EUROPEAN COMMISSION
DG COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

Directorate C - Enabling and Emerging Technologies
Unit C.1 - High Performance Computing and Applications

EOSC EU Node Resources and Services Onboarding Policy

Version 1.0

RESOURCES AND SERVICES ONBOARDING POLICY

1. Purpose

This Resources and Services Onboarding Policy ("*RSOP*") defines the rules and conditions for onboarding third-party Resources *("Resources"*) and Services *("Services"*) to the EOSC EU Node by their legal owners, as granted by the European Commission, Directorate General for Communications Networks, Content and Technology, Unit C.1 High Performance Computing and Applications (hereinafter referred to as *"Operating Unit"*).

2. Scope

The EOSC EU Node serves as a production infrastructure enabling international and interdisciplinary research by onboarding third-party scientific *Resources* and *Services* that are available on the research market.

It is not a mechanism for commercial providers to step into the market. Commercial providers must comply with applicable EU and national public procurement regulations (Directive 2014/24/EU[1]). This policy ensures that eligible *Resources* and *Services* meet production-quality standards, are maintained and supported, and contribute to the broader European and global research ecosystem.

This policy applies to all third-party legal entities (hereinafter referred to as *"Contributors"* represented by their designated *User* referred as *"Contributor Representative"*) seeking to onboard their eligible *Resources* and *Services* to the EOSC EU Node directly.

Registration of *Contributors* is handled on a first-come-first-served basis by the operators of the EOSC EU Node at best-effort (i.e. not guaranteed). Onboarding of *Resources* and *Services* to the EOSC EU Node is made available to *Contributors* at the sole discretion of the *Operating Unit* and can be revoked at any time. No onboarding services and processes are provided or supported by the EOSC EU Node other than those prescribed in Annex A "*Onboarding processes*" of this policy.

[1] Directive - 2014/24 - EN - EUR-Lex

All other forms of contributions to the EOSC EU Node by the *Users* fall under the scope of the User Access Policy (UAP)[2] and Acceptable Use Policy (AUP)[3].

Enrolment of Nodes into the EOSC Federation is out of the scope of this policy. Third-parties must consult with the latest Node Enrolment Policy (NRP)[4].

3. Eligibility

3.1. Contributors

The following eligibility requirements are mandatory for the *Contributors*:

(a) Legal entity must be established in EU27 Member States or countries associated to Pillar 1 of the Horizon Europe Work Programme (Associated Countries)[5] (subject to change under the subsequent EU Multiannual Financial Framework) or intergovernmental organization of EU interest.

(b) Compliance with the preliminary "*Guidelines on onboarding policies during the EOSC Federation build-up phase*[6]" and alignment with the purpose of the EOSC Federation and its key outcomes outlined in the "*EOSC Federation Handbook*[7]", ensuring adherence to applicable ethical, legal, technical, and security requirements and alignment with EOSC principles, including openness, FAIR data practices, and interoperability.

(c) Provision of added value to the EOSC ecosystem, including support for European level collaboration and international and interdisciplinary research.

(d) Alignment with the EOSC EU Node's commitment to open science and support for multi-disciplinary and cross-border research, beyond a single research domain or national context.

(e) Financial and operational sustainability sufficient to ensure long-term contribution to the EOSC ecosystem.

The satisfaction of these eligibility requirements is evaluated based on:

- The self-declaration of the *Contributor* provided via the EOSC EU Node's Contributors Dashboard by the designated *User* representative. The *Contributor* may be requested to provide an additional signed statement from its legal representative.

- Additional documentation which may be requested from the *Contributor*, including by not limited to, mission statement, legal status and governance, financial statements, open science strategy and activities.

---

[2] https://open-science-cloud.ec.europa.eu/support/user-access-policy
[3] https://open-science-cloud.ec.europa.eu/support/acceptable-use-policy
[4] https://open-science-cloud.ec.europa.eu/support/node-registration-policy
[5] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/list-3rd-country-participation_horizon-euratom_en.pdf
[6] https://zenodo.org/records/18873066
[7] https://zenodo.org/records/18454649

- Publicly available information related to the *Contributor's* activities.

3.2. Services

In the context of this policy *Services* include, inter alia, infrastructure services, execution environments, research support services (including associated research products), scientific application services, and virtual research environments.

The onboarding processes for *Services* are described in Annex A "*Onboarding Processes*".

The following eligibility requirements are defined for *Services*:

(a) The scope of the *Service* must be multi-country and multi-disciplinary, providing added value to the EOSC ecosystem by supporting both international and interdisciplinary research.

- A *Service* with a narrower scope must pursue onboarding in an appropriate (i.e. thematic, national, other) Node of the EOSC Federation; should this not be possible, the *Service* may be considered eligible for onboarding to the EOSC EU Node.
- The *Service* may already be onboarded to other Node(s) of the EOSC Federation, subject to their onboarding policies, it is not the reason for exclusion (e.g., service features and/or integration options may differ).
- If the *Service* has got associated research products/outcomes stored internally, those will not be onboarded to the EOSC EU Node. For onboarding of *Resources* see Clause 3.3.

(b) The *Contributor* of the *Service* must assume full ownership, responsibility, and accountability of the *Service* vis-à-vis the EOSC EU Node for all matters related to this policy and regardless of the stakeholders, governance, agreements, technologies, and provision models involved.

- There must be an established and enforced "Access Policy" of the *Service* transparently available in compliance with the AUP and UAP of the EOSC EU Node.
    - Open Access is appropriate but no commercial, 'freemium', or other access models are permitted.

(c) The minimum Technology Readiness Level[8] of the *Service* must be at TRL 7 "*System prototype demonstration in operational environment*", together with defined support and maintenance commitments, including Service Level Agreements (SLAs) where applicable.

[8] https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

- Compliance with the latest "*EOSC AAI Architecture*[9]" and its technical requirements for authentication and authorization is mandatory.
- Compliance with the EOSC EU Node's service integration patterns and the applicable cybersecurity and personal data protection laws, regulations, policies, standards, and guidelines set out by the *Operating Unit* is mandatory.
- Provision of the *Service* under a Service Management System (SMS) compliant with recognised standards, such as ISO/IEC 200001 or FitSM, and aligned with ITIL best practices is mandatory.
- Adequate capacity of resources (human, infrastructure) should ensure the provision of the *Service* for up to 500 daily and 50 concurrent users.
- The general availability of the *Service* (even if provided best-effort) should meet the EOSC EU Node's operational threshold in production.

(d) Scalable service architecture and deployment model that appropriately limits the liability exposure of the EOSC EU Node acting as a channel-to-market for the *Service*.

- Use of common Free and Open-Source Software (FOSS) in line with both the Open-Source Software Strategy of the European Commission and the recommendation of the European Interoperability Framework is mandatory. The software, its API descriptions, deployment details and management practices must be fully documented and made available transparently to public.
- All service components must be deployed and provisioned over sovereign infrastructure resources located in EU27 and/or ACs (on premises or in compliant third-party clouds).
- In case infrastructure resources are requested to be provided by the EOSC EU Node, these are subject to approval by the Operating Unit, see Annex B "*Infrastructure Hosting*".

The satisfaction of these eligibility requirements of *Services* is evaluated based on:

- The self-declaration of the *Contributor* provided via the EOSC EU Node's Contributors Dashboard by the designated *User* representative. The *Contributor* may be requested to provide an additional signed statement from its legal representative.

- Additional documentation which may be requested from the *Contributor*, including by not limited to evidence of users across EU27 and/or ACs and multiple disciplines, evidence of international/interdisciplinary use cases, service demonstration and/or access credentials, service management documentation and processes, support channels (Helpdesk), risk assessment and security policy, GDPR-compliance, service architecture and deployment documentation, service provision agreements and SLAs, access policy, capacity plan and (any) requested EOSC EU Node infrastructure resources, open source software repositories and documentation.

- Publicly available information related to the *Service*.

[9] https://zenodo.org/records/15388270

3.3. Resources

In the context of this policy the *Resources* include: "*Data Sources"* (including harvestable targets to repositories), "*Training Materials"*, and "*Interoperability Guidelines"*.

The onboarding processes for all type of *Resources* are described in Annex A "*Onboarding Processes*".

3.3.1. Data Sources

The following eligibility requirements are defined for *Data Sources*:

(a) The research products/outcomes made available by the *Data Source* must have demonstrable and primarily international and interdisciplinary scope.

- A *Data Source* with research products/outcomes in narrower scope must pursue onboarding to an appropriate (i.e. thematic, national or other) Node of the EOSC Federation; should this not be possible, the *Data Source* may be considered eligible for onboarding to the EOSC EU Node or be considered for onboarding to the OpenAIRE Knowledge Graph instead.
- The *Data Source* may already be onboarded to other Node(s) of the EOSC Federation, subject to their onboarding policies, it is not the reason for exclusion.
- The *Data Source* must not be collections or catalogues of *Services*:
    - if the *Data Source* also contains *Services*, these *Services* will be ignored from all onboarding activities,
    - if the *Data Source* is considered to be a *Service* itself, it must be onboarded as a *Service*, see Clause 3.2.

(b) The *Contributor* of the *Data Source* must assume full ownership, responsibility, and accountability of the *Data Source* (i.e. target) vis-à-vis the EOSC EU Node for all matters related to this policy and regardless of the stakeholders, governance, agreements, technologies, and provision models involved.

- The research products/outcomes of the *Data Source* must be produced either by the *Contributor* or by third-party with demonstrable and primary affiliation to the *Contributor*.
- Alternatively, the *Contributor* must provide demonstrable added value to research products/outcomes, e.g.:
    - actively contributed by their original creators (e.g., data curation, reference data, scientific database) or
    - collected and replicated to ensure EU sovereignty.
- A *Data Source* providing research products/outcomes (with a commercial or any other agreement) collected from other Data Sources (i.e. aggregator or metadata catalogue) is not eligible. The *Contributor* may apply to onboard it as a *Service*.
- There must be an established and enforced "Access Policy" of the *Data Source* transparently available in compliance with the AUP and UAP of the EOSC EU Node.

- Open Access is appropriate but no commercial, 'freemium', or other access models are permitted.

(c) The minimum Technology Readiness Level[10] of the *Data Source* must be TRL 7 "*System prototype demonstration in operational environment*", together with defined support and maintenance commitments, including Service Level Agreements (SLAs) where applicable.

- Compliance with the latest "*Registration of Research Product Catalogues in the EOSC EU Node*[11]" is mandatory.
- Compliance with the latest "*EOSC AAI Architecture*[12]"and its technical requirements for authentication and authorization is mandatory (if applicable).
- Research products/outcomes must be citable via "*EOSC-compliant PIDs*[13][14]"
- Compliance with the EOSC EU Node's resource integration patterns and the applicable cybersecurity and personal data protection laws, regulations, policies, standards, and guidelines set out by the *Operating Unit* is mandatory.
- Provision of the *Data Source* under a Service Management System (SMS) compliant with recognised standards, such as ISO/IEC 200001 or FitSM, and aligned with ITIL best practices is mandatory.
- Adequate capacity of resources (human, infrastructure) should ensure the scalable provisioning of the *Data Source* to the users of the EOSC EU Node.
- The general availability of the *Data Source* (even if provided best-effort) should meet the EOSC EU Node's operational threshold in production.

3.3.2. Training Materials

The following eligibility requirements are defined for *Training Materials*:

(a) The *Training Materials* must be directly relevant to:

- the *Resources* and/or *Services* of the EOSC EU Node or those successfully onboarded to the EOSC EU Node by *Contributors,*
- the EOSC Federation in general (subject to approval of the *Operating Unit*), or
- any Open Science practices in general (subject to approval of the *Operating Unit*).

(b) The *Training Materials* must be produced wholly (e.g., content, images, graphics, videos) by the *Contributor*, or third-party creators affiliated with the *Contributor*, or third-party creators that have transferred all their relevant rights to the *Contributor*.

---

[10] https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf
[11] https://zenodo.org/records/17513272
[12] https://zenodo.org/records/15388270
[13] https://op.europa.eu/el/publication-detail/-/publication/35c5ca10-1417-11eb-b57e-01aa75ed71a1
[14] https://zenodo.org/records/11354246

- The *Training Materials* must be available in a Moodle-compatible format suitable for publication in the OpenPlato[15] service.
- The *Training Materials* must be available in the English language and optionally in any other EU27 language.
- There must be an established and enforced "Access Policy" of the *Training Material* transparently available in compliance with the AUP and UAP of the EOSC EU Node.
    - Open Access is appropriate but no commercial, 'freemium', or other access models are permitted.

3.3.3. Interoperability Guidelines

The following eligibility requirements are defined for *Interoperability Guidelines*:

(a) The *Interoperability Guideline* must be officially recognized and approved by the Governance of the EOSC Federation as an "EOSC Interoperability Guideline".

(b) The *Interoperability Guideline* must be produced wholly (e.g., content, images, graphics, videos) by the *Contributor*, or third-party creators affiliated with the *Contributor*, or third-party creators that have transferred all their relevant rights to the *Contributor*.

- It must be deposited in Zenodo[16] with an appropriate Open Access license.
- It must be available in the English language and optionally in any other EU27 language.

The satisfaction of these eligibility requirements of *Resources* is evaluated based on:

- The self-declaration of the *Contributor* provided via the EOSC EU Node's Contributors Dashboard by the designated *User* representative. The *Contributor* may be requested to provide an additional signed statement from its legal representative.

- Additional documentation which may be requested from the *Contributor*, including by not limited to: evidence of users/scope across countries and multiple disciplines, service demonstration and/or access credentials, service management documentation and processes, support channels (Helpdesk), risk assessment and security policy, GDPR-compliance, service architecture and deployment documentation, service provision agreements and SLAs, access policy, capacity plan and (any) requested EOSC EU Node infrastructure resources, open source software repositories and documentation, evidence of affiliations of research products and/or creator, evidence of added value for research products, data source demonstration and/or access credentials, rights statements from creators, licenses of content, confirmation from the EOSC Federation Governance.

- Publicly available information related to the *Resource*.

[15] https://openplato.eu/
[16] https://zenodo.org/

4. Compliance of Contributors

Contributors remain solely responsible for the quality-assured operation and provision of their onboarded *Resources* and *Services* in accordance with this policy, including all aspects of their operation, maintenance, end-user-support, security incident management, SLA commitments (if any), and data protection. *Contributors* must timely report to the *Operating Unit* any anticipated or occurred change in their status or the status of their *Resources* and *Services* related to the application of this policy.

Contributors must timely and effectively respond to security, operational, or service-related incidents affecting their *Resources* and *Services*.

Contributors must comply with the General Data Protection Regulation (GDPR[17]) or equivalent (in case of intergovernmental organisations) and with the EOSC EU Node's ethical guidelines[18] to ensure responsible data handling.

The *Operating Unit* may perform periodic or ad hoc evaluations regarding the conformance of *Contributors*, onboarded *Resources* and *Services*, with this policy. *Contributors* must provide relevant information requested by the *Operating Unit* and comply in cases any incompliance is identified.

All material, information, and communication with the *Operating Unit* are confidential, unless otherwise stated in relation to this policy.

Contributors themselves, their onboarded *Resources* and *Services*, that fail to continuously and uninterruptedly meet applicable eligibility, compliance, operational, or support obligations, or at the sole discretion of the *Operating Unit*, may be offboarded or de-registered, in accordance with a structured and documented decommissioning process. This may include but not limited to:

- Failure to comply with this policy or to inform the *Operating Unit* about anticipated or occurred incompliance with this policy.
- Failure to comply with applicable EOSC Federation level policies or to inform the *Operating Unit* about anticipated or occurred incompliance with such policies.
- Failure to comply with the AUP, UAP, Privacy Statement, Copyright and Cookie policies of the EOSC EU Node.
- Failure to collaborate with the *Operating Unit*, provide requested information, or enact decisions of the *Operating Unit* related to the application of this policy.
- Compromising the security, standing, integrity, or interests of the *Operating Unit*.

[17] General data protection regulation (GDPR) | EUR-Lex
[18] Ethics and Good Administration - European Commission

5. Policy Enforcement and Modification

5.1. Enforcement

This policy will be enforced by the *Operating Unit* (in particular, the EOSC EU Node administrators). Any violation of this policy may result in the suspension or termination of *Contributor's* access. The *Operating Unit* reserves the right to audit access logs and user activities to ensure compliance with this policy.

5.2. Updates and Changes

Policy Changes: The *Operating Unit* reserves the right to modify this policy at any time. *Contributors* will be notified of significant changes and continued use of the *Services* and *Resources* (i.e. relying on the onboarding capabilities of the EOSC EU Node) implies acceptance of the updated terms.

Service Updates: The *Operating Unit* may release software updates, including security patches or new features. *Contributors* are required to update their software (if needed) to continue using the *Services* and/or access the *Resources*.

Service Modifications: The *Operating Unit* may decide to modify or discontinue the onboarding related *Services* or *Services features and functionalities* at its discretion. *Contributors* may lose access to certain functionalities, *Services* and/or *Resources* (including content and data exposed via the EOSC EU Node), without prior notice.

6. Data Privacy and Control

Users accessing *Services* and *Resources* through federated identities (IdPs) acknowledge that their home organization may have control over their account and personal data. The *Operating Unit* may notify home organizations about the usage and the corresponding personal data associated with such federated accounts, especially in cases of compromised personal data.

6.1. Privacy

The *Operating Unit* of the EOSC EU Node respects user privacy but assumes no liability for any personal data management by third parties associated with federated identities. *Users* must comply with their home institution IdP's privacy policies and other guidelines.

For more information, visit the Privacy Statement of the EOSC EU Node[19].

6.2. Termination and Personal Data Retention

Upon termination of a *User's* access (whether by the *User* itself or the *Operating Unit*), access to *Services* and *Resources* and the associated personal data will be immediately revoked. The *Operating Unit* will delete or disassociate corresponding data (including the *Contributor*

[19] https://open-science-cloud.ec.europa.eu/privacy-statement

Representative role), except where legally required to retain it. *Users* are advised to maintain regular backups of their user data.

7. Computer Security Incident Response

The *Operating Unit* of the EOSC EU Node is committed to ensuring the security and integrity of its own *Services* and *Resources*, the content and user data processed within it. In the event of a computer security incident, the *Operating Unit* will follow established procedures to identify, mitigate, and respond to any security threats or breaches.

Contributors are required to immediately report any suspected or confirmed security incidents, such as unauthorized access, data breaches, vulnerabilities or malware infections, to the EOSC EU Node's Computer Security Incident Response Team (CSIRT) via: security@open-science-cloud.ec.europa.eu

EOSC EU Node administrators will promptly investigate all reports. *Contributors* who fail to follow the security standards applying to all European Commission information systems[20] or who are found to be responsible for a security incident due to negligence or misconduct may face access restrictions, suspension, or termination of their account.

In the case of a significant security breach, the *Operating Unit* will inform affected *Users/Contributors* in a timely manner. Notifications will include details about the incident, any data compromised, and recommended actions *Users/Contributors* should take.

8. Disaster Recovery

The *Operating Unit* of the EOSC EU Node is committed to ensuring the continuity and availability of its own *Services* and *Resources* in the event of a disaster. The EOSC EU Node has an established Disaster Recovery Plan (DRP) designed to minimize service disruptions, protect data integrity, and restore normal operations as quickly as possible.

Regular backups of critical systems and user data are performed (including the onboarding processes). These backups are securely stored in geographically dispersed locations to ensure data availability in the event of a localized disaster. Backup frequency and retention policies are aligned with EU regulations on data protection and disaster recovery.

9. Helpdesk Support

For enquiries and support relating to this policy, *Users/Contributors* may contact the EOSC EU Node Helpdesk[21].

[20] https://commission.europa.eu/publications/security-standards-applying-all-european-commission-information-systems_en
[21] https://open-science-cloud.ec.europa.eu/support/helpdesk

10. Limitation of Liability

10.1. General Liability

EOSC EU Node provides its own *Services* and *Resources* (including those related to onboarding) on an "as-is", "as-available" and "best-effort" basis. To the maximum extent permitted by applicable law, the *Operating Unit* of the EOSC EU Node and its affiliated parties (i.e., third-party service and resource providers) will not be liable for any direct, indirect, incidental, consequential, or special damages arising out of or in connection with the use of the *Services* and *Resources*, even if advised of the possibility of such damages. This includes, but is not limited to, damages for loss of profits, data, or other intangible losses.

10.2. Service Availability

EOSC EU Node strives to ensure the availability and reliability of its *Services*, including those related to onboarding. However, the *Operating Unit* of the EOSC EU Node makes no guarantees regarding the uninterrupted or error-free operation of its own *Services* and *Resources*, the accuracy of any information, content or data provided through the *Websites*, or the ability of the *Services* to meet the user's specific needs.

Services and *Resources* may be unavailable from time to time due to maintenance or unforeseen disruptions. The *Operating Unit* of the EOSC EU Node does not guarantee continuous availability of *Services* and is not liable for any data loss resulting from service outages.

10.3. Data Integrity

While EOSC EU Node implements strong security measures to protect user data, the *Services* and *Resources* cannot guarantee absolute security. *Contributors* are solely responsible for ensuring they maintain appropriate backups of their own data. The *Operating Unit* of the EOSC EU Node will not be liable for any data loss or corruption arising from the use of its *Services* and *Resources*.

10.4. Third-Party Services and Resources Onboarded

EOSC EU Node may integrate with or provide access to third-party *Services* and *Resources* as a federated system of systems under this policy. The *Operating Unit* of the EOSC EU Node makes no warranties or representations about these third-party *Services* and *Resources* and will not be liable for any issues arising from their use, users assume all risks associated with their use. *Users* are responsible for reviewing and agreeing to the terms of service of any third-party services and resources they utilize through the *Websites*. Third-party terms do not alter this policy.

10.5. Legal Compliance

The *Operating Unit* of the EOSC EU Node makes every effort to comply with applicable laws and regulations. However, *Contributors* are solely responsible for ensuring their use of the *Services* and *Resources* (including those related to onboarding) complies with any applicable legal and regulatory requirements. The *Operating Unit* will not be liable for any *Contributor's* failure to comply with such laws.

10.6. Force Majeure

The *Operating Unit* shall not be liable for any failure to the EOSC EU Node's *Services* and *Resources* its obligations under this policy if such failure results from causes beyond its reasonable control, including but not limited to natural disasters, acts of war, terrorism, labour disputes, or governmental actions.

POLICY STATEMENTS

- Node Registration Policy: https://open-science-cloud.ec.europa.eu/support/node-registration-policy
- Acceptable Use Policy of the EOSC EU Node: https://open-science-cloud.ec.europa.eu/support/acceptable-use-policy
- User Access Policy of the EOSC EU Node: https://open-science-cloud.ec.europa.eu/support/user-access-policy
- Privacy Statement for the EOSC EU Node: https://open-science-cloud.ec.europa.eu/privacy-statement
    - *Services* accessible via the *Websites* may have additional Privacy Statements published in their domains.
- Copyright Notice: https://commission.europa.eu/legal-notice_en#copyright-notice
- Cookies Policy: https://commission.europa.eu/cookies-policy_en

The Data Protection Officer of the Commission is: data-protection-officer@ec.europa.eu

The Computer Security Incident Response Team (CSIRT) contact is: security@open-science-cloud.ec.europa.eu

The Security Contact for this policy is: CNECT-LISO@ec.europa.eu

Annex A – Onboarding Processes

Contributors Dashboard

Onboarding is initiated and managed via a dedicated section of the User Space of the EOSC EU Node (hereinafter referred to as "*Contributors Dashboard*"). Access to the *Contributors Dashboard* is available to all authenticated users of the EOSC EU Node according to its User Access Policy (UAP)[22].

Contributor registration

A *Contributor* must successfully register in the *Contributors Dashboard* via its authorized representative *User* (hereinafter referred to as "*Contributor Representative*"). The *Contributor Representative* must be duly authorised to represent the *Contributor* on whose behalf *Resources* and *Services* are onboarded to the EOSC EU Node.

A *Contributor* must be represented by only one *Contributor Representative* during the Contributor registration process. After the successful Contributor registration, the *Contributor Representative* may delegate this role to additional *Users* at their own discretion. These *Users* (also referred as *Contributor Representatives*) must be duly authorised to represent the *Contributor* on whose behalf *Resources* and *Services* are onboarded to the EOSC EU Node.

A *User* may be a *Contributor Representative* for more than one *Contributors*.

The registration process is as follows:

(a) The *Contributor Representative* must provide all required information in the *Contributors Dashboard* and submit the application for review.

(b) The *Operating Unit* may review the provided information and validate the satisfaction of the eligibility criteria of this policy or request additional information or revisions.

(c) The *Contributor Representative* must address the review of the *Operating Unit* and re-submit the application for review.

(d) Steps (b) and (c) are repeated until the application is accepted or rejected. All decisions of the *Operating Unit* are binding for the *Contributor*.

- In case of acceptance, the *Contributor* is successfully registered in the EOSC EU Node, and its *Contributor Representative* may initiate onboarding for *Resources* and *Services*.
- In case of rejection, the *Contributor* may request its re-registration no earlier than 3 months after its rejection.
- In case of disputes, the EOSC Tripartite Governance[23] can be contacted for seeking mediation.

In addition, the following apply for successfully registered *Contributors*:

---

[22] https://open-science-cloud.ec.europa.eu/support/user-access-policy
[23] Tripartite Collaboration - EOSC Association

- The *Contributor* must maintain all provided information as part of its original registration updated, complete, and accurate via the *Contributors Dashboard*. In this case, points b) to d) of the registration process are followed.
- The *Operating Unit* may review the satisfaction of the eligibility criteria of this policy for a successful registered *Contributor* at its own discretion and at any point in time. In this case, points b) to d) of the registration process are followed.
- The *Contributor* may request the change of its *Contributor Representative* by contacting the Helpdesk of the EOSC EU Node.
- The *Contributor* may request to be de-registered via the *Contributors Dashboard*. This action is irrevocable and will result into the offboarding of the Contributor's *Resources* and *Services* (if any).
- The *Contributor* may be re-registered by the *Operating Unit* at its own discretion. This action is irrevocable and will result into the offboarding of the Contributor's *Resources* and *Services* (if any).

Onboarding a Service

A successfully registered *Contributor (*i.e. the *Contributor Representative)* may initiate the onboarding of a *Service* via the *Contributors Dashboard*.

The onboarding process is as follows:

(a) The *Contributor Representative* must provide all required information in the *Contributors Dashboard* and submit the application for review.

(b) The *Operating Unit* may review the provided information and validate the satisfaction of the eligibility criteria of this policy or request additional information or revisions. This will include the technical validation of all applicable EOSC Interoperability Guidelines and technical requirements of the current policy (see Annex B "*Technical Requirements for Services*").

- The *Contributor* may confidentially be provided with:
  - appropriate access to the testing and staging environments of the EOSC EU Node,
  - access to technical documentation, APIs, and services of the EOSC EU Node,
  - access to collaboration and development management services of the EOSC EU Node.

- The *Contributor* must:
  - provide access to the testing, staging, and production environments of its Service,
  - actively collaborate with the *Operating Unit* on all matters related to the Technical Requirements (see Annex B) and operational requirements of the *Service* in the testing, staging, and production environments,
  - assume the responsibility and effort required for the satisfaction of the Technical Requirements (see Annex B).

- The *Operating Unit* will establish the acceptance criteria and assess the *Service* and its operational characteristics in the testing and staging environments before rolling out in production. This includes the establishment and agreement on a transparent and harmonised Access Policy to the *Service* (if applicable) in line with the AUP and UAP of the EOSC EU Node.

(c) The *Contributor Representative* must address the review of the *Operating Unit*, ensure the required revisions in the *Service* and its operational characteristics are performed, and re-submit the application for review.

(d) Steps (b) and (c) are repeated until the application is accepted or rejected. All decisions of the *Operating Uni*t are binding for the *Contributor*.

- In case of acceptance, the *Service* is successfully onboarded in the production environment of the EOSC EU Node.
    - The *Service* may be presented in the Resource Hub and registries of the EOSC EU Node.
    - The *Service* may be presented in the User Space of the EOSC EU Node.
    - The *Service* may be integrated with other EOSC EU Node services.
- In case of rejection, the *Contributor* may request the re-onboarding of the *Service* no earlier than 6 months after its rejection.
- In case of disputes, the EOSC Tripartite Governance[24] can be contacted for seeking mediation.

In addition, the following apply for onboarded *Services*:

- The *Contributor* must maintain all provided information as part of the *Service* onboarding updated, complete, and accurate via the *Contributors Dashboard*. In this case, points b) to d) of the registration process are followed.
- The *Operating Unit* may review the satisfaction of the eligibility criteria of this policy for a successful onboarded *Service* at its own discretion and at any point in time. In this case, points b) to d) of the registration process are followed.
- The *Contributor* may request to offboard its *Service* via the *Contributors Dashboard*. This action is irrevocable and will result in the removal of the *Service* from the EOSC EU Node.
- A *Service* may be offboarded by the *Operating Unit* at its own discretion. This action is irrevocable and will result in the removal of the *Service* from the EOSC EU Node.

Onboarding a Resource

A successfully registered *Contributor (*i.e. the *Contributor Representative)* may initiate the onboarding of a *Resource* via the *Contributors Dashboard*.

In the context of this policy a *Resource* can include: a *Data Source*, a *Training Material*, and an *Interoperability Guideline*.

[24] Tripartite Collaboration - EOSC Association

The onboarding process is as follows:

(a) The *Contributor Representative* must provide all required information in the *Contributors Dashboard* and submit the application for review.

(b) The *Operating Unit* may review the provided information and validate the satisfaction of the eligibility criteria of this policy or request additional information or revisions. This may include the technical validation of all applicable interoperability guidelines and requirements of the current policy.

(c) The *Contributor Representative* must address the review of the *Operating Unit*, perform the required revisions in the *Resource*, and re-submit the application for review.

(d) Steps (b) and (c) are repeated until the application is accepted or rejected. All decisions of the *Operating Unit* are binding for the *Contributor*.

- In case of acceptance of a *Data Source*, it is successfully onboarded in the EOSC EU Node.
    - The *Data Source* may be presented in the Resource Hub and included in the registries of the EOSC EU Node.
    - Research products/outcomes of the *Data Source* may be harvested and aggregated in the Knowledge Graph of the EOSC EU Node and presented in its Resource Hub according to its Inclusion Criteria (see Annex D).
    - Research products/outcomes of the *Data Source* may be subjected to additional validation and curation processes conducted by the EOSC EU Node (see Annex E).

- In case of acceptance of a *Training Material*, it is successfully onboarded in the EOSC EU Node.
    - The *Training Material* may be presented in the Resource Hub and included in Learning Management System (OpenPlato) of the EOSC EU Node.
    - The *Training Material* may be provided as part of a curated collection and/or learning path in the Learning Management System of the EOSC EU Node.

- In case of acceptance of an *Interoperability Guideline*, it is successfully onboarded in the EOSC EU Node.
    - The *Interoperability Guideline* may be presented in the Resource Hub and included in the registries of the EOSC EU Node

- In case of rejection of a *Resource*, the *Contributor* may request the re-onboarding of the *Resource* no earlier than 3 months after its rejection.

- In case of disputes, the EOSC Tripartite Governance[25] can be contacted for seeking mediation.

In addition, the following apply for onboarded *Resources*:

- A *Contributor* must maintain all provided information as part of *Resource* onboarding updated, complete, and accurate via the *Contributors Dashboard*. In this case, points b) to d) of the registration process are followed.
- The *Operating Unit* may review the satisfaction of the eligibility criteria of this policy for a successful registered *Resource* at its own discretion and at any point in time. In this case, points b) to d) of the registration process are followed.
- The *Contributor* may request to offboard its *Resource* via the *Contributors Dashboard*. A *Resource* may also be offboarded by the *Operating Unit* at its own discretion
    - *Data Source*: This action is irrevocable and will result into the removal of the harvested research products/outcomes (if any) from the EOSC EU Node Knowledge Graph.
    - *Training Material:* This action is irrevocable and will result into the removal of the *Training Material* from the Learning Management System.
    - *Interoperability Guideline*: This action is irrevocable and will result into the removal of the *Interoperability Guideline* from the Resource Hub of the EOSC EU Node.

[25] Tripartite Collaboration - EOSC Association

Annex B -Technical Requirements for Services

Service Environments

The *Service* must be available in at least three different deployment environments, with appropriate access granted to the Operating Unit:

- **Production:** the permanent production environment of the *Service* targeting end users, integrated with the EOSC EU Node production environment, and provisioned according to the operational requirements of the currently policy.
- **Staging:** must be identical to the Production environment (only differing in the sizing of infrastructure resources used), integrated only with the EOSC EU Node Staging environment, and is used exclusively to validate, and quality-assure the Service and its integration with the EOSC EU Node.
- **Testing:** may differ from the Production environment, integrated only with the EOSC EU Node testing environment, and used exclusively for development purposes.

Integration with EOSC EU Node Services

The *Service* may be requested to be integrated with the following services, components, and APIs of the EOSC EU Node, at the discretion of the *Operating Unit*:

- **AAI** (mandatory): Register the *Service* in the EOSC EU Node AAI for user authentication and authorization, accepting the Terms and Conditions of the Operating Unit's contractor.
- **User Space:** The main point for provisioning, managing quota, and accessing EOSC EU Node services.
- **Accounting** (mandatory if the virtual credit model of the EOSC EU Node is applied): Define and report the usage of service offerings (quota, credits).
- **Order Management Service & Service Offers** (mandatory if the virtual credit model of the EOSC EU Node is applied): Define service offerings on the EOSC EU Node and enable provisioning/deprovisioning flows for those offerings.
- **Monitoring** (mandatory) with two integration options available:
    - Provide access to an existing monitoring service offering availability and reliability information.
    - Register the service in the Monitoring Service of the EOSC EU Node.
- **Helpdesk** (mandatory) with two integration options available (triaging always takes place from the Level 1 Support Unit of the EOSC EU Node):
    - Operate Level 2/3 Support Units in the EOSC EU Node Helpdesk.
    - Integrate an existing Helpdesk system with the EOSC EU Node Helpdesk.

Service Access Policy

The *Service* must be provisioned under a transparent and harmonised Service Access Policy (SAP):

- Fully compliant with the automated authorization model and Access Policy Groups of the EOSC EU Node as prescribed in its User Access Policy (UAP).
- Fully compliant with the Acceptable Use Policy (AUP) of the EOSC EU Node.
- Consistent with the *Service* capacity plan and minimum eligibility requirements for daily and concurrent users.
- An SAP template may be provided by the *Operating Unit* and subjected to its approval.

Access Groups

The *Service* must be provisioned according to the following requirements:

- The authorization of users and Service Limits must be automated based on their Access Group. Service Limits prescribe the characteristics of the Service provision (e.g., quota) of the Service per Access Group.
- The *Service* must be available at least to Access Group AP-B users (Investigator) and optionally to Access Groups AP-A1 (Collaborator) and AP-A (Observer) with identical or lower Service Limits.
- The *Service* must not be provided to Access Group AP-0 users (Explorer), i.e., not authenticated users.
- The *Service* may be provided to EOSC EU Node Groups.

Virtual Credits

The *Service* must be provisioned under the virtual credit model of the EOSC EU Node if hosted on the EOSC EU Node infrastructure resources (otherwise it is optional). See Annex C "*Infrastructure Hosting*". The following requirements apply:

- A *User* must be able to consume their Credit Allocation of their personal wallets, as defined in the UAP of the EOSC EU Node.
- A *Group* must be able to consume their Credit Allocation of their Group wallets (if the service is provided to Groups), as defined in the UAP of the EOSC EU Node.
- The billing model (i.e., Service Weights in credits per Service limit) for the Service must be defined to effectively manage demand and represent the actual underlying resource utilization for *Service* provision.
- The billing model may be reservation-based (perpetual or fixed duration) or on-demand (i.e., pay-as-you-go).
- The cost model and Service Weights are defined by the Operating Unit, with any change subject to its approval.

Other Requirements

The following requirements must be satisfied:

- Support persistent identifiers (PIDs) for shared datasets, software, and other digital objects, where applicable.
- Dedicated service contact points for technical, operational, and security issues.
- Dedicated end-users' support available via Helpdesk.
- Implement appropriate security controls, including defined roles, responsibilities, procedures, and best practices, based on a documented risk assessment.
- Prepare and publish a Privacy Statement for the *Service*. Identify and document EU GDPR roles (e.g. Data Controller, Data Processor, or Third Party) and responsibilities for the Service and implement all legal obligations. Where GDPR does not apply directly, equivalent safeguards must be implemented.
- Implement a backup, restoration, and disaster recovery policy.
- Implement automated quality-assurance workflows and validation for the *Service*.
- All software developed by the *Contributor* covering the scope of the *Service* onboarding with the EOSC EU Node available with an Open-Source license (the original license of the software project if relevant, or EUPL).
- Produce, publish and maintain documentation and training material covering the scope of the *Service* as onboarded in the EOSC EU Node (available with Creative Commons

Attribution 4.0 license). Relevant *Training Material* must be onboarded according to this policy.

Annex C – Infrastructure Hosting

The *Service* may opt-in to be hosted wholly or partly on the EOSC EU Node's underlying infrastructure.

- Infrastructure resources to be provided for *Services* may include:
  (a) Managed Container Platform
  (b) Virtual Machine Service
  additionally storage resources (Bulk Data Transfer service endpoint and/or Enterprise File Sync and Share domain), and the required network connectivity. No other infrastructure resources or related services are to be provided.
- Infrastructure resources are provided to the *Contributor* for free-of-charge and as-is, under the Acceptable Usage Policy (AUP) of the EOSC EU Node.
- Infrastructure resources are to be used exclusively for the provision of the *Service* to EOSC EU Node users.
- The exact type, size, characteristics, and availability of the provided infrastructure resources are exclusively subject to the approval of the *Operating Unit*, which may revoke their availability at any point in time.

The *Contributor* remains fully and solely responsible for the provision of the *Service* under the requirements of the current policy.

Hosting organisations and legal status

The EOSC EU Node's underlying infrastructure that may be made available for *Contributors* to host their onboarded *Services* are provided by two organisations: Poznan Supercomputing and Networking Centre (PSNC) with headquarter in Poznan, Poland and Safespring AB with headquarter is Stockholm, Sweden.

The hosting organisations are contracted by the *Operating Unit* under the Service Contract "Managed Services for the European Open Science Cloud (EOSC) Platform" CNECT-LUX-2022-CD-0023 - Lot 2: Managed Container Platform and Virtual Machine Services for the EOSC Exchange (Infrastructure Services): *CONTRACT NUMBER – LC-02474277*

The current service contract is due to expire on 13 February 2027. The Operating Unit is committed to re-procure the EOSC EU Node services as a 4-year Framework Contract until 2031.

Technical service descriptions

(a) Managed Container Platform

The container platform service provides a managed runtime environment for containerised workloads based on Kubernetes/OKD. It is intended for teams that require a consistent, production-grade execution layer without operating the control plane, worker nodes, networking stack or supporting services themselves. The platform is available in two physical sites - at Poznan Supercomputing and Networking Centre (PSNC) in Poznan, Poland, and at Safespring AB in Kalix, Sweden. *Contributors* may host their applications in one or two sites.

- Platform architecture

The platform is built on OKD, a Kubernetes-compatible distribution, exposing standard Kubernetes APIs and resource models. Workloads are deployed as containers using native Kubernetes resources such as Deployments, StatefulSets, Jobs and CronJobs.
Core components also include:

- Integrated container image registry - for storing and versioning images
- S3-compatible object storage - for scalable, durable storage of unstructured data, accessible via standard S3 APIs

The platform lifecycle (patching, upgrades, security fixes) is managed centrally.

- Tenant model and access

  Contributors may be provisioned with one or more dedicated Kubernetes namespaces within a managed cluster.
  Namespaces provide:
  - Logical isolation of workloads and resources
  - Scoped access control via RBAC
  - Independent resource quotas and limits
  - Separation of environments (e.g. dev, test, production)

  Access to the platform is provided via standard interfaces (e.g. kubectl/oc, API, OKD Console), with permissions restricted to assigned namespaces. *Contributors* operate within these namespaces without access to cluster-level components.

- Workload management

  Applications are deployed and executed within isolated containers/pods. The platform supports:
  - Horizontal scaling (HPA/manual) based on CPU, memory or custom metrics
  - Rolling updates and rollbacks
  - Self-healing via liveness and readiness probes
  - Resource management using requests and limits
  - Namespace-level quotas to control consumption

  Stateful workloads are supported using StatefulSets with persistent storage.

- Networking and exposure

  The platform provides built-in service networking and ingress:
  - Cluster-internal service discovery (DNS-based)
  - Ingress controllers for HTTP/HTTPS exposure
  - Automatic TLS certificate provisioning
  - Network policies to control traffic between workloads

  Applications can be exposed externally without managing certificates or external load balancers directly.

- Observability

  The platform includes integrated observability components:
  - Metrics collection (Prometheus-compatible)
  - Centralised logging across containers and namespaces
  - Telemetry pipelines for resource and workload data

    - Alerting mechanisms based on defined thresholds

- Supported data services

  Data management capabilities include:
    - Persistent storage provisioning via storage classes and dynamic volume allocation
    - Automated backup mechanisms
    - S3-compatible object storage

  In addition, the platform includes ready-to-deploy:
    - PostgreSQL
    - MySQL

  These can be configured in high-availability setups (replication/failover) and are integrated with platform storage, monitoring and backup mechanisms.

- Security model

  Security is enforced at multiple layers:
    - TLS encryption for ingress endpoints (automated)
    - Role-based access control (RBAC) scoped to namespaces
    - Image registry access control
    - Namespace isolation and quotas
    - Regular platform patching and updates

- Operations and support

  The platform is operated with continuous oversight:
    - 24/7 monitoring of cluster and infrastructure components
    - Proactive issue detection and remediation
    - Regular performance and security validation
    - Support for deployment, configuration and troubleshooting

(b) Virtual Machine Service

Our service provides a managed Infrastructure-as-a-Service (IaaS) environment for virtual machines based on OpenStack. It is intended for teams that need virtual compute, storage, and networking resources without operating the underlying OpenStack platform, hypervisors, or infrastructure components.

- Platform architecture

  The service is based on OpenStack and exposes standard IaaS capabilities for provisioning and managing virtual machines.
  Core components include:
    - Compute (VM lifecycle management)
    - Block storage (persistent volumes)
    - Image service (VM templates)
    - Virtual networking (subnets, routing, security groups)

Contributors consume infrastructure through a managed abstraction layer rather than interacting directly with OpenStack internals.

- Tenant model and access

  Contributors' access is provided through a central service portal integrated with the platform.
  Key characteristics:
  - Contributors are onboarded via the portal
  - Access control is managed through centralised AAI (authentication and authorization infrastructure)
  - Each *Contributor* is assigned a dedicated tenant/project
  - Resource allocation is based on predefined custom T-shirt size quotas (bundled CPU, RAM, storage, and networking limits) to be decided by the *Operating Unit* on a case-by-case basis.

  This model removes the need for direct OpenStack account and quota management by end users.

- Workload management

  Within each tenant, *Contributors* can:
  - Create, start, stop, and delete VMs
  - Use predefined or custom images
  - Attach and manage block storage volumes
  - Configure access via SSH keys and cloud-init

  Resource usage is constrained by assigned quota (i.e. custom T-shirt size model).

- Networking

  The service provides standard OpenStack-based virtual networking:
  - Private tenant networks and subnets
  - Floating IPs for external access
  - Security groups for basic traffic filtering
  - Routing between internal and external networks

  Physical network infrastructure is fully managed by the platform.

- Storage services

  Storage is provided through OpenStack block storage services:
  - Persistent volumes for VMs
  - Snapshot capability for backup/restore use cases
  - Image repository for VM templates

- Security model

  Security is implemented through:
  - Centralised AAI for authentication and authorization
  - Tenant isolation via OpenStack projects
  - Security groups for network-level access control
  - TLS for API and portal access

- Operations and support

  The platform is operated with continuous oversight:
  - 24/7 monitoring of cluster and infrastructure components
  - Proactive issue detection and remediation
  - Regular performance and security validation
  - Support for deployment, configuration and troubleshooting

Annex D – Inclusion Criteria

The EOSC EU Node Knowledge Graph ("*KG*"), available through the EOSC EU Node Resource Hub ("*Resource Hub*"), aims to deliver an entry point for the discovery of research data, publications, software, and other outputs of the EOSC EU Node and the EOSC Federation.

The KG is populated with metadata harvested from:

- Default sources (required by the *Operating Unit*):
  - (a) OpenAIRE Graph
  - (b) CELLAR
  - (c) CORDIS
  - (d) European Open Data Portal
  - (e) Software Heritage
  - (f) Open Research Europe
  - (g) JRC Data Catalogue
- EOSC EU Node/Federation catalogues and registries:
  - (h) EOSC EU Node Service Catalogue
  - (i) EOSC EU Node Tools Hub
  - (j) Resource and Service catalogues of other EOSC Node of the federation.

The present Annex sets out the inclusion policies and applicable restrictions governing the ingestion of metadata from these and future *Data Sources* into the *KG*, with the objective of ensuring coherence, quality, and consistency of the resources made available through the Resource Hub.

Inclusion Criteria

(a) OpenAIRE Graph

The OpenAIRE Graph[26] acquires metadata information from data sources worldwide that researchers use to publish and share their research products. The principle is to potentially trust all sources and scientists, while tracking provenance, analysing completeness and trust of the metadata records collected from them, to identify anomalies and provide feedback to data source providers and scientists, improving the quality of the publishing process.

The *KG* is bootstrapped from the OpenAIRE Graph with the following restrictions and inclusion criteria:

- **Projects**: The OpenAIRE Graph collects project and grant information from more than 300 funding organisations worldwide. Only projects funded under programmes of the European Commission (EC) are eligible for inclusion in the *KG*.
- **Topics and Subjects**: Subject classification within the *KG* is based on the Fields of Science ontology[27] .

[26] https://graph.openaire.eu/
[27] https://explore.openaire.eu/fields-of-science

- **Data sources, Authors and Organizations**: The *KG* includes *Data Sources*, Authors, and Organisations that feature at least one connection to a Research Product that satisfies the EOSC *KG* inclusion criteria.
- **Research Products**: Research Products are publications, research data, software, and other types of outputs that do not fall within the preceding categories. The inclusion criteria for Research Products from the OpenAIRE Graph are:
    - All **Research Products** must have at least one Persistent Identifier (PID) of type DOI, ArXiv, PubMed, Handle, SoftwareHeritageID, or accession numbers (like PDB, ENA, UNIPROT)
    - **Publications** must have at least:
        - Title
        - Author
        - Abstract
        - Date of Publication
    - **Research Data** must have at least:
        - Title
        - Author
        - Date of Publication
    - **Software** must have at least:
        - Title
        - Date of Publication

(b) CELLAR

CELLAR[28] is the common data repository of the Publications Office of the European Union. The inclusion criteria for Research Products from the CELLAR are:

- **All metadata** records that have a Title are included.

(c) CORDIS

The EOSC KG gets data from CORDIS as available and documented[29]. Specifically, it includes the datasets with metadata about publications and deliverables declared by projects funded under FP7, H2020, and HE. Such metadata records are included in the EOSC KG via the OpenAIRE Graph, which also includes projects from the Erasmus+ web site[30].

The inclusion criteria for **Publications** from CORDIS are:

- One Persistent Identifier (PID) of type DOI, ArXiv, PubMed, Handle
- Title
- Author
- Abstract
- Date of Publication

[28] https://op.europa.eu/web/cellar/
[29] https://cordis.europa.eu/about/services
[30] https://erasmus-plus.ec.europa.eu/projects/projects-lists

(d) European Open Data Portal

The European Open Data Portal (ODP[31]) is the official portal for European data.
The inclusion criteria for Research Products from the European Open Data Portal are:

- **Publications** must have at least:
  - One Persistent Identifier (PID) of type DOI, ArXiv, PubMed, Handle
  - Title
  - Author
  - Abstract
  - Date of Publication
- **Datasets and software** must have at least:
  - Title

(e) Software Heritage

Software Heritage[32] keeps an extensive archive of known software versioning repositories worldwide. As such, (i) the large majority of software repositories it archives is not the outcome of scientific process, and (ii) it does not provide any bibliographic metadata (e.g. attribution, description, publishing, etc).

The OpenAIRE Graph integrates methods to full-text mine articles to identify references to Software Heritage that *implicitly* point to research software. Accordingly, the EOSC KG relies on the OpenAIRE Graph to identify bibliographic metadata of research software available in Software Heritage.

Any software in the OpenAIRE Graph available in Software Heritage is included.

(f) Open Research Europe

Open Research Europe (ORE[33]) is an open access publishing venue for European Commission-funded researchers across all disciplines, with no author fees.

The inclusion criteria for Research Products from ORE are:

- At least one Persistent Identifier (PID) of type DOI, ArXiv, PubMed, Handle
  - Title
  - Author
  - Abstract
  - Date of Publication

(g) JRC Data Catalogue[34]

No restrictions: all metadata records are included.

---

[31] https://data.europa.eu/
[32] https://www.softwareheritage.org/
[33] https://open-research-europe.ec.europa.eu/
[34] https://data.jrc.ec.europa.eu/

(h) EOSC EU Node Service Catalogue

No restrictions: all metadata records are included.

(i) EOSC EU Node Tools Hub

No restrictions: all metadata records are included.

(j) Resource and Service Catalogues of other EOSC Nodes of the federation

The inclusion criteria for **Research Products** are the same applied to the OpenAIRE Graph. **Services** have no restrictions: all metadata records are included.

Annex E – Curation

The research products/outcomes' curation practice performed by the operators of the EOSC EU Node includes:

- Automated spam detection.
- Manual curation to tag records as spam and to confirm/reject automatically identified spam records.