Discoverer Acceptable Use Policy (AUP)

Rules for lawful, ethical, and secure use of Discoverer and Discoverer+

Version 1.0 · 8 June 2026

Related documents:

- Discoverer Access Policy
- Discoverer Use Policy (DUP)

Veselin Kolev
v.kolev@discoverer.bg

Discoverer Petascale supercomputer
Sofia Tech Park, Sofia, Bulgaria
https://discoverer.bg
https://docs.discoverer.bg

Contents

Preface

Scope of the document

This document defines the acceptable use rules for the Discoverer petascale supercomputer hosted at SofiaTech Park, Sofia, Bulgaria. It applies to all End Users granted access through PetaSC, whether via national calls, EuroHPC allocation, commercial contracts, benchmark or development access, discretionary allocation, or any other authorised access mode described in the Access Policy.

The Discoverer infrastructure comprises two clusters: Discoverer (CPU cluster) and Discoverer+ (GPU cluster). This policy covers use of both unless a section states otherwise.

PetaSC is the consortium that operates the Discoverer petascale supercomputer — both the Discoverer CPU cluster and the Discoverer+ GPU cluster — at SofiaTech Park, including shared storage, access systems, and user support (see §3).

Relationship to other policies

This Acceptable Use Policy (AUP) complements

- the Discoverer Access Policy, which governs how access time is allocated; and
- the Discoverer Use Policy (DUP), which governs day-to-day operational and technical rules (scheduling, storage, backup, retention, software, and similar); and
- the operational documentation at https://docs.discoverer.bg, which all users must follow when accessing the clusters.

In case of conflict, the order of precedence shall be: contractual project agreement, this AUP, the DUP, the documentation at docs.discoverer.bg, and other published operational guidelines, unless mandatory law provides otherwise.

Successful applicants and commercial customers must accept this AUP before receiving system credentials. For allocations submitted through EuroHPC JU allocation portals, acceptance is recorded in the portal application process (§14). For projects allocated directly by PetaSC without such a portal submission, the signature blocks in §14 apply.

1. Introduction

1.1 Purpose

This Acceptable Use Policy defines the rules under which End Users may access Discoverer and Discoverer+. Its purpose is to ensure lawful, ethical, secure, and fair use of a shared public investment in high-performance computing.

1.2 Principles

Use of Discoverer resources should align with the principles of the Discoverer Access Policy and the EuroHPC JU regulatory framework:

- primary use for public research and innovation;
- transparent and equitable allocation through published calls where applicable;
- limited commercial activity within published ceilings and civilian-use restrictions;
- responsible stewardship of shared compute, storage, and network capacity.

1.3 Actors

PetaSC is the consortium that operates the Discoverer petascale supercomputer (Discoverer and Discoverer+). It runs the service through the Discoverer Management Team (DMT), chaired by the chairman of PetaSC. The Operational Manager (OM) oversees day-to-day operations and security; the Business Development Manager (BDM) oversees user onboarding and allocations. Principal Investigators (PIs) represent project teams. End Users are individuals authorised to use the system. Full role descriptions appear in the Access Policy (§2.9).

2. Scope and applicability

2.1 Covered systems and services

This policy applies to all services operated by PetaSC for awarded and commercial users, including:

- Discoverer (CPU cluster) — login nodes, compute nodes, and CPU partitions such as `cn`;
- Discoverer+ (GPU cluster) — login nodes, compute nodes, and GPU partitions such as `common`;
- project and home storage reachable from either cluster;
- data transfer endpoints, support desk, and training materials referenced during onboarding.

Operational details of login paths, authentication, POSIX identities, and directory provisioning are defined in the DUP (§2, §3.6, §3.7, §11.1). Day-to-day procedures and current technical settings are defined in the documentation at docs.discoverer.bg — in particular Access, Onboarding guide, and SSH Security — which every End User is obliged to follow.

2.2 Covered users

This policy binds

- Principal Investigators and Co-Investigators named in access applications or contracts;
- project members granted LDAP accounts under a PI's roster;
- commercial customers and their technical staff;
- service account owners where PetaSC has approved a federation or other non-interactive use (DUP §3.1);
- any person using Discoverer credentials, whether or not they signed this document personally (the PI remains responsible for team conduct).

2.3 Access modes

All access modes described in the Access Policy (§3) — Regular, Benchmark, Development, Fast Track, Commercial, and Discretionary — are subject to this AUP. Mode-specific obligations (publication, payment, reporting) remain as stated in the Access Policy and award letter.

2.4 Duration of applicability

This AUP applies from the date of acceptance until all access credentials are revoked and retention periods for stored data have ended. Provisions on confidentiality, misuse records, and publication acknowledgement survive termination where relevant.

3. Definitions

For the purposes of this policy

- Discoverer — the CPU cluster of the Discoverer supercomputing service, including its login nodes and CPU compute partitions.
- Discoverer+ — the GPU cluster of the service, including its login nodes and GPU compute partitions.
- End User — any person granted an LDAP/POSIX account and authorised to access one or both clusters under an approved allocation or commercial contract.
- LDAP directory — the shared identity store from which both clusters obtain POSIX accounts; PetaSC staff assign the POSIX username and primary group name at onboarding from Given Name and Family Name, or from an anonymised name if requested then only (see DUP §3.6); each user receives a UID and primary GID at creation, both permanently reserved to that username even after cluster access ends; each record includes Given Name, Family Name, and e-mail address (AUP §8.1); supplementary group membership controls cluster entitlement and project access.
- Project POSIX group — a group created in LDAP when a project is onboarded; it owns the project storage directory, and users join a project by becoming members of that group (DUP §3.7).
- Login node — a shared server reachable by SSH; the only permitted user entry point to each cluster; not a personal workstation; local CPU, memory, and I/O are limited and shaped per user account (DUP §11.1–§11.3).
- Principal Investigator (PI) — the person responsible for a project allocation, as defined in the Access Policy.
- Acceptable Use Policy (AUP) — this document.
- Discoverer Use Policy (DUP) — the companion operational policy covering scheduling, storage, login procedures, and related technical rules.
- PetaSC — the consortium that operates the Discoverer petascale supercomputer at SofiaTech Park, comprising the Discoverer (CPU) cluster and the Discoverer+ (GPU) cluster, together with shared storage, identity and access systems, scheduling, and user support. Juridical representation and consortium composition are described in the Access Policy.
- Misuse — use that violates this AUP, the DUP, the Access Policy, or an applicable contract, including the examples in §11.2.
- Open R&I access — non-commercial access where results are published and used for non-profit purposes, as described in the Access Policy.
- Commercial access — paid access where results may remain confidential, subject to

Access Policy §3.6.

4. Permitted use

4.1 General permitted activities

End Users may use Discoverer and Discoverer+ for activities consistent with their access award or contract, including scientific simulation, data analysis, machine learning, algorithm development, benchmarking, visualisation, and preparation of publications or industrial results within agreed confidentiality terms.

4.2 Use aligned with approved project or contract

Workloads and stored data must match the scope described in the approved proposal, technical request, or commercial agreement. Material deviation requires prior written approval from PetaSC.

4.3 Open research and innovation results

For non-commercial access modes, users must publish results within the timeframe stated in the Access Policy and acknowledge EuroHPC and PetaSC resources (§10.1). Results must be used for non-profit purposes unless commercial access terms apply.

4.4 Commercial civilian applications

Commercial access is permitted only for civilian applications. Users must comply with eligibility and embargo rules in Access Policy §3.6 and certify civilian use at onboarding.

5. Prohibited use

5.1 Unlawful activities

Users must not use Discoverer, Discoverer+, or associated storage for any purpose contrary to applicable national, EU, or international law, including downloading or storing illegal content via cluster network access (DUP §10.4).

5.2 Military and weapons-related applications

Users must not use resources for the design, development, or analysis of weapons, military systems, or dual-use applications intended for military end-use. Project results must not be applied to military purposes unless explicitly authorised by law and PetaSC in writing (such authorisation is not expected for standard access modes).

5.3 Activities outside approved scope

Prohibited activities include

- running workloads unrelated to the approved proposal or contract;
- cryptocurrency mining or similar revenue generation not covered by the award;
- personal or recreational use unconnected to the project;
- reselling or sublicensing access;
- storing datasets or software collections unrelated to the granted access purpose.

5.4 Security violations

The following are prohibited

- unauthorised access to Discoverer, Discoverer+, or any PetaSC system;
- sharing SSH private keys, VPN credentials, or LDAP accounts between individuals;
- adding, altering, or removing SSH public keys on Discoverer systems without PetaSC approval (including via `~/.ssh/authorized_keys` or similar);
- attempting password authentication or other credential mechanisms not explicitly authorised by PetaSC;
- connecting to Discoverer login nodes without using the required VPN tunnel, or otherwise circumventing network access controls;
- connecting to Discoverer or Discoverer+ without LDAP group membership authorising that cluster;
- network scanning, soliciting, or attacks from login nodes or compute nodes;
- downloading or distributing illegal content through cluster network access;

- privilege escalation, port scanning, deployment of malware, or denial-of-service activity;
- any action that breaches the security access policy referenced in the Access Policy.

See also DUP §10.4 and §11.1 for cluster network rules and SSH access-path requirements (Access, VPN, SSH Access).

5.5 Unethical conduct

Users must conduct work in line with recognised research ethics and applicable regulatory frameworks, including ethics review requirements of their home institution. Where EU AI Act obligations apply to a workload, users must implement appropriate risk management and documentation.

5.6 Resource abuse

Users must not deliberately degrade service for others through scheduler abuse, storage flooding, excessive load on login nodes or use of login nodes as personal workstations (beyond per-account shaping limits; DUP §11.2, §11.3), runaway job arrays, consumption beyond allocation limits, abusive querying of the SLURM SQL accounting database (DUP §4.8), or misuse of cluster network capacity (DUP §10.4). Operational limits are detailed in the DUP.

5.7 Restricted jurisdictions and embargoed entities

Commercial and other access is not available to persons, organisations, or countries subject to EU embargoes or sanctions that prohibit use of EuroHPC resources, consistent with Access Policy §3.6.

6. User obligations

6.1 Accurate representation of work

Users must not misrepresent project purpose, data sources, or intended results in applications, reports, or communications with PetaSC.

6.2 Credential and account stewardship

Each End User must

- use an individual LDAP/POSIX account with a unique username, UID, and primary GID assigned by PetaSC at onboarding; shared personal accounts are not permitted;
- request anonymised POSIX naming only during onboarding if required; renaming to anonymised or alternative usernames after onboarding is not offered (DUP §3.6);
- protect SSH private keys and VPN credentials; request any add, change, or removal of SSH public keys through PetaSC support and use only keys PetaSC has provisioned (DUP §11.1);
- never modify login authorisation by editing `~/.ssh/authorized_keys` or equivalent on Discoverer systems;
- never share private keys or delegate login to another person;
- use SSH public-key authentication exclusively on login nodes (password authentication is not offered);
- follow the correct access path for each cluster — VPN then SSH for Discoverer, direct SSH for Discoverer+ (DUP §11.1);
- access only clusters for which their LDAP group membership entitles them, and only project directories for which they are members of the project POSIX group (DUP §3.6, §3.7);
- submit jobs only under authorised SLURM project accounts; must not use another project's account to hide usage (DUP §4.7);
- notify PetaSC immediately if a key, VPN credential, or account may have been compromised;
- ensure team members who leave a project are removed promptly from the project POSIX group and other access lists;
- export personal files from the home directory before ceasing membership in all valid projects (DUP §8.5).

The PI is responsible for keeping the project roster accurate so that project POSIX group and LDAP memberships reflect current collaborators, for ensuring project-directory data

are transferred within 30 days after the project end date (DUP §8.4), and for ensuring the team operates within the storage quotas fixed at onboarding from the approved application (DUP §7.2), including internal agreement on how project storage is used.

6.3 Compliance with operational rules

Users must follow this AUP, the DUP, the documentation published at https://docs.discoverer.bg, and reasonable instructions from PetaSC staff acting in an operational or security capacity.

6.4 Collaboration and fair sharing

Users must respect allocation limits so that shared resources remain available to other projects. Non-commercial projects receive equal queue priority under DUP §4.4; users must not attempt to obtain preferential scheduling outside authorised QoS. Within a project, members must stay within the fixed storage quota agreed at onboarding (DUP §7.2) and align internally on how that shared space is used; PetaSC does not resolve disputes over internal project storage sharing.

6.5 Incident reporting

Users must report suspected security incidents, credential compromise, malware, or policy violations to PetaSC without undue delay through the support contact in §13.

6.6 Project reporting obligations

Projects must meet reporting, workshop, and publication obligations stated in the Access Policy (§3.2.4, §4.2) and their award letter, including final reports within published deadlines.

7. Security and access control

7.1 Authentication and authorisation

Login node access is governed by the following mandatory controls (detailed in DUP §11.1 and §3.6):

Authentication

- SSH is the only permitted protocol for interactive access to login nodes;
- only public-key authentication is accepted; password authentication is disabled;
- SSH public keys are registered and maintained by PetaSC in a central system; at rest they are stored as hashes only, to reduce exposure to harvest-now-decrypt-later quantum threats (Quantum-resistant LDAP secure store of public OpenSSH keys);
- they are not user-managed through `~/.ssh/authorized_keys` on login nodes;
- users must request PetaSC approval before adding, changing, or deleting an SSH public key used for login (DUP §11.1);
- PetaSC may change permitted SSH ciphers, public-key algorithms, and hash functions on the server side; users must adapt clients and keys as documented in SSH Security (DUP §11.1).

Procedural guides: Access, Onboarding guide, Login nodes.

Network path

- Discoverer (CPU cluster) — users must connect through an established VPN tunnel to the PetaSC network, then SSH to the Discoverer login node;
- Discoverer+ (GPU cluster) — users SSH directly to the Discoverer+ login node; no VPN is required for this path.

Authorisation

- both clusters use the same LDAP directory; each user has a consistent POSIX username, UID, and primary GID on Discoverer and Discoverer+ (DUP §3.6);
- LDAP group membership, assigned by PetaSC according to the active award or contract, determines which cluster or clusters a user may access;
- project data access requires membership in the project POSIX group that owns the project storage directory (DUP §3.7);
- possession of a valid SSH key does not by itself grant access to a cluster or project without the appropriate group memberships;

- loss of all project and cluster entitlements disables access but does not remove the LDAP account or release the user's UID and primary GID.

End Users must not attempt to bypass these controls. Compute nodes are reachable only through the workload manager, not by direct SSH from users.

7.2 Acceptable network use

Users must not use login nodes or compute nodes for network scanning, soliciting, attacks, or download of illegal content. Unauthorised network services, spam relay, and reconnaissance against PetaSC or external systems from Discoverer infrastructure are prohibited (DUP §10.4).

PetaSC reserves the right to monitor network use on the cluster and to analyse traffic as necessary to protect the platform, detect abuse, and comply with law. Monitoring may include connection metadata and, where justified, traffic content. Users who breach fair use of the cluster network may be sanctioned under §11.3.

7.3 Software installation and supply chain

Users installing software remain responsible for licensing, security patching, and vulnerability of that software. Do not install or execute known malicious code. Container and user software policies appear in DUP §9 and §12.

7.4 Vulnerability disclosure

If a user discovers a vulnerability in PetaSC systems, they must report it promptly to PetaSC and must not exploit it beyond the minimum steps needed to demonstrate the issue.

8. Data protection, confidentiality, and export control

8.1 Personal and sensitive data

PetaSC processes personal data relating to End Users to provision and operate access to Discoverer and Discoverer+.

Account personal data

The LDAP directory described in DUP §3.6 stores the following personal data for each End User account:

- Given Name;
- Family Name;
- e-mail address.

These data are used to identify the account holder, maintain accurate project rosters, deliver operational and security communications, and fulfil reporting obligations under the Access Policy. End Users must provide accurate details at onboarding and notify PetaSC without undue delay if their name or e-mail address changes. Updates to Given Name or Family Name do not alter the POSIX username assigned at onboarding (DUP §3.6).

User workload data

End Users may store and process additional personal or sensitive data within project datasets on Discoverer storage. The PI and each End User remain responsible for ensuring that such processing complies with applicable law (including the GDPR where it applies), that appropriate legal bases and safeguards are in place, and that data are not used on the system beyond the scope of the approved project or contract.

Stored datasets must relate to the granted access purpose. Users are responsible for exporting project data within 30 days after the project end date and home-directory data within 30 days after they no longer belong to any valid project, as defined in DUP §8.4 and §8.5.

PetaSC does not routinely inspect user dataset content. SLURM usage is not anonymised: project account names, limits, and consumption are visible to all users with cluster access (DUP §4.7, §14.1).

Where law, contractual audit rights, or a substantiated security concern requires it, PetaSC may inspect or restrict stored data and may cease storage access as described in §11.3 and DUP §7.6.

Requests regarding access, correction, or erasure of account personal data should be directed to PetaSC using the contact details in §13.

8.2 Confidential commercial data

Commercial customers may process confidential data on Discoverer subject to contract terms. PetaSC implements logical separation through project accounts and access controls but does not provide certified commercial confidentiality regimes unless explicitly agreed in writing.

8.3 Export-controlled technology and data

Users are responsible for identifying export-controlled software or data before transfer to Discoverer. PetaSC may refuse, quarantine, or remove content that violates export-control law or licensing conditions.

8.4 Data location and cross-border transfer

Primary data processing and storage occur in Bulgaria within the PetaSC facility unless otherwise agreed. Users exporting data from Discoverer remain responsible for lawful transfer to their home organisation or collaborators.

9. Commercial access conditions

9.1 Civilian use certification

Commercial users certify at onboarding that workloads are civilian applications only, consistent with Access Policy §3.6.

9.2 Contractual relationship

Commercial access is governed by pay-per-use contracts referencing Access Policy §3.6.1 and §3.8. Service levels and pricing are agreed case by case.

9.3 AUP agreement for commercial customers

Commercial customers must accept this AUP before credentials are issued, using the signature process in §14. PetaSC may audit usage for billing and compliance with civilian-use and security rules.

10. Acknowledgement and reporting

10.1 Publication acknowledgements

Publications and dissemination material must acknowledge use of EuroHPC and PetaSC resources and state the access mode where applicable. A minimum acknowledgement appears in DUP Appendix A; mandatory wording for Union allocations may also appear on Acknowledgements and in EuroHPC call documentation.

10.2 Dissemination and outreach

Where the access mode requires it, PIs must present results at PetaSC workshops or comparable events and support public outreach activities.

10.3 Final and interim reports

PIs must submit final reports using PetaSC or EuroHPC templates within published deadlines (typically within six months of allocation end for Regular access). Failure to report may affect future applications from the same PI or group. Job-level SLURM records may be purged six months after project expiration (DUP §14.5); export accounting data from Accounting before that date if needed for reporting.

11. Monitoring, misuse, and enforcement

11.1 Monitoring

The OM and operational team monitor utilisation, security events, network traffic, and policy compliance through logs, metrics, and filesystem tools. Monitoring is limited to what is necessary for operations, security, and accounting. SLURM accounting and queue information are visible to all authenticated cluster users and are not anonymised by PetaSC (DUP §4.7); see Accounting. Network monitoring on the cluster is described in DUP §10.4.

11.2 Definition of misuse

Misuse includes, without limitation

- significant under-usage of allocation without justification (Access Policy §3.2.4);
- unethical behaviour or breach of this AUP;
- breach of security controls or the Access Policy security provisions;
- running tasks or storing data inconsistent with the approved proposal or contract;
- storing datasets that do not match the purpose of provided access, violate applicable law, or threaten system security;
- scanning or overloading the SLURM SQL accounting database with useless or repetitive queries (DUP §4.8);
- breach of fair use of the cluster network, including scanning, soliciting, attacks, or illegal downloads (DUP §10.4).

11.3 Graduated sanctions

Depending on severity, PetaSC may

- issue a written warning to the PI or user;
- cancel running or pending jobs;
- reduce allocation or scheduling entitlement;
- restrict or cease access to storage for affected datasets or project directories;
- suspend LDAP, VPN, or cluster access temporarily or permanently, including banning users who abuse the SLURM SQL accounting database (DUP §4.8);
- revoke access entirely, as authorised under the Access Policy (§2.8);
- affect future applications from the same PI or group.

PetaSC reserves the right to restrict or cease access to the storage system for data and datasets that do not match the purpose of provided access, that violate applicable law, or

that compromise system security. Such action may include quarantine, read-only lock, or deletion after notice where practicable. Immediate action without prior notice is permitted when required to protect the platform or comply with law.

PetaSC may sanction network abuse without prior notice where immediate action is required to protect the cluster network or external parties (DUP §10.4).

11.4 Appeals

Rejected applicants and users subject to enforcement may request explanation or appeal under procedures published in the relevant call or contract, consistent with Access Policy §2.7.

11.5 Recording and future allocations

Confirmed misuse is recorded and may be considered in future allocation decisions involving the same PI or user group.

12. Changes to this policy

Amendments require approval by the DMT and chairman of PetaSC where material. Updated versions are published on the Discoverer website. Active users are notified of substantive changes.

13. Contact and support

General support and policy questions: contact details on https://discoverer.bg and Getting help.

Operational documentation (mandatory for all users): https://docs.discoverer.bg. A section-by-section index of documentation pages appears in DUP Appendix D.

Support desk hours: at least 8×5 (09:00–17:00 Eastern European Time), per Access Policy §3.8.

Security incidents: report through the support channel with subject line indicating security urgency; escalation to the OM.

Data protection requests relating to account personal data: contact PetaSC using the same support channel.

14. Acceptance and signatures

This section applies to projects allocated directly by PetaSC — for example national calls handled on the Discoverer website, commercial contracts, benchmark or development access, discretionary allocation, or other routes where the application is not submitted through a EuroHPC JU allocation portal.

For allocations awarded after submission through a EuroHPC JU allocation portal, the PI and project team accept this AUP as part of the portal application or award workflow. The signature blocks in §14.1 and §14.2 are not used for those projects; End User obligations in §14.3 still apply when credentials are issued.

14.1 Principal Investigator / authorised signatory

For direct allocations only.

Name

Organisation

Project / account ID

Signature

14.2 PetaSC representative

For direct allocations only.

Name

Role (BDM or delegate)

Signature

14.3 End User acknowledgement

Each End User confirms by receiving credentials or by written roster attestation that they have read this AUP and the DUP, agree to comply, and will follow the operational documentation at https://docs.discoverer.bg. This applies regardless of whether the project was allocated directly or through a EuroHPC JU allocation portal.

Document history

Version	Date	Author	Summary of changes
1.0	8 June 2026	Veselin Kolev <v.kolev@discoverer.bg> on behalf of PetaSC support team	Published: acceptable use rules aligned with DUP and Access Policy; security, storage, and reporting obligations; cross-links to docs.discoverer.bg
1.0	8 June 2026	Veselin Kolev <v.kolev@discoverer.bg> on behalf of PetaSC support team	§14: signature blocks limited to direct PetaSC allocations; EuroHPC portal submissions accept AUP through portal workflow