



ENVRI
FAIR

D4.7

Policies for common service catalogue, policy landscape in EOSC domain

Work Package	WP4
Lead partner	UKRI
Status	Final
Deliverable type	Report
Dissemination level	Public
Due date	31 March 2023
Submission date	30 June 2023

Deliverable abstract

This document presents the policies planned for the ENVRI-Hub service catalogue within the context of interoperation with EOSC and the FAIR principles. The ENVRI-Hub catalogue is supplied by the Research Infrastructures within ENVRI-FAIR (or more specifically their digital asset suppliers) and so it is necessary for the policies of the RIs to be sufficiently compatible to avoid problems of conflicting policies when accessing digital assets at the RIs from the ENVRI-Hub. The key policy drivers (EOSC Rules of participation, FAIR principles, and ENVRI-Hub initial documents) were documented in D4.6 where policy recommendations for the RIs were made, in order for their policies to be compatible with ENVRI-Hub and hence EOSC and FAIR. The next steps to create policies for the ENVRI-Hub were also documented in D4.6 following ENVRI-FAIR Policy workshop 4 where the approach was discussed. While ENVRI RIs are finalising their policies and their implementation through guidelines (best practice) and IT implementation (technology) this deliverable lays out the policies needed at ENVRI-Hub and the steps to realisation.



DELIVERY SLIP

	Name	Partner Organization	Date
Main Author	Keith Jeffery	UKRI	16 May 2023
Contributing Authors	Helen Glaves Mairi Best	UKRI FZJ	16 May 2023
Reviewer(s)	Helen Glaves	UKRI	26 June 2023
Approver	Andreas Petzold	FZJ	30 June 2023

DELIVERY LOG

Issue	Date	Comment	Author
V 0.1	20 December 2021	First draft for internal circulation	Ari Asmi
V 2	17 February 2023	Improved version	Keith Jeffery
V 3	28 March 2023	Final version	Keith Jeffery
V 4	16 May 2023	Finalised version after internal review	Keith Jeffery
V 5	26 June 2023	Additional input from Mairi Best on landscape survey	Mairi Best
V 6	27 June 2023	Final version	Keith Jeffery

DOCUMENT AMENDMENT PROCEDURE

Amendments, comments and suggestions should be sent to the Project Manager at manager@envri-fair.eu.

GLOSSARY

A relevant project glossary is included in Appendix A. The latest version of the master list of the glossary is available at <http://doi.org/10.5281/zenodo.4471374>.

PROJECT SUMMARY

ENVRI-FAIR is the connection of the ESFRI Cluster of Environmental Research Infrastructures (ENVRI) to the European Open Science Cloud (EOSC). Participating research infrastructures (RI) of the environmental domain cover the subdomains Atmosphere, Marine, Solid Earth and Biodiversity / Ecosystems and thus the Earth system in its full complexity.

The overarching goal is that at the end of the proposed project, all participating RIs have built a set of FAIR data services which enhances the efficiency and productivity of researchers, supports innovation, enables data- and knowledge-based decisions, and connects the ENVRI Cluster to the EOSC.

This goal is reached by: (1) well defined community policies and standards on all steps of the data life cycle, aligned with the wider European policies, as well as with international developments; (2) each participating RI will have sustainable, transparent, and auditable data services, for each step of data life cycle, compliant to the FAIR principles. (3) the focus of the proposed work is put on the implementation of prototypes for testing pre-production services at each RI; the catalogue of prepared services is defined for each RI independently, depending on the maturity of the involved RIs; (4) the complete set of thematic data services and tools provided by the ENVRI cluster is exposed under the EOSC catalogue of services.

TABLE OF CONTENTS

D4.7 - Policies for common service catalogue, policy landscape in EOSC domain.....	4
1 Introduction.....	4
1.1 Rationale	4
1.2 Target audiences.....	4
1.3 How to use this document	4
1.4 Definition and purpose of ENVRI-Hub Policies	5
1.5 A note on timescales	5
2 ENVRI Policy Process	6
3 Policy Framework for ENVRI-Hub	6
3.1 Introduction.....	6
3.2 Policies Required	7
3.3 Guidelines Required.....	8
3.4 IT Implementation.....	8
3.5 Introduction.....	9
3.6 RI control	9
3.7 The Policies.....	9
3.8 Three Key Policies	10
3.9 The Other Policies.....	12
4 The Policy Landscape in ENVRI.....	12
4.1 Introduction.....	12
4.1.1 The 'legal' policies	12
4.1.2 The Other Required Policies.....	14
5 The Way Forward: Next Steps.....	15
5.1 Policies for ENVRI Hub and ENVRI RIs	15
5.2 ENVRI Hub Policy Implementation	15
6 ANNEX 1. EPOS Policy Template.....	16
7 ANNEX 2. An Example EPOS Policy Document	17
8 ANNEX 3. Consolidated EPOS Policy Document	18

D4.7 - Policies for common service catalogue, policy landscape in EOSC domain

1 Introduction

1.1 Rationale

European Open Science Cloud, FAIR principles, and operational project requirements of ENVRI FAIR all require several changes in the data systems of the ENVRI research infrastructures. These demands are not, however, only concentrated on the purely technical aspects, and can require significant changes in the operations and the policies of the participating RIs. Emerging and existing International and National laws provide constraints. As one of the key aspects of these developments is the perceived need for further interoperability, building a common and interoperable platform for these policies would be beneficial.

Throughout the project this issue has been addressed incrementally, actioned through four workshops and documented in deliverables. Sufficient commonality of RI policies is necessary so that they align with those of ENVRI-Hub and specifically the catalogue to which the RIs contribute metadata describing their digital assets. Inconsistent policies may preclude access from ENVRI-Hub to the relevant digital assets. The RIs in ENVRI have or are well on the way to having in place, appropriate policies for themselves. This document presents the first iteration of a policy framework and policies for the ENVRI-Hub consistent with the policies of the RIs providing the metadata describing their digital assets to the catalogue of ENVRI-Hub.

1.2 Target audiences

The main target audiences for this document are (in order):

1. Managers of the ENVRI-Hub who need to have responsibility for the policy framework within which the ENVRI-Hub operates.
2. Technical developers of the ENVRI-Hub who need to ensure the policies are supported/enforced by the software and processes of ENVRI-Hub.
3. Management staff of the ENVRI RIs (inc. upcoming infrastructures), particularly staff working between the high-level decision making and practical application level in the research infrastructures. They are approached in their role to develop these Policy decisions, and to create associated practices within their organizations.
4. Strategic leadership of ENVRI RIs, from Directors General (or similar) to their high-level direction groups (General Assemblies at that like, often representatives of Member states). They are approached as they are often responsible to approve the policies and discuss their strategic importance in their organizations.
5. Technical developers within the ENVRI RIs or associated projects, especially in the data systems. They are approached in to gain understanding the relevant policy requirements for their technical choices, and as a way to bring this policy information to user interfaces and metadata of the data products.
6. EOSC Association and other international and regional communities, who are approached as users and stakeholders of these policy suggestions.

The target audiences are focusing on Development (1), Approval (2), Implementation (3), and Alignment (4) of policies. The most important target audiences (1 and 2) – but also the other target audiences – have been approached using ENVRI workshops.

1.3 How to use this document

This document creates a first iteration of the policies (defined in the next chapter), for the ENVRI-Hub. The document can thus be used for:

- RIs to ensure that their policies are congruent with those of ENVRI-Hub and identify any developments needed.

- ENVRI-Hub developers to ensure that the relevant software, especially that related to the catalogue, implements those policies.
- EOSC related entities to understand the organisational changes needed in the RIs relating to the requirements from EOSC.

There are several reasons why we would also suggest caution. Due to the draft state and continuously developing EOSC landscape, the policies may need revision. In fact, the topic of policies is usually regarded as live with evolving policy documents and associated guidelines and IT implementation. Similarly, policies at RIs may need revision due to changing local legislation or the shifting objectives of the RI organisation.

1.4 Definition and purpose of ENVRI-Hub Policies

Purposes of these policies:

- **Internal use:** *to direct the organization's internal procedures and development, give motivation and guidance on needed actions (behaviours) and to justify internally processes. Here the targets are people directly working in the research infrastructures or via an agreement. This can be considered as (co)development use of policies.*
- **External stakeholder use;** *to show compliance and strategic goals to external stakeholders (funding bodies, member organizations, certification authorities etc.). This also includes compliance with EOSC Rules of Participation, and (optionally) CoreTrustSeal or other authorities or organizations as well as international or national laws. In this context, a key stakeholder group for many ESFRIs (RIs included in the ESFRI roadmap) are national funding bodies, which have their own requirements for FAIR data production and other issues related to open science, and having public policy decisions on this subject can be a good way to show that these requirements are taken into account in the infrastructure operations. This can be considered an *upstream use* of policies.*
- **Informing External clients(users):** *to demonstrate accessibility and interoperability to user communities (e.g., domain and data scientists, service developers, Virtual Research Environments, external data searches, companies, etc.). This use of policies is important particularly in relation to Users and Access but can be crucial for many other policies as well. A key aspect is to communicate to these communities via policy documents or metadata, what are the limitations and organizational decisions related to their use of infrastructure policies. This can be considered to be a *downstream use* of policies.*

The ENVRI policy framework is built on data interoperability (commonly via services offered) and most of the policies studied are thus connected directly or indirectly to organizational aspects related to them. The results are intended to be generally applicable, and some level of abstractness is unavoidable. Thus, challenges emerge from trying to generalize policies, and to make them separable from the details specific to the organization of which they are part. To alleviate this issue, there is a need to model and define both the policy decisions and individual ENVRI RI organizations in an abstract way.

For this reason, the ENVRI cluster of organisations needs to have policies to enable their objectives to be met. RI organizations within ENVRI need to have their own policies, and a major objective of WP4 of ENVRI-FAIR has been to reconcile any differences. This then permits the creation of common policies (with guidelines and IT implementation) for the ENVRI-Hub.

1.5 A note on timescales

The whole policy process in ENVRI-FAIR has been delayed. This is partly due to the reorganisation of the WP4 leadership team and associated reallocation of resources to continue this work. The COVID-19 pandemic precluded face to face meetings which are of great benefit to policy development and can only be substituted partially by online meetings. The other contributing factor has been the changing policy landscape, with more legislation and evolving policy drivers from organisations with which ENVRI needs to interoperate. In addition, policy issues are not of great interest to those concerned with technical (IT) interoperability and so the policy work in the RIs of ENVRI has generally not been a high priority.

2 ENVRI Policy Process

The ENVRI policy process has already been described in D4.6, and supported by landscape surveys D4.2, D4.5, and constrained by the external factors in D4.4. Essentially this process has consisted of the following steps (Figure 1):

1. Define the policy drivers: in the case of ENVRI these are largely coming from EOSC, FAIR and the ENVRI-Hub
2. Document the requirements from those drivers as policy statements (related to the drivers e.g., EOSC)
3. Transform policy statements into defined policies (related to activities necessary for ENVRI to operate e.g., security, curation)
4. Re-interpret the policy statements as guidelines (desk instructions on what to do)
5. Implement the guidelines as technical IT (e.g., authorisation of access)

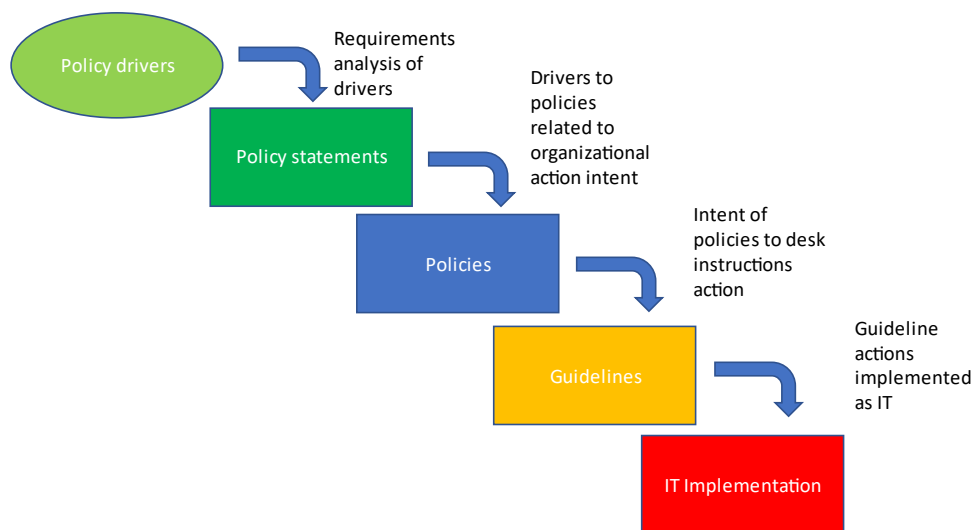


Figure 1: ENVRI Policy Process

3 Policy Framework for ENVRI-Hub

3.1 Introduction

As discussed at the workshops held during the ENVRI-FAIR project, and documented in D4.6, the policy framework for ENVRI needs to be seen in a wider context (Figure 2) where the ENVRI-Hub sits in the middle of a very large field of policies consisting of (a) legislation; (b) policies of organisations cooperating with individual RIs; (c) policies of individual ENVRI RIs; (d) a context of organisations (bottom row of diagram) with their own policies and constraints which affect the ENVRI-Hub (and hence to some extent RIs in ENVRI). All these areas of policy affect the policies appropriate for, and achievable with, the ENVRI-Hub.

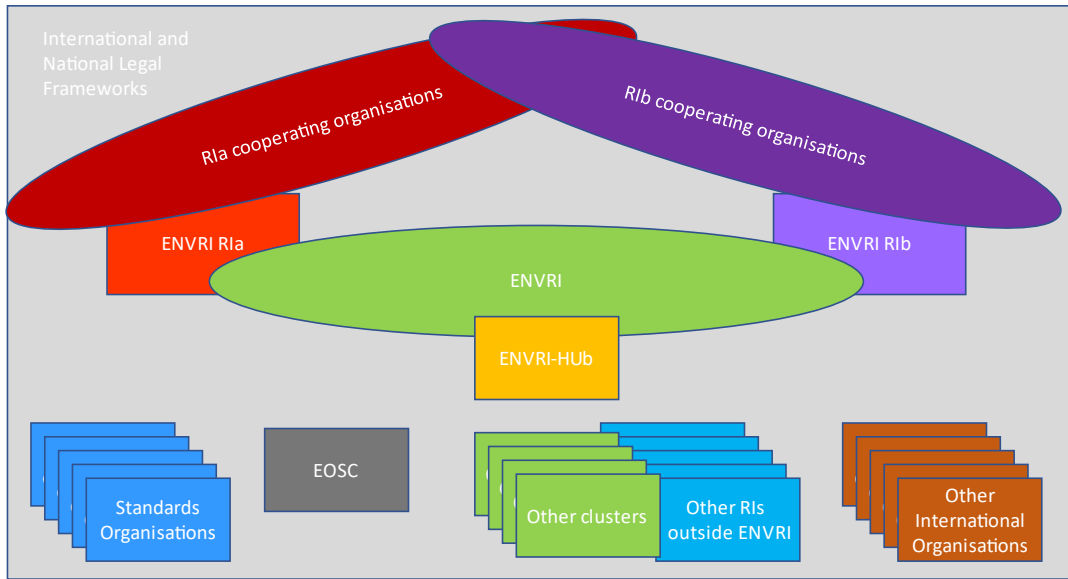


Figure 2 The Wider Context of ENVRI Policy

For interoperation, it is necessary for the RI specific policies within ENVRI and at ENVRI-Hub to be compatible (and also compatible with the policies of external stakeholders such as EOSC). The list generated and agreed at Workshop 4 is given in Table 1.

Table 1: Policy Interoperation - Measures in policies to achieve interoperation in ENVRI-FAIR: ENVRI-Hub / RI –RI / interface to EOSC

Measure	Justification	Remark
Terms and Conditions	T&C: Liability, respect terms	All Require SUFFICIENT conformity for interoperation
Cookies	For certain functions (maintaining state) and collecting usage data	
Privacy	GDPR conformance	
Authentication	Valid user	
Authorisation	Valid user	
Metadata (FAIR) Curation Provenance	discovery, contextualization, workflow orchestration including curation and provenance	
Licensing Acknowledgement Citation	usage conditions, attribution/citation/acknowledgement	

3.2 Policies Required

The policies in scope and out of scope for ENVRI RIs (and hence ENVRI-Hub) were documented in the annexes of deliverable D4.6. Following the four workshops and the deliverables reporting on progress, especially D4.6, we find that the policies required for ENVRI-Hub are of three kinds: (a) those for interoperation (Figure 3) including identifiers under FAIR metadata; those for availability (physical security, disaster recovery); (c) those for open science (RRI). The aim has been to develop the minimum set of policies required to meet the specified requirements.

Policies in scope in this context are

- Physical Security
- Disaster Recovery
- Privacy
- Authentication
- Authorisation
- Terms and Conditions

- Cookies
- Metadata
- Identifiers
- Licensing
- Curation
- Provenance
- Quality Assurance
- Acknowledgement
- Responsible Research and Innovation

3.3 Guidelines Required

From the above, the guidelines required can be determined. There is a n:m relationship between policies and guidelines: a guideline may be derived from several policies and one policy may be referenced by several guidelines. The guidelines cover provision of and access to digital assets, managing personal data privacy, ensuring security for availability of digital assets and for protection of personal data and ensuring open science through Responsible Research and Innovation (RRI).

Guidelines for provision

- Asset Provision Data,
- Asset Provision Services,
- Asset Provision Software,
- Asset Provision Documentation
- Asset Provision Publication

Guidelines for access to digital assets

- Asset Access Data
- Asset Access Services
- Asset Access Software
- Asset Access Documentation
- Asset Access Publication

Guideline for Personal Data Privacy

Guidelines for security for availability of digital assets and for protection of personal data

- Security: Physical Security
- Security: Disaster Recovery
- Security: Authentication
- Security: Authorisation

Guideline ensuring open science through RRI

3.4 IT Implementation

The proposed model for IT Implementation (based on the EPOS-ERIC approach) is illustrated in Figure 3 where the red ellipse indicates the scope of the IT support for policies and guidelines:

How it all links together (EPOS example)

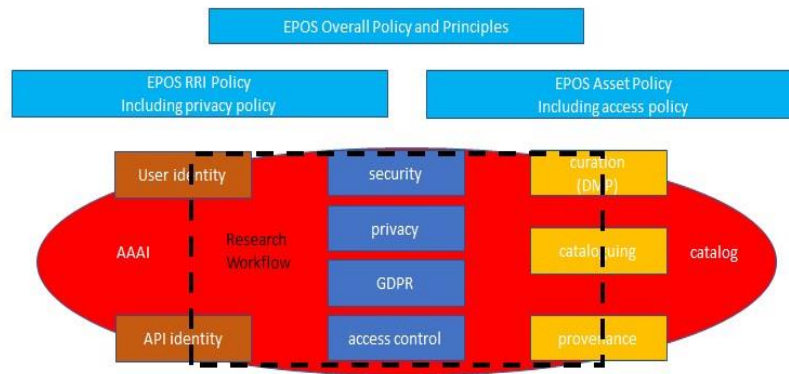


Figure 3: IT Implementation

3.5 Introduction

In parallel with assisting RIs to share best practice and develop policies, guidelines and IT implementations, it is necessary also to have a similar policy environment for ENVRI-Hub. The catalogue of ENVRI-Hub contains rich, graph-structured metadata records describing digital assets of the RIs in such a way as to make them discoverable, contextualizable, accessible, interoperable and reusable. Different RIs can supply metadata records of varying levels of richness, but the principle is that RIs expose metadata records for the assets being made available to the ENVRI community (and wider), including their conditions of use that reflect the RI-specific policies. The aim is to maximise compatibility between the policies of the ENVRI-Hub and those of the ENVRI RIs (and their asset suppliers) to reduce friction and increase interoperability.

3.6 RI control

In parallel with assisting RIs to share best practice and develop policies, guidelines and IT implementations, it is necessary also to have a similar policy environment for ENVRI-Hub. The catalogue of ENVRI-Hub contains rich, graph-structured metadata records describing digital assets of the RIs in such a way as to make them discoverable, contextualizable, accessible, interoperable and reusable. Different RIs can supply metadata records of varying levels of richness, but the principle is that RIs expose metadata records for the assets being made available to the ENVRI community (and wider), including their conditions of use that reflect the RI-specific policies. The aim is to maximise compatibility between the policies of the ENVRI-Hub and those of the ENVRI RIs (and their asset suppliers) to reduce friction and increase interoperability.

3.7 The Policies

The proposed policies for the ENVRI-Hub catalogue are in the following list.

- Most policies concerned with (a) the rights and responsibilities of humans, (b) the rights and protection of digital assets and (c) the interaction between (a) and (b).
- The purposes of the catalogue related to policies
 - a) Curation: availability of digital assets and FAIR
 - b) Security: protection of digital assets
 - c) Privacy of personal data
 - d) Authorisation of access (for protection of digital assets and recording of provenance, citation and usage)
 - e) Licensing: protection of digital assets, name of license and authorisation parameters

- f) Provenance: tracking of asset evaluation and use for privacy
- g) Citation: tracking for accreditation of researcher
- h) Usage tracking: for statistics indicating popularity and usage of personal data

The catalogue

- a) Metadata: representation of policy elements: syntax and semantics, integrity
- b) API
- c) GUI / query interface

How well does the catalogue support policy?

- a) Sufficient information in the metadata, consistency
- b) Sufficient processes/procedure (IT implementation) utilising the metadata to support/enforce policy as defined in guidelines.

The catalogue provides a mechanism for technical interoperability.

However, we also need interoperability of IT implementations based on conforming policies and guidelines.

3.8 Three Key Policies


Three key policies are regarded as essential and critical for ENVRI-Hub in order to protect the organisation and ensure compliance with applicable laws and directives. These are:

1. Privacy
2. Terms and Conditions
3. Cookies


EPOS is used as an example for the ENVRI-Hub developers to follow. The key to implementation is to obtain user consent. This requires appropriate buttons for the user to click alongside a brief explanation and the link to the corresponding policy document. The consent form used in EPOS is illustrated Figure 4.

EPOS POLICIES

I consent to Terms and Conditions

Here you will find the conditions under which you use the EPOS ICS-C portal. This includes acceptable use and liability disclaimer. If you do not consent to such use of the portal, further access to the portal is denied. 

I understand and acknowledge the Privacy Policy document

The Privacy policy explains how EPOS-ERIC manages and protects personal data, particularly in the sense of GDPR (General Data Protection Regulation). If you do not consent to such use of your personal data, further access to the portal is denied. 

COOKIES


Websites utilise cookies to store certain information. EPOS-ERIC ICS-C portal uses cookies only to monitor performance anonymously, information used in improving the portal. You may choose to allow these cookies or not. Either choice does not prevent use of the portal. 

Figure 4: User Consent pop-up Form

The policy documents indicated by the document symbol anchors in the consent pop-up form above are available at:

https://www.epos-eu.org/sites/default/files/Privacy_Policy.pdf

https://www.epos-eu.org/sites/default/files/Terms_and_Conditions.pdf

https://www.epos-eu.org/sites/default/files/Cookie_Policy.pdf

The essential content of each of the three policies is illustrated in the following Figure 5, Figure 6 and Figure 7 using as examples the current content of the EPOS policies.

Privacy (relates to GDPR)

<https://www.epos-eu.org/epos-eric-privacy-policy>

Information about us and this policy

Information we may collect about you

Your legal rights

Glossary

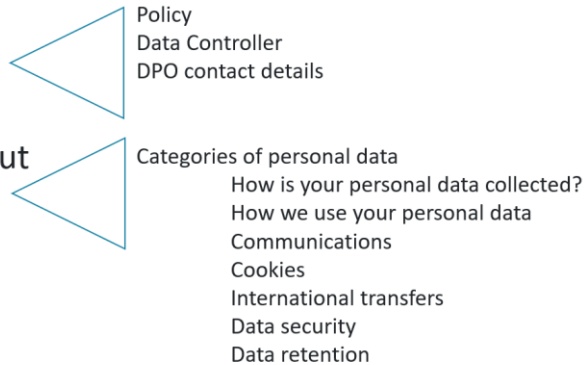


Figure 5: Privacy Policy Essentials

Terms and Conditions

https://www.epos-eu.org/sites/default/files/Terms_and_Conditions.pdf

Your responsibility

By using our Portal, you accept these terms.
You must keep your account details safe

We may change the Portal

We may make changes to these terms
We may make changes to our Portal
We may suspend or withdraw our Portal
We may transfer this agreement to someone else

Use of material on Portal

How you may use material on our Portal...
Permitted uses
Do not rely on information on our Portal
We are not responsible for Portals we link to
Rules about linking to our Portal.

Breach of these Terms

Which country's laws apply to any disputes

EPOS ICS-C Terms and Conditions If you disagree with any part of these terms and conditions, please do not use our website.

By accepting these Terms and Conditions, you enter into an agreement with EPOS ERIC, an international organisation with registered offices at EPOS ERIC, in Via di Vigna Murata 605 - 00143 Rome Italy - FISCAL CODE 96409510581 - VAT N° IT15152381008 ("EPOS ERIC "), made up by the contents of these Terms, in order to regulate the user's access and use of the Portal.

Figure 6: Example of Terms and Conditions Essentials from the EPOS portal

Cookies

https://www.epos-eu.org/sites/default/files/Cookie_Policy.pdf

- 👉 What are cookies?
- 👉 Why we use cookies?
- 👉 Are all cookies the same?
- 👉 How to manage cookies using our website To give you the best experience on the cookie management side, we classify cookies

Figure 7: Example of Cookies Essentials from the EPOS portal

Appropriate policies and pop-up forms, based on the EPOS example, are being created for the ENVRI-Hub by the ENVRI development team. These will be implemented before the end of the ENVRI-FAIR project.

3.9 The Other Policies

The other policies for ENVRI-Hub are currently being developed (May 2023). It has been suggested that the policy template used in EPOS (ANNEX 1. EPOS Policy Template) should be used by the ENVRI-Hub developers for each separate policy, which will produce appropriate policies such as the example in ANNEX 2. The policies can then be combined together into a consolidated document that is referenceable from the ENVRI-Hub, as has been done in EPOS (ANNEX 3. Consolidated EPOS Policy Document).

4 The Policy Landscape in ENVRI

4.1 Introduction

Policy landscape surveys were conducted early in the project and documented in deliverable D4.2, and also later in the project leading to D4.5. These surveys demonstrate considerable progress in policy development and implementation in the individual RIs of ENVRI (necessary for provision of metadata describing assets to the ENVRI-Hub catalogue) and in the development of the ENVRI Hub. The overall status of the landscape is reported in detail in D4.5, but the two tables below provide a summary as of June 2023.

4.1.1 The 'legal' policies

The state of data policy implementation, concerning the three major 'legal' policies – terms and conditions/liability, cookies, and privacy (especially personal data privacy), is shown in Table 2: The State of Implementation of 'legal' policies. Colours indicate state of policy element: green=yes, yellow=in progress/partial, red=no. "No"(red) is not always a lack of addressing the policy, sometimes it reflects a different decision by the RI; "in progress/partial" (yellow) is usually a function of the state of development of the RI overall. This figure is designed to be viewed primarily as a heatmap, with a focus on the colour shading of the cells; text in the cells is simply the URLs of the relevant policy, and details of this data are available in D4.3. Note that almost all RI's have adopted full "legal" data policies, including terms and conditions/liability, cookies, and privacy policies, and have implemented pop-up consent forms (predominance of green).

Table 2: The State of Implementation of 'legal' policies

Research Infrastructure	AGOS	ACTRIS	ICOS	EISCAT	SIOS	eLTER	LifeWatch	DiSSCo	AnaEE	EPOS	DANUBIUS	EURO ARGO	EMSO
Data Policy	https://www.iagos.org/data-policy/	https://intranet.actris.eu/index.php/s/NvtzH7PBGo	https://www.icos-cp.eu/data-services/about	https://eiscat.se/scientist/data/	https://www.sios-svalbard.ora/site	Not yet published	https://www.life-watch.italy.eu/en/data-policy-en/	Not yet operational.	https://www.anaee.eu/sites/anaee/files/Media	https://gnss-metadata.eu/Guidelines/EPOS-	not yet implemented	https://argo.ucsd.edu/organization/	http://data.emso.eu/
Terms and Conditions	https://www.iagos.org/data-policy/	https://www.actris.eu/ppgm-privacv-policv-	https://www.icos-cp.eu/data-services/about	https://eiscat.se/scientist/data/	https://www.sios-svalbard.ora/site	https://deims.org/terms	for DAR and	https://www.life-watch.eu/terms-and-conditions/	https://www.anaee.eu/legal-notice	https://www.epos-eu.org/sites/default/files/2019-08/epos-privacy-policy.pdf	not yet implemented	Terms and Conditions being revised.	https://emso.eu/wp-content/uploads/2019/08/EMSO-privacy-policy.pdf
Liability	https://www.iagos.org/imprint/	https://www.actris.eu/ppgm-privacv-policv-	https://www.icos-cp.eu/data-services/about	https://eiscat.se/about/?highlight=liability	https://www.sios-svalbard.ora/site	https://deims.org/terms	and acceptable-use-	https://www.life-watch.eu/acceptable-use-policy-2021/	https://www.anaee.eu/legal-notice	https://www.epos-eu.org/sites/default/files/2019-08/epos-privacy-policy.pdf	not yet implemented	Terms and Conditions being revised.	http://emso.eu/privacy-policy/
Cookies	https://www.iagos.org/data-privacv/	https://www.actris.eu/ppgm-privacv-policv-	https://www.icos-cp.eu/privacy	https://eiscat.se/about/gdpr-general-data-privacy	https://www.sios-svalbard.ora/SIO	https://elteri.eu/privacy-policy	https://www.life-watch.eu/privacv-policy-2021/	https://www.dissco.eu/privacy-statement	https://www.anaee.eu/legal-notice	https://www.epos-eu.org/sites/default/files/2019-08/epos-privacy-policy.pdf	not yet implemented	Terms and Conditions being revised.	https://emso.eu/privacy-and-data-protection/
Privacy	https://www.iagos.org/data-privacv/	https://www.actris.eu/ppgm-privacv-policv-	https://www.icos-cp.eu/privacy	https://eiscat.se/about/gdpr-general-data-privacy	https://www.sios-svalbard.ora/SIO	https://elteri.eu/privacy-policy	https://www.life-watch.eu/privacv-policy-2021/	https://www.dissco.eu/privacy-statement	https://www.anaee.eu/legal-notice	https://www.epos-eu.org/sites/default/files/2019-08/epos-privacy-policy.pdf	not yet implemented	Terms and Conditions being revised.	https://emso.eu/privacy-and-data-protection/
Pop-up notifications	no	yes	yes	general-data-privacy only, for others - written statement with a	yes	yes, for DEIMS	no	no	Yes for AnaEE websites updated 2022-	Yes e.g. https://www.ics-c.epos-	not yet implemented	There is no identification or tracking of	yes

not yet accepted

4.1.2 The Other Required Policies

The initial response (2020) and current (2023) RI status of the other required policies for interoperability are shown in Table 3. Questions used in the preliminary policy landscape analysis (D4.2) were rearranged by policy category: Licensing, Authorisation, Metadata (FAIR), Provenance/Citation/Acknowledgement and Curation (see discussion above). This table is designed to be viewed primarily as a heatmap, with a focus on the colour shading of the cells indicating the evolution of responses to the questions: green=yes, yellow=in progress/partial, red=no. Details of this data and analysis are available in D4.5.

Table 3 demonstrates that, while many RI's were well advanced in a number of items at the beginning of the project (predominance of yellow and green), significant progress has been made during the project (shift from yellow to green for a number of RIs). Note, "no" (red) is not necessarily a lack of the policy, but sometimes a different decision by the RI in the context of the question; "in progress/partial" (yellow) is usually a function of the state of development of the RI overall. It should be noted that while most RI's have reached a relatively mature stage of policy development, not all policies are necessarily aligned with each other or with the ENVRI Hub. This is currently being addressed (June 2023).

Table 3: Heatmap showing state of Other Required Policies for Interoperability

Research Infrastructure	IAGOS	ACTRIS	ICOS	EISCAT	SIOS	eLTER	LifeWatch	DISSCo	AnaEE	EPOS	DANUBIUS	EURO ARGO	EMSO
2020 Questions	2020	2020	2020	2020	2020	2020	2020	2020	2020	2020	2020	2020	2020
Licensing	2023	2023	2023	2023	2023	2023	2023	2023	2023	2023	2023	2023	2023
1. licence policy? which?	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
1.2. metadata same? which?	Red	Green	Green	Red	Green	Green	Green	Green	Green	Green	Green	Green	Green
1.1. machine readable?	Yellow	Green	Green	Red	Green	Green	Green	Green	Green	Green	Green	Green	Green
7. data ownership and licencing?	Green	Green	Green	Green	Green	Red	Yellow	Yellow	Yellow	Green	Green	Green	Green
Authorisation	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
6. data access?	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Metadata (FAIR)	Yellow	Yellow	Yellow	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Green	Green
4. metadata? exceptions?	Yellow	Yellow	Yellow	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Green	Green
4.1 metadata standard(s)?	Yellow	Yellow	Yellow	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Green	Green
4.3 quality control of metadata?	Red	Green	Green	Red	Green	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Green	Green
4.4 shared/openly accessible?	Green	Yellow	Green	Yellow	Yellow	Green	Green	Yellow	Yellow	Green	Yellow	Green	Green
Provenance/Citation/Acknowledgement	Yellow	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Green	Green
2. dataset definition?	Yellow	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Green	Green
2.1. data versioning?	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
4.5. authorship?	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
3. persistent identifiers?	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Curation	Red	Yellow	Green	Red	Green	Red	Red	Yellow	Yellow	Green	Yellow	Green	Green
8. service level agreement?	Red	Yellow	Green	Red	Green	Red	Red	Yellow	Yellow	Green	Yellow	Green	Green
9. data and metadata consistently available?	Red	Yellow	Green	Red	Green	Red	Red	Yellow	Yellow	Green	Yellow	Green	Green
5. retention?	Red	Yellow	Green	Red	Green	Red	Red	Yellow	Yellow	Green	Yellow	Green	Green

5 The Way Forward: Next Steps

5.1 Policies for ENVRI Hub and ENVRI RIs

The requirement for moving forward with compatibility between the policies of the RIs, the asset suppliers in ENVRI, and the ENVRI-Hub was explained in D4.6.

As outlined above, there has been an increased awareness and understanding of the importance and implementation of policies within the ENVRI community throughout the ENVRI-FAIR project, which has been partly driven by the four Policy workshops. There is now general agreement on the need for policies including those that are required. In addition, there is recognition of the need for compatibility (as far as possible) between policies of the RIs in the ENVRI community and the ENVRI Hub.

The differences recorded between the landscape surveys (D4.2 and D4.5) illustrate this progress. However, managing policies must also consider the likely evolution of relevant legislation and organisational objectives.

5.2 ENVRI Hub Policy Implementation

Workshop 4 specifically discussed the appropriate policies for the ENVRI-Hub and how they could be implemented. It is agreed that, before the end of the project, the ENVRI-Hub will have the three key policies in place. The implementation of the other policies is ultimately a decision for the ENVRI-Hub development team, but the EPOS examples have been provided to indicate a potential mechanism for rapid implementation of policies with an appropriate level of support.

6 ANNEX 1. EPOS Policy Template

1. Why? Do we have a policy and what does it cover
2. Who? – target
3. Who? – Authors
4. When? Is the policy applicable (version, dates)
5. Where? Is the policy applicable (countries, regions)
6. What?... Is the policy
7. How? Is the policy implemented (i.e., relates to which guidelines)

not yet accepted by EC

7 ANNEX 2. An Example EPOS Policy Document

Why? Do we have a policy and what does it cover

A metadata policy is needed to align with the FAIR principles: metadata provide the information to utilise digital assets.

Who? – target

All users of EPOS who provide (asset suppliers) or utilise (users) EPOS assets.

Who? – Authors

Keith Jeffery

When? Is the policy applicable (version, dates)

Version 2: 20220112

Where? Is the policy applicable (countries, regions)

The metadata policy is applicable in all countries of the world.

What? Is the policy

The metadata policy is that all providers of EPOS assets (asset suppliers within the TCS and the ICS-C system) must ensure rich metadata describing each digital asset at the appropriate level of granularity. Rich metadata is metadata sufficient for the purpose: discovery, contextualisation (relevance/quality), access (appropriate information to control access including licensing), (re-)use (including any changeable parameters to control the asset). The metadata must be in the current EPOS standard for the metadata catalogue (CERIF) to be recognised as an asset within the EPOS Delivery Framework.

How? Is the policy implemented (i.e. relates to which guidelines)

The metadata policy relates to the asset provision and asset access guidelines. The policies related to these guidelines – and to metadata - are security (including authentication, authorisation, physical security and disaster recovery), privacy, licensing, citation/acknowledgement and curation.

The policy is realised by providing appropriate procedures to assign rich metadata to an asset. It relates also to the pre-existing EPOS Data Policy.

8 ANNEX 3. Consolidated EPOS Policy Document

1. Introduction

The purpose of this policy document is to bring together the separate policies of EPOS for Data and Service providers as well as Users to provide the policy background to ensure that EPOS Data and Services are managed and used in ways that maximise public benefit following FAIR principles (Findability, Accessibility, Interoperability, and Reusability). This policy should be read in conjunction with the [EPOS ERIC Statutes](#) (C 2018/7011) and [EPOS Data Policy](#).

Guidelines are also being produced to provide guidance to users and data/service providers on best practice to comply with the policies.

EPOS's mission is to establish and underpin sustainable and long-term access to solid Earth science data and services integrating diverse European Research Infrastructures under a common federated framework. By improving and facilitating the integration, access, use, and re-use of solid Earth science data, data products, services, and facilities, EPOS aims at transforming the European research landscape, driving discovery, and developing solutions to geo-related challenges facing European society.

2. Policy applicability

These policies apply to digital assets providers as well as users who utilise EPOS digital assets.

3. Policy references

The policies are regularly updated in line with any changes in response to the evolution of the EPOS organisational and strategic assets. Any queries or suggestions relating to this policy should be sent to management@epos-eric.eu.

4. Definitions

Terms and phrases in this policy shall have the meanings ascribed to them below.

Digital assets	means a resource with economic or social value that an individual, corporation, or country owns or controls with the expectation that it will provide a future benefit. Digital assets are reported on a company's balance sheet and are bought or created to increase a firm's value or benefit the firm's operations.
Data and Services	mean data, data products, services and software as well as any other technical services supporting the provision of "Data and Services". Data and services are digital assets.
Data and Service Provider	means the organisation in charge of providing "Data and Services".
Data Supplier	means entities granting rights of redistribution of their DDSS through EPOS by signing a Supplier Letter with Data and Service Providers.
DDSS	Means Data, Data Products, Services and Software.
EPOS	means the European Plate Observing System Research Infrastructure as defined by Statute.
EPOS Data Portal	means the Integrated Core Services Central Hub (ICS-C).
EPOS Delivery Framework	means the EPOS framework where the relationships among the key actors are regulated by specific rules and procedures. It includes the EPOS ERIC legal seat

	(represented by the ECO), the Integrated Core Services (ICS) and Integrated Core Services Central Hub (ICS-C) and the Thematic Core Services (TCS).
GDPR	means the General Data Protection Regulation (EU) 2016/679.
General Assembly	means EPOS ERIC General Assembly.
Metadata	means data describing in digital form EPOS digital assets
Statutes	means the Statutes of EPOS ERIC.
TCS	means EPOS Thematic Core Services
Users	means individual or institution that utilises the EPOS Services to access Data and Data Products and/or Tools and Software. Access includes discovery, download, execution, or any other use.

6. Provenance

The provenance policy aims to ensure the record of the life history of digital assets in the EPOS Delivery Framework. Any operation that is carried out on an digital assets has to be recorded (a) for audit; (b) to provide information upon which an end-user can judge the suitability and quality of the digital assets for their purpose; (c) to encourage re-use and reproducibility.

All providers of EPOS digital assets (digital assets suppliers within the TCS and the ICS-C system) shall ensure the availability of the life history of an digital assets by providing appropriate provenance procedures to track and document the life history of an digital assets. Guidelines associated with the provenance policy are digital assets provision and digital assets access guidelines *[under definition]*.

7. Identifier

The identifiers policy is intended to align with the FAIR principles: persistent unique identifiers allow reference to, and direct access to, digital assets.

All providers of EPOS digital assets (digital assets suppliers within the TCS and the ICS-C system) shall ensure a universally unique, resolvable persistent identifier for each digital assets at the appropriate level of granularity. Furthermore, since digital assets may have more than one (usually role-based) identifier, identifiers should be federated so that the digital assets can be accessed or referenced by any of the identifiers for the appropriate purpose. Wherever possible, existing standards for identifiers should be followed. The policy is realised by providing appropriate procedures to assign a persistent universally unique identifier to an digital assets. It relates also to the [EPOS Data Policy](#).

Guidelines associated with the Identifier policy are digital assets provision and digital assets access guidelines *[under definition]*.

8. Quality assurance

The quality assurance policy is intended to guarantee that all users of EPOS shall be assured of the quality of the data provided. EPOS ERIC and Data and Services Provider are responsible to assess the quality of data, products, services, and software.

Quality control of the data, products, services, and software rests with the Supplier. Service Providers are responsible for checking the quality parameters of the metadata descriptions that provide information for discovery, contextualization, and provenance and traceability. It relates also to the [EPOS Data Policy](#).

EPOS will disseminate good practice and shall provide a mechanism to obtain User feedback on DDSS quality. EPOS will ensure a continuous process of review and assessment to verify that EPOS DDSS provision is operating as envisioned, seeking improvements and preventing/eradicating problems. EPOS will give emphasis monitoring the quality of the

services provided (e.g. response time, number of successful requests). External audit on quality assurance and quality control is also foreseen through an External Scientific Advisory Board.

Guidelines associated with the quality assurance policy are *[under definition]*.

9. Metadata

The metadata policy aims to align with the FAIR principles: metadata provides the information to utilise digital assets.

All providers of EPOS digital assets (digital assets suppliers within the TCS and the ICS-C system) shall ensure rich metadata describing each digital assets at the appropriate level of granularity. Rich metadata is metadata sufficient for the purpose of discovery, contextualization (relevance/quality), access (appropriate information to control access including licensing), and (re-)use (including any changeable parameters to control the digital assets). The metadata must be in the current EPOS standard for the metadata catalogue (CERIF) to be recognized as a digital asset within the EPOS Delivery Framework.

The policy is realised by providing appropriate procedures to assign rich metadata to a digital asset. It relates also to the pre-existing EPOS Data Policy.

Guidelines associated with the metadata policy are digital assets provision and digital assets access guidelines *[under definition]*.

10. Licensing

The EPOS licensing policy will facilitate effective rights/ownership management over redistribution of Data, Data Products, Software and Services (DDSS) acquired/created by EPOS. EPOS shall only redistribute DDSS to which an appropriate licence has been applied/affixed ([EPOS Data Policy](#)). EPOS aims to grant one default licence set for EPOS-managed DDSS, namely the Creative Commons 4.0. licence (CC:BY or CC:BY:NC). In exceptional cases where a licence cannot be applied, the Service Providers shall inform EPOS ERIC and shall indemnify EPOS ERIC from any damage, cost or liability.

EPOS recognises that it is essential that metadata for DDSS are easily and freely accessible at any time, with as few restrictions as possible, to ensure the widest dissemination and publicity for EPOS managed DDSS. In order to achieve this, Digital Asset Suppliers shall affix open licences, preferably Creative Commons 4.0 CC:BY, to their metadata. The licence applied will place obligations on users of the digital asset, such as acknowledgement where appropriate information is provided.

Software will be treated differently to other EPOS managed DDSS and licensed under a software licence in common usage. Software made available as digital assets by Digital Asset Suppliers shall have affixed an appropriate software licence. The licence applied will place obligations on users of the software digital asset such as acknowledgement and possibly constraining software developed from that supplied to utilise the same licence. It is recommended to use GPLv3 for Academic purposes (protecting open use) and Apache2 for business purposes (protection of intellectual property). In the case of the EPOS data portal and associated systems, GPLv3 shall be used unless specific components (e.g., an API) are to be developed in a commercial environment in which case Apache2 shall be used.

11. Security/Authentication

The security/authentication policy aims to define the governance of persons accessing or providing EPOS digital assets within the EPOS Delivery Framework (EDF) and to record their usage of digital assets if/when required. In particular, authentication ensures that a person is who they claim to be. It is part of the security policy, the other parts being authorization, physical security, and disaster recovery.

All users and suppliers of EPOS digital assets shall be authenticated at the appropriate stage of access. EPOS will implement appropriate authentication wherever required either from a

supplier or user perspective. EPOS will use any information about users gained through authentication mechanisms according to the [privacy policy](#).

The policy is implemented by a check of a person's identity with respect to EPOS declared by a responsible person. The implementation requires that mechanisms are in place to allow users to authenticate themselves using EPOS approved Identity Providers (IdPs). (the approved IdPs are listed in the guidelines).

The implementation (guidelines) includes checking that the user is not barred from accessing EPOS due to any legal restrictions.

Guidelines associated with the security/authentication policy are the security guidelines *[under definition]*.

12. Security/Authorisation

The security/authorisation policy aims to define the governance of persons supplying or accessing EPOS digital assets within the EPOS Delivery Framework (EDF). In particular, authorisation defines the digital assets (or digital assets classes) a person may access, in what role (e.g. user, manager), in what modality (**C**reate; **R**ead; **U**ppdate; **D**ele; **E**xecute; **d**ownload) and within what time period. Authorisation balances the rights of the user (such as open access) against the rights associated with the digital assets (such as a licence). A prerequisite is user authentication. It is part of the security policy, the other parts being authentication, physical security and disaster recovery.

All users of EPOS digital assets must be authorised to access digital assets in the appropriate role, modality, time period either explicitly (permissions linked to authenticated identity) or by default (where the digital assets is not so protected). The latter is so-called anonymous use, although the user identity (authentication) and relevant attributes may be utilised for recording usage.

The policy is implemented by a record of a person's rights to access EPOS digital assets in the appropriate role, modality, time period declared by a responsible person.

The implementation requires that, for any EPOS digital assets that requires authorisation a process exists for a defined, authorised person to declare that a given user has a right to access a specific EPOS digital assets in the appropriate role, modality, time period, and that the person (user) is registered at a node of the EPOS delivery framework with appropriate details in the associated Identify Provider (IdP).

Guidelines associated with the security/ authorisation policy are the security guidelines. *[under definition]*.

13. Curation

The curation policy aims to define the lifecycle management of digital assets in the EPOS Delivery Framework.

All providers of EPOS digital assets (digital assets suppliers within the TCS and the ICS-C system) must ensure: a) availability of the digital assets (whether DDSS or metadata) and b) the integrity and availability of the digital assets (subject to security, authentication, authorisation policies). Digital assets quality is dealt with in the quality assurance policy.

The policy is realised by (a) deciding whether a digital assets should be curated or deleted; in the latter case a 'tombstone' metadata record should be available; (b) provision of appropriate backup and replication procedures sufficient to recover digital assets should there be unavailability or corruption due to e.g., a security breach or power failure.

Guidelines associated with the curation policy are digital assets provision and digital assets access guidelines. *[under definition]*.

14. Disaster Recovery

The disaster recovery policy aims to ensure that IT resource investments made by EPOS are protected against service interruptions, including large-scale disasters, by the development, implementation, and testing of disaster recovery plans.

This policy applies to all facilities of EPOS that operate, manage or use IT services or equipment to support mission-critical functions.

IT resource investments made by EPOS shall be protected against service interruptions, including large-scale disasters, by the development, implementation, and testing of disaster recovery plans. In particular, the following actions plans and actions be implemented:

- plans for disaster recovery shall be developed by IT management;
- disaster recovery plans shall be updated at least annually and following any significant changes to the computing or telecommunications environment of EPOS;
- IT staff of EPOS shall be trained to execute the disaster recovery plan;
- annual testing of the disaster recovery plan shall be done;
- an external auditor shall audit disaster recovery plans.

Guidelines associated with the disaster recovery policy are *[under definition]*.

15. Physical security

The Physical Security Policy aims to protect and preserve information, physical digital assets, and human digital assets. Thus, EPOS information, physical digital assets, and human digital assets shall be protected and preserved:

- physical access to the server rooms/areas shall completely be controlled and servers shall be kept in the server racks under lock and key;
- access to the servers shall be restricted only to designated Systems and Operations Personnel;
- besides them, if any other person wants to work on the servers from the development area then he/she shall be able to connect to the servers only through Remote Desktop Connection with a Restricted User Account;
- critical backup media shall be kept in a fireproof off-site location in a vault.

All facilities of EPOS that operate, manage, or use IT services or equipment to support mission critical functions shall:

- establish the rules for granting, control, monitoring, and removal of physical access to office premises;
- identify sensitive areas within the organisation;
- to define and restrict access to the same.

Guidelines associated with the physical security policy are *[under definition]*.

16. Terms and Conditions

The Terms and Conditions aims to govern the contractual relationship between EPOS and its users of the sites <https://www.epos-eu.org> and <https://www.epos-eu.org/dataportal>. The relationships between EPOS ERIC and Data and Service Providers for the purposes of provision are additionally subject to separate agreements.

Full Terms and Conditions are available at: https://www.epos-eu.org/sites/default/files/Terms_and_Conditions.pdf

17. Cookies

The Cookies Policy aims to describe how the site <https://www.epos-eu.org> uses cookies and processes personal data of users who visit it. In compliance with the obligations arising from national and EU legislation (EU Regulation 679/2016) and subsequent amendments, this Site respects and protects the privacy of visitors and Users, making every possible and proportionate effort not to infringe their rights. This cookie policy applies only to the online activities of this Site and is valid for visitors/Users of the Site. It does not apply to information collected through channels other than this Website. The purpose of the policy is to provide

maximum transparency regarding what information the Site collects and how it uses it. EPOS-ERIC ICS-C portal <https://www.epos-eu.org/dataportal> uses cookies only to monitor performance anonymously, information used in improving the portal. You may choose to allow these cookies or not. Either choice does not prevent use of the portal.

Full Cookies policy is available at:

https://www.epos-eu.org/sites/default/files/Cookie_Policy.pdf

18. Privacy

The Privacy Policy aims to give information on how EPOS collects and processes personal data, through the use of the site www.epos-eu.org or when subscribed to EPOS services or otherwise engaged with any of EPOS projects or applying for a position with EPOS. In compliance with the obligations arising from national and EU legislation (EU Regulation 679/2016) and subsequent amendments, this Site respects and protects the privacy of visitors and Users, making every possible and proportionate effort not to infringe their rights.

Full privacy policy is available at: <https://www.epos-eu.org/epos-eric-privacy-policy>

19. Attribution, Acknowledgement, Citation

The Attribution, Acknowledgement, Citation Policy aims to: i. ensure that appropriate Attribution, Acknowledgement, Citation information is included with any data or service provided to a user; ii. support efforts to improve Attribution, Acknowledgement, Citation of original (digital assets) providers/suppliers in scientific publications and during the whole research data life-cycle.

Generally, within global research and academic fields, an acknowledgement is a declaration or avowal of one's own act, often used to acknowledge ownership, supply or provision, thereby giving the DDSS legal validity, and works to prevent the recording of false or fraudulent claims. Creative Commons licences utilising the "BY" element will require acknowledgement to be given to the Supplier. Both acknowledgement and citation rely on attribution: the association of the digital assets with a person or organisation that created (directly or by assembling, curating), and has ownership or delegated stewardship, of the digital assets.

All DDSS supplied by EPOS will be provided by licence. One of the obligations of a licensee will be to acknowledge or cite the source of the digital assets (where known).

Owners, Suppliers or Providers may well be requested by EPOS to provide details of how they wish to be acknowledged, and users will be legally bound to match those requirements. This is usually defined by the licence.

This policy applies to all owners, suppliers, providers and users of EPOS DDSS.

Guidelines associated with the Attribution, Acknowledgement, Citation policy are *[under definition]*