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 User Access Policy

Version 2.2

USER ACCESS POLICY

1. Purpose

This User Access Policy ("UAP") defines the access groups, their corresponding access rights, service limits, and virtual credit allocation policies for the users of the EOSC EU Node's Resources ("*Resources*") and Services ("*Services*") 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*"). This policy ensures users have the appropriate level of access according to their role and affiliation while maintaining system integrity, security, and compliance with EU regulations and applicable law.

2. Scope

This policy applies to all users of the EOSC EU Node, covering access to *Services* and *Resources*, with the underlying infrastructure, provided through the EOSC EU Node (hereinafter referred to as "*Websites*"). The policy outlines how users are categorized into access groups, their corresponding rights, obligations, and resource usage limits.

This policy does not apply for third-party onboarded services and resources. For information, users shall visit the user access policies of those third-party providers.

3. Access Groups and Access Rights

The following sections define the access groups used within the EOSC EU Node for the *Services* and *Resources* provisioned by the *Operating Unit*, their corresponding access rights, service limits, and credit allocation policies (i.e. all together referred to as "*Access Policy*" – *AP-x*).

3.1. Access Group AP-0 (Explorer)

Access Group AP-0 includes all users who are not authenticated (i.e., not logged in). This group is granted open access to publicly available content on the *Websites*.

Access Rights

Users in Access Group AP-0 are granted the following rights:

- **Access to Web Front-office (public website)**: Access to all publicly available content.
- **Access to Resource Hub (open access)**: Access to all open-access resources, including datasets, publications, and tools.
- **Access to Trainings Portal (all open training materials)**: Access to open educational content, tutorials, and guides.
- **No Access to personalized features of the *Websites***.
- **No Access to the User Space**, in particular.
- **No Access to infrastructure and application *Services***.

Service Limits

- Not applicable

Credit Allocation

- Not applicable

3.2. Access Group AP-A (Observer)

Access Group AP-A includes users who have successfully authenticated via eduGAIN inter-federation[1] and EU Login[2] including eIDAS access federation[3]. This group allows for users from all federated Identity Providers (IdPs), except social media and guest IdPs. Self-registration is also possible via the EU Login service[4].

Access Rights

In addition to the rights granted to AP-0 users, AP-A user have access to the following:

- **Access to personalized features of the *Websites*.**
- **Access to User Space (view only)**: Users can view their personalized user space but cannot modify their settings.
- **Access to infrastructure and application *Services* (view only)**: No ability to incorporate, modify or upload data.

Service Limits

- Not applicable.

Credit Allocation

---

[1] eduGAIN https://edugain.org/
[2] EU Login https://webgate.ec.europa.eu/ern/userguide/Content/A.HOW%20TO%20JOIN/Register%20on%20EU-Login.htm
[3] eIDAS https://eidas.ec.europa.eu/
[4] EU Login registration https://webgate.ec.europa.eu/cas/eim/external/register.cgi

- **0 Credits**: No credit allocation available. Users can view their user space but cannot use the infrastructure and application Services.

3.3. Access Group AP-A1 (Collaborator)

Access Group AP-A1 includes users authenticated via eduGAIN inter-federation and EU Login, with specific restrictions:

- **eduGAIN**: IdPs restricted to EU27[5] and Horizon Europe Associated Countries[6], filtered for affiliation attributes of *employee* and *staff*[7] (i.e., faculty, students, affiliates, members, alums and library-walk-in are excluded from this group).
- **EU Login**: Restricted to European Commission and its agencies staff, filtered by *domain attribute* (i.e., citizen scientists authenticated via eIDAS are excluded).

Access Rights

In addition to the rights granted to AP-A users, AP-A1 users are granted the following:

- **Access to User Space**: Users can access the application Services of the EOSC EU Node and a limited set of the infrastructure services.
- **Access to application Services**:
  - **Large File Transfer**: Uses FileSender technology to transfer arbitrary large files via the web.
  - **File Sync and Share**: Uses ownCloud technology to synchronise and share files and folders with collaborators.
  - **Interactive Notebooks**: Uses Jupyter technology giving access to Small and Medium (S/M) environment only to launch interactive notebooks.
- **Access to infrastructure Services (limited):**
  - **Virtual Machines:** Uses OpenStack technology giving access to Small (S) environment to provision compute resources with storage and network.
  - **Cloud Container Platform:** Uses Kubernetes technology giving access to Small (S) environment to provision containerised applications.

Service Limits

- **Large File Transfer**: Up to 1TB transfer (upload) per month.
- **File Sync and Share**: Up to 50GB personal storage space.
- **Interactive Notebooks**:
  - Small (S) environment: Up to 2 vCPU with 4GB RAM, 20GB local and 50GB remote storage, 1 Gbps network bandwidth.
  - Medium (M) environment: Up to 4 vCPU with 8GB RAM, 100GB local and 200GB remote storage, 10 Gbps network bandwidth
- **Virtual Machines**:

[5] EU27 countries https://european-union.europa.eu/easy-read_en
[6] Horizon Europe Associated Countries https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/list-3rd-country-participation_horizon-euratom_en.pdf
[7] eduPersonAffiliation attribute https://technical.edugain.org/doc/GN3-11-012%20eduGAIN_attribute_profile.pdf

    - Small (S) environment: Up to 2 vCPU with 8GB RAM, 200GB local and 500GB remote storage, 1 Gbps network bandwidth
- **Cloud Container Platform:**
    - Small (S) environment: Up to 2 vCPU with 8GB RAM, 200GB local and 500GB remote storage, 1 Gbps network bandwidth

Credit Allocation

- **500 Credits**: Credit is only consumed upon completed reservations of *Services* and *Resources*, with the following conditions:
    - Reservations are limited in size (as per service limits) and time.
    - Allocation policies:
        - **First Come First Served**: *Services* and *Resources* are allocated on a first-come, first-served basis.
        - **Use It or Lose It**: *Services* and *Resources* not adequately used (e.g., less than 5% of CPU utilization for 30 consecutive days) may be reclaimed.

3.4. Access Group AP-B (Investigator)

Access Group AP-B includes users authenticated via eduGAIN inter-federation, with the following restrictions:

- **eduGAIN**: IdPs restricted to EU27 and Horizon Europe Associated Countries, filtered for affiliation attributes of *faculty* only (i.e., expected attribute of academic researchers).

Access Rights

In addition to the rights granted to AP-A1 users, AP-B users are granted the following:

- **Access to User Space (full)**: Users have full access to their personalized user space including both application and infrastructure *Services* of the EOSC EU Node.
- **Access to application Services**:
    - **Large File Transfer**: Uses FileSender technology to transfer arbitrary large files via the web.
    - **File Sync and Share**: Uses ownCloud technology to synchronise and share files and folders with collaborators.
    - **Interactive Notebooks**: Uses Jupyter technology giving access to Small, Medium and Large (S/M/L) environments to launch interactive notebooks.
- **Access to infrastructure Services**:
    - **Virtual Machines**: Uses OpenStack technology giving access to Small, Medium and Large (S/M/L) environments to provision compute resources with storage and network.
    - **Cloud Container Platform**: Uses Kubernetes technology giving access to Small, Medium and Large (S/M/L) environments to provision containerised applications.
- **Access to Order Management (Gated Resources)**:

    - **Bulk Data Transfer**: Uses File Transfer Service (FTS) technology to transfer bulk data, transfer sizes to be negotiated on a case-by-case basis.
- **Access to Group Management (team creation)**: Users can create and manage teams/groups for collaborative work.

Service Limits

- **Large File Transfer**: Up to 1TB transfer (upload) per month.
- **File Sync and Share**: Up to 50GB personal storage space.
- **Interactive Notebooks**:
    - Small (S) environment: Up to 2 vCPU with 4GB RAM, 20GB local and 50GB remote storage, 1 Gbps network bandwidth
    - Medium (M) environment: Up to 4 vCPU with 8GB RAM, 100GB local and 200GB remote storage, 10 Gbps network bandwidth
    - Large (L) environment: Up to 8 vCPU with 16GB RAM, 1 GPU with 16GB RAM, 200GB local and 500GB remote storage, 10 Gbps network bandwidth
- **Virtual Machines**:
    - Small (S) environment: Up to 2 vCPU with 8GB RAM, 200GB local and 500GB remote storage, 1 Gbps network bandwidth
    - Medium (M) environment: Up to 8 vCPU with 64GB RAM, 1TB local and 2TB remote storage, 10 Gbps network bandwidth
    - Large (L) environment: Up to 8 vCPU with 32GB RAM, 1 GPU with 16GB RAM, 2TB total storage, 10 Gbps network bandwidth
- **Cloud Container Platform**:
    - Small (S) environment: Up to 2 vCPU with 8GB RAM, 200GB local and 500GB remote storage, 1 Gbps network bandwidth
    - Medium (M) environment: Up to 8 vCPU with 64GB RAM, 1TB local and 2TB remote storage, 10 Gbps network bandwidth
    - Large (L) environment: Up to 8 vCPU with 32GB RAM, 1 GPU with 16GB RAM, 2TB total storage, 10 Gbps network bandwidth
- **Bulk Data Transfer**: Data transfer sizes to be negotiated on a case-by-case basis.
- **Access Group Management (team creation):** User can create at most 2 groups and cannot be a member of more than 4 groups. Unlimited number of authenticated user (AP-A and above) can be invited as a group member. The group members will inherit the Access Rights to existing *Services* and *Resources* of the main AP-B user of the group but cannot initiate any new services.

Credit Allocation

- **1500 Credits: for users.** Credit is consumed upon completed reservations of *Services* and *Resources* with the following conditions:
    - Reservations are limited in size (as per service limits) and time.
    - Allocation policies:
        - **First Come First Served**: *Services* and *Resources* are allocated on a first-come, first-served basis.
        - **Use It or Lose It**: *Services* and *Resources* not adequately used (e.g., less than 5% of CPU utilization for 30 consecutive days) may be reclaimed.

- **3000 Credits: for groups.** Upon the creation of a group, it is automatically assigned regardless of the number of users in the group.

4. Credit Allocation and Replenishment

4.1. Credit Allocation

Credits are virtual, they have no monetary value.

Credits are allocated to users based on their access group policies as follows:
- **AP-0**: Not applicable
- **AP-A**: 0 Credits.
- **AP-A1**: 500 Credits.
- **AP-B**: 1500 Credits for users, 3000 Credits for groups.

The EOSC EU Node does not support automatic transition between these access groups. If users need different access group allocation and access rights, they must issue a Helpdesk ticket.

Users who are authenticated via their eduGAIN/eIDAS inter-federated IdPs that are configured in a way that the EOSC EU Node *is unable to allocate the user in the appropriate access group* (e.g., missing eduPersonAffiliation and/or Domain attributes) shall contact their home IdP operator first before submitting a Helpdesk ticket. Users can review and validate their individual attributes within the Settings page of the User Space.

4.2. Credit Replenishment

Credits are replenished to the default allocation every three months (90 days) period. The period begins when the user logs in to the EOSC EU Node for the first time.

Credits are not transferrable between periods. Unused credits expire at the end of the period.

Reserved service environments are deactivated upon reservation revoked by the owner/user or ended due to credit or time expiration. The infrastructure resources are released/deleted 10 days later. Users are automatically notified 5 days before deactivation (if the reservation was for longer than 5 days).

4.3. Additional Credit Requests

Users requiring additional credits or extended access beyond their default allocation must submit a request through the Helpdesk. These requests will be reviewed on a case-by-case and best-effort basis (i.e. not guaranteed).

4.4. Service Weights and Metrics

The following table outlines the weights and metrics for credit consumption of the native pre-procured *Services* and *Resources* of the EOSC EU Node.

Service	Small	Medium	Large	Metric
Virtual Machines (OpenStack)	10	40	400	Credits per day
Cloud Container Platform (OKD)	10	40	400	Credits per day
Bulk Data Transfer (FTS)		Negotiated		Case by case
Interactive Notebooks (Jupyter)	0.04	0.5	50	Credits per hour
File Sync and Share (ownCloud)		10		Credits per month
Large File Transfer (FileSender)		7		Credits per month

Note that this table *in not applicable to third-party onboarded services and resources*. For information, uses shall visit the user access policies of those third-party providers.

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 user 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. Users will be notified of significant changes and continued use of the *Services* and *Resources* implies acceptance of the updated terms.

Service Updates: The *Operating Unit* may release software updates, including security patches or new features. Users 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 *Services* or *Services features and functionalities* at its discretion. Users may lose access to certain functionalities, *Services* and/or *Resources* (including content and data), 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 Policy of the European Commission referenced below.

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

Any remaining credits or reservations will be forfeited upon termination, and there will be no reimbursement for unused Credits.

7. Computer Security Incident Response

The *Operating Unit* of the EOSC EU Node is committed to ensuring the security and integrity of its *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.

Users 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. Users who fail to follow the security standards applying to all European Commission information systems[8] 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 and organizations in a timely manner. Notifications will include details about the incident, any data compromised, and recommended actions users should take.

8. Disaster Recovery

The *Operating Unit* of the EOSC EU Node is committed to ensuring the continuity and availability of its *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. These backups are securely stored in geographically dispersed locations to ensure data availability in the event of a

[8] Security standards applying to all European Commission information systems: https://commission.europa.eu/publications/security-standards-applying-all-european-commission-information-systems_en

localized disaster. Backup frequency and retention policies are aligned with EU regulations on data protection and disaster recovery.

9. User Responsibilities

9.1. Equipment and Connectivity

Users are responsible for providing the necessary equipment (e.g., internet connection, devices) to access EOSC EU Node's *Services* and *Resources*. The *Operating Unit* is not liable for any additional costs incurred by users for their connectivity or equipment.

9.2. Maintaining backup copies

Users are responsible for maintaining backup copies of any critical content and data they store within the EOSC EU Node's *Services* and *Resources*. Users should follow best practices for data protection and ensure they are aware of the EOSC EU Node's recovery procedures.

9.3. Legal Compliance

Users agree to use the *Services* and *Resources* in compliance with applicable laws and regulations. Misrepresentation of location or identity to bypass service restrictions is prohibited.

For more information, visit the EOSC EU Node Acceptable Use Policy referenced below.

10. Helpdesk Support

Users experiencing issues related to access rights, service limits, or credit allocation (i.e. this User Access Policy – UAP) must contact the Helpdesk. The Helpdesk will handle requests for elevated privileges, additional credits, or access group modifications on a case-by-case and best-effort basis (i.e. not guaranteed).

11. Limitation of Liability

11.1. General Liability

EOSC EU Node provides its services on an "as-is" and "as-available" basis. To the maximum extent permitted by applicable law, the *Operating Unit* of the EOSC EU Node and its affiliated parties (i.e., onboarded 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.

11.2. Service Availability

EOSC EU Node strives to ensure the availability and reliability of its services. However, the *Operating Unit* of the EOSC EU Node makes no guarantees regarding the uninterrupted or error-free operation of its *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.

11.3. Data Integrity

While EOSC EU Node implements strong security measures to protect user data, the *Services* and *Resources* cannot guarantee absolute security. Users 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*.

11.4. Third-Party Services and Resources

EOSC EU Node may integrate with or provide access to third-party services and resources as a federated system of systems. 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 User Access Policy.

11.5. Legal Compliance

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

11.6. 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

- Acceptable Use Policy of the EOSC EU Node: https://open-science-cloud.ec.europa.eu/support/acceptable-use-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 *UAP* is: CNECT-LISO@ec.europa.eu