail service is protected with spam filters, antivirus software, phishing protection and management of authorized devices.

SOCIB personnel must agree on an Information Technology contract clause in order to ensure good practices for the user of IT infrastructure.

9. Funding and Resource Planning

SOCIB is a **public consortium with indefinite duration** and with **structural funds**, that can be expressed in terms of 35 FTE numbers. Total annual funding for SOCIB operations is up to 2 million Euros. Therefore, the repository has sufficient funding for staff resources, IT resources, and a budget for attending meetings when necessary, for the next 3-5 years.

Additionally, SOCIB also has several [partnership agreements](#) in international, national or regional research projects, and accordingly, some **additional project based funding** also exists.

SOCIB ensures continuity of access and preservation for the data repository at present and in the future. The Data Center Facility and the Computing and IT Service constantly improve their services to meet the requirements of long-term access and availability of data in the repository. The latest developments and technological progress to stay informed of the best practices for long-term preservation are followed.

The funding for the two departments in charge of the repository is sufficient to maintain core operations and activities (data archiving and dissemination, information service).

In the case of a potential risk, a remote backup stored in the secondary Data Center, as mentioned on chapter 8 (security) of this document, eventually will provide continuity of access to the data.

In the unlikely case of a SOCIB closing and according to Spanish regulation, all information and scientific data will be transferred to the most appropriate partner institution as well as any economic obligations (e.g. [DIGITAL.CSIC](#) is the institutional repository of the Spanish National Research Council, CSIC).