PURPOSE

This policy establishes the framework for fair and responsible access to the Cyprus Marine and Maritime Institute (CMMI) Research Infrastructure (RI). It reflects CMMI's commitment to open access to publicly funded research infrastructures including complying with applicable laws, policies and governing regulations. By providing clear guidelines and expectations for users, collaborators, employees, and third parties, this policy promotes transparency, collaboration, and the responsible use of the CMMI infrastructure. This policy is aligned and linked with the CMMI Open Science Policy and is fully aligned with other relevant CMMI policies. Specific terms and conditions apply to each part of the open-access infrastructure. This Policy also implements the Deputy Ministry of Research, Innovation and Digital Policy (DMRIDP) Guidance for Open Access Policies for Publicly Funded Research and Technology Infrastructures. For CMMI RI components that have been developed, operated or upgraded through public funding, this Policy constitutes CMMI's Institutional Open Access Policy under the national framework.

The Policy is published on CMMI's official website and on the National Electronic Research Infrastructure Registry Platform (CRI). Operational details that could compromise security, cybersecurity, safety, export-control compliance, confidentiality, commercial sensitivity or the integrity of controlled infrastructure may be maintained in internal or component-specific procedures, while still providing sufficient public information for users to understand how to request access.

The policy offers an overview of the prevailing regulatory framework for granting access to internal and external users. It is designed to facilitate innovative research and development, enhance workforce skills, and foster collaboration. Additionally, the policy aims to encourage interaction across a broad spectrum of social and economic activities, including business, industry, and public services, to maximize the return on investment in the CMMI Research Infrastructure and drive innovation, competitiveness, and efficiency.

Research Infrastructures are at the core of the knowledge triangle of research, education, and innovation, playing vital roles in advancing knowledge, developing technology, and applying both for practical applications. By offering access to high-quality services, engaging researchers and innovators, attracting new users, and preparing the next generation of researchers, the infrastructure significantly contributes to building an efficient research and innovation environment in Cyprus, Europe and the wider region. Access to the CMMI Research Infrastructure entails legitimate and authorized use of its services, which may be provided through physical or digital facilities and via physical, remote, or virtual access modes. Open access under this Policy means open, fair, transparent, documented and rules-based access through predefined procedures. It does not mean unlimited, unconditional, unsupervised or free access. Access remains subject to availability, technical feasibility, safety, ethics, data protection, intellectual property, confidentiality, research security, legal compliance, state-aid requirements and financially sustainable operation. The following sections set out the applicable principles, governance arrangements, procedures and safeguards for such access.

SCOPE

This policy applies to all users of the CMMI Research Infrastructure, including CMMI staff, and where relevant, external researchers from academia and research institutions, industry partners, startups and small-to-medium enterprises (SMEs), public authorities and policymakers, civil society organizations, and other stakeholders. The infrastructure supports a diverse range of activities such as research, development, training, testing, validation, and commercialization efforts. It provides users with physical and where appropriate, remote, and virtual access to state-of-the-art facilities, advanced equipment, comprehensive data repositories, and interactive digital platforms.

This Policy applies to all CMMI research and technological infrastructure components, resources and services that are publicly funded or made available for external access, including physical facilities, scientific equipment, digital infrastructure and platforms, scientific data generated or held by CMMI, technical and scientific support services, testing, validation, analysis, certification-related services, training, and other infrastructure-enabled services.

CMMI maintains component-specific access procedures for major RI components or services. These procedures translate this Policy into operational rules for each infrastructure component, including service description, technical specifications, access units, exact contact point, application route, scheduling, user training, safety requirements, cost/rate card, data/IP conditions, and any justified restrictions or controlled-access measures. This Policy sets the common institutional provisions; component-specific procedures provide the detailed implementation.

Access to the infrastructure is governed by the principles and operational controls set out in this Policy and remains subject to CMMI's capacity, legal/ethical compliance, and financially sustainable arrangements (e.g., access fees, project funding, or agreed in-kind support that contribute to full economic costs). This policy is fully aligned with EU and international regulations, including the European Charter for Access to Research Infrastructures, and also ensures that users adhere to CMMI's standards on data protection, ethical research practices, safety and responsible use. By fostering collaboration across sectors and disciplines, the CMMI Research Infrastructure promotes an inclusive, innovative, and efficient research environment.

DEFINITIONS

Research Infrastructure (RI): Facilities and resources supporting marine and maritime research, including laboratories, vessels, data centres, and digital platforms.

Users: Individuals or organizations utilizing the RI for research, development, or educational purposes.

Access: Authorized use of the RI, which may be physical, remote, or virtual.

Access Unit: Metrics defining usage, such as processing time, data exchange, or resource engagement.

Sensitivity Level (of RI components): A risk-informed classification used to determine proportionate access conditions and safeguards for different infrastructure components and services.

Standard-access component: RI component/service presenting no elevated security, export-control, or confidentiality exposure beyond standard operational controls.

Elevated-sensitivity component: RI component/service where additional safeguards are justified due to dual-use potential, sensitive data, critical infrastructure relevance, or increased confidentiality/ commercial sensitivity.

High-sensitivity / controlled component: RI component/service where controlled access is necessary due to classified or security-sensitive information, high dual-use exposure, export-control or sanctions risks, or other legal/public-order constraints.

Publicly funded Research Infrastructure: A CMMI RI component, resource or service developed, operated, upgraded or supported through public funding, including institutional, national or European funding, and therefore subject to the principles of transparent and equitable access set out in the national framework.

Component-specific procedure: A public or controlled operational document, service page, rate card or access protocol that applies this Policy to a specific RI component, service, platform, dataset or equipment item.

CRI Platform: The National Electronic Research Infrastructure Registry Platform (www.cri.gov.cy), through which public information on eligible research infrastructures and access routes may be published and maintained.

RI Access Manager: The institutional role or function responsible for coordinating implementation of this Policy, maintaining access governance, ensuring publication/update of access information, overseeing monitoring data and coordinating escalation where needed. The Policy assigns responsibilities to roles; named individuals and contact details may be published in CRI entries and component-specific procedures and updated without requiring amendment of this Policy.

Access Contact Point: The role, mailbox or named contact for a specific RI component or service, responsible for receiving enquiries, supporting applicants and coordinating the applicable access procedure. RI components or services are assigned a dedicated email address monitored by the named contact.

Access Request: A request by an internal or external user for access to an RI component, service, dataset, platform, staff expertise or access unit under this Policy.

Reasoned decision: A written decision approving, conditionally approving or refusing an access request, including a brief explanation of the main reasons, conditions, timing, pricing basis and any

applicable restrictions, to the extent disclosure is lawful and compatible with confidentiality and security requirements.

Working days: Business days in Cyprus, excluding weekends and public holidays, unless the applicable component-specific procedure states otherwise.

GUIDING PRINCIPLES

The guiding principles of the Cyprus Marine and Maritime Institute (CMMI) Research Infrastructure Open Access Policy are aligned with the European Charter for Access to Research Infrastructures [1] and the National Policy of the Republic of Cyprus for Open Science Practices [2]. This Charter sets out non-regulatory principles and guidelines to be used as a reference when defining access policies for Research Infrastructures and related services.

These principles support transparent, lawful, safe and responsible access to the CMMI Research Infrastructure, while remaining compliant with legal, ethical, safety, and research security requirements. They support the free circulation of researchers and knowledge, and foster collaboration and transparency, with open access to data and research outputs where lawful and appropriate [3].

The specific guiding principles of CMMI's Open Access Policy include:

Fairness: Ensuring equitable access, usage, and sharing of data resources, promoting collaboration, transparency, and responsible data management practices among all users.
Openness: Fostering a collaborative environment that encourages the free exchange of ideas, knowledge, and resources, enabling innovation, transparency, and broad access to data and research outputs.
Non-Discrimination: In granting access to users, CMMI shall not discriminate on any grounds.
Legal Conformity: When providing access to CMMI's research infrastructure, compliance with national and international laws and agreements, particularly in areas such as intellectual property rights, protection of privacy, ethical considerations, safety, security, and public order, will be secured.
Research Security and Strategic Autonomy: Applying precise and proportionate safeguarding measures that keep access open and safe, using risk-based governance for sensitive components while upholding openness, academic freedom, legal conformity and the principles set out in this Policy.
Transparency: Publishing clear information on available infrastructure, access routes, assessment criteria, pricing approach, response times and basic terms of use, while protecting sensitive details where justified.
Equal Treatment and Objective Assessment: Applying objective, predefined and proportionate criteria to comparable requests and avoiding unjustified differences in treatment between eligible users.

Proportionality: Tailoring requirements, due diligence, pricing, documentation, security measures and access restrictions to the type of infrastructure, purpose of use, risk profile, resource demand and legal obligations.
Accountability: Keeping appropriate records of access requests, assessments, reasons for decisions, use of infrastructure, outputs and revenues, and using those records for internal management, auditability and national reporting where required.
Sustainability: Ensuring that access arrangements protect the safe, effective and financially sustainable operation, maintenance and development of the infrastructure and do not undermine CMMI's mission or contractual obligations.
Open Science and FAIR-oriented Data: Supporting open science, acknowledgement of infrastructure use, publication of non-proprietary outputs and FAIR data practices where lawful, ethical, technically feasible and compatible with confidentiality, IP and security obligations.

USERS

The users of the CMMI Research Infrastructure encompass a diverse group of individuals, teams, and institutions spanning academia, industry, business, public services, defence and security bodies, and civil society. Specifically, the infrastructure serves stakeholders such as marine and maritime companies, ports, marinas, law enforcement agencies, public authorities, startups, small-to-medium enterprises (SMEs), and members of the broader research and innovation community.
Specifically, eligible user categories may include, where applicable: public or private academic institutions, centres of excellence, research institutes, public research organisations, enterprises, start-ups and SMEs, public organisations and authorities, non-profit organisations, international organisations or research networks, individual researchers, civil society organisations, and other stakeholders whose proposed use is lawful, feasible and aligned with the applicable access route.

Eligibility and prioritisation is not be based solely on the identity of the user. CMMI will primarily consider the purpose of use, scientific/technical quality, expected public, scientific, economic or technological value, feasibility, resource availability, user readiness, safety, ethics, data protection, confidentiality, research security and the financial sustainability of the proposed access.

Users engage in activities that include, but are not limited to, the conception and creation of new knowledge, development of innovative products, processes, methods, and systems, and the management and execution of research projects. Research teams may consist of experienced researchers, doctoral candidates, technical staff, and students contributing to academic and practical advancements within their areas of expertise. Startups and SMEs benefit from access to state-of-the-art facilities for developing, testing, and validating their innovations, while marine and maritime organizations, including ports and marinas, gain access to advanced tools and data to enhance operational efficiency and sustainability.

The infrastructure also supports public authorities and law enforcement agencies by providing intelligent systems and tools for monitoring incidents and improving maritime safety and security. Dedicated testbeds are available for validating the requirements of end users and public authorities, ensuring that solutions are tailored to address their specific operational needs. Researchers will play a critical role in conducting this validation work, applying their expertise to ensure the robustness, reliability, and practical utility of the solutions developed within the infrastructure. By fostering collaboration among diverse user groups, the CMMI Research Infrastructure supports innovation, workforce development, and the advancement of sustainable practices in marine and maritime activities, ultimately enhancing the economic, social, and environmental impact of the sector.

ACCESS

Access to the CMMI Research Infrastructure (RI) encompasses the legitimate and authorized use of its resources, offered in physical, remote, or virtual formats. The infrastructure supports a broad spectrum of activities, providing users with access to advanced facilities, computational tools, datasets, training opportunities, and expert support. Designed to foster collaboration and innovation, access is granted transparently and equitably to eligible users, ensuring alignment with the infrastructure's policies, ethical standards, and operational guidelines. Detailed frameworks, including specific access modes, units, and associated fees, are outlined in subsequent sections to provide a comprehensive understanding of how users can engage with the infrastructure effectively and responsibly. Over time, CMMI will develop a component-specific framework for each major piece of its research infrastructure, which will be shared with potential users in addition to this policy, to enable users to develop their requests, for CMMI to evaluate, and ultimately form service agreements for the desired services together.

Access Modes

The CMMI Research Infrastructure (RI) offers two primary access modes to ensure fair and efficient utilization of its resources: Excellence, and Market-Driven Access outlined further below. Access requests will be mapped, where relevant, to the following purpose-based access channels: (a) non-proprietary/open research access for non-commercial research and innovation, normally linked to publication, acknowledgement and FAIR-oriented practices; (b) strategic or public-interest access for public policy, civil protection, regulatory support, national priorities or documented high-public-benefit needs; (c) service access with cost recovery for analyses, testing, training, data processing or other services delivered through defined access units; and (d) proprietary/commercial access for confidential projects, product development or use without an obligation to publish, subject to full or commercial charging and clear IP, confidentiality and liability terms.

Component-specific procedures state which access channels are available for each RI component, the applicable access units, whether access is physical, remote or virtual, and any specific limits, prerequisites or booking rules.

Excellence-Driven Access: This mode prioritizes high-quality, innovative research based on scientific merit, originality, and collaborative potential. Users are granted access to the best facilities, resources, and services available, enabling groundbreaking research and technological development across geographical and disciplinary boundaries. Excellence-driven access is designed to support not-for-profit organizations, academia, and public authorities, subject to agreements with CMMI that outline the specific terms of access and confirm how full economic costs (including relevant overheads) will be covered (e.g., via project funding, institutional support, or agreed in-kind contributions). Evaluation criteria include the scientific and technical quality of the proposed work, as well as its feasibility, safety, and ethical compliance.

Market-Driven Access: This mode ensures open and equitable access to all users, subject to CMMI's capacity, safety, and compliance requirements. In cases of resource constraints or high demand, prioritisation is be applied in accordance with published, objective and proportionate criteria, first taking into account legal, safety, public-interest, existing contractual, mission-critical and technical constraints. Funding at full commercial rates may be considered only within the market-driven/proprietary channel and only where it is consistent with equal treatment, state-aid rules, and sustainable use of the infrastructure. Market-driven access operates transparently, with users informed of any changes to access conditions in advance. Strategic discounts or "loss-leader" arrangements may be considered only where there is a clear, documented mutual benefit and an approved plan for sustainable value creation.

Evaluation criteria will include feasibility, safety, ethical compliance, and strategic considerations related to the Infrastructure's sustainable growth and CMMI's research and innovation priorities. Capacity management measures may be applied (e.g., scheduling windows, quotas, supervised use, or prioritisation rules) to protect assets and deliver services effectively. In the case of overlapping requests, CMMI will make every effort to accommodate all parties, but will prioritise according to its strategic objectives if this is not possible.

Access Units

Access Units are measurable components that define the extent of access provided to users within the CMMI Research Infrastructure (RI). These units ensure fair and efficient allocation of resources, enabling optimal utilization of the infrastructure while maintaining transparency and equity among users.

Access Units serve as a standardized framework to:

- **Facilitate Resource Allocation:** Ensure that resources are distributed equitably among users, avoiding overuse or underutilization.
- **Monitor Utilization:** Provide a clear and measurable method for tracking how resources are used across different projects.
- **Support Planning and Costing:** Help users and administrators plan resource requirements and associated costs effectively.

Access Units include:

Usage Time:

- Hours or sessions dedicated to using computational resources, including high-performance computing (HPC) systems, simulation tools, and data processing or extraction pipelines.
- Experimental time in laboratories, testing facilities, or other physical infrastructure. Use of physical spaces such as laboratories, meeting rooms, or collaborative workstations.
- Rental time of physical equipment, such as sensors, experimental tools, or maritime-specific hardware (e.g., underwater ROVs, drones). For high-value, high-risk, or safety-critical assets, access may be limited to operation by trained CMMI personnel or require close supervision, with CMMI maintaining control of assets at all times. For externally operated equipment, CMMI may require the provision of a refundable security deposit, bank guarantee, or equivalent financial safeguard to cover potential damage, loss, or misuse. Users may also be required to demonstrate adequate insurance coverage (e.g., public liability, professional indemnity, and/or equipment insurance), naming CMMI as additional insured where appropriate. All rental agreements will clearly define liability, responsibility for consumables, repair or replacement costs, downtime losses, and compliance with safety and regulatory requirements.
- Usage time of specialized infrastructure like IoT-enabled systems, measurement devices, or analytical tools.

Physical Samples, Archives and Collections:

- Number of physical samples/artefacts curated and the associated storage period and handling requirements.
- Number of retrieval, analysis, transfer, or disposal requests, including any chain-of-custody requirements where relevant.

Data Volume:

- Volume of data transferred, including data ingestion, processing, and retrieval.
- Volume of data accessed, generated by CMMI (e.g., historical, environmental, or operational data).

Data Storage and Management:

- Volume and Time of storage for user-generated or shared data, including cloud-based repositories.
- Volume and Time of archival services for long-term preservation of research outputs.

License Units (Software, Digital Models, Algorithms, Platforms and Applications):

- Number of licenses to access proprietary or licensed software tools, such as simulation

and modelling platforms.
- Number of uses of digital twins or virtual environments for experimentation and training.
- Number of deployments of pre-trained machine learning (ML) models tailored to maritime or environmental applications.
- Number of developed or customized ML models or algorithms for user-specific needs.
- Number of digital platforms for remote collaboration, data visualization, and project management.

Human Resources and Expertise:

- Person-months (PMs) of CMMI staff for consultation and support, including technical guidance, dedicated project support, mentorship for research activities, training, and domain-specific expertise.

Network and Communication Services:

- Number of users who access CMMI-operated secure communication channels, including remote systems for data transfer and real-time collaboration.
- Number of users of networked infrastructure for multi-stakeholder projects or geographically dispersed teams.

Licensing and Intellectual Property Services:

- Number of sessions to consult on usage rights for proprietary CMMI resources, including data, models, or patents.
- Number of sessions to support navigating licensing agreements and intellectual property management.

Access Fees

Access to the infrastructure will be provided based on specific agreements between the parties involved. These agreements will be based on the principles laid out here, as well as component-specific frameworks if they exist, and will specify the applicable access units, conditions (including safety and research-security safeguards), and the financial model through which full economic costs are covered (fees, project funding, or other agreed arrangements). All terms and conditions associated with the use of the infrastructure will be transparent and publicly available.

CMMI may apply full pricing, partial pricing or zero direct charge, depending on the access channel, user category where relevant, type of service or equipment, operational cost, consumables, required technical support, duration of use, source of funding and documented strategic or public-interest considerations. Any partial or zero-charge access must be justified, documented and compatible with funding conditions, state-aid rules, competition law and the prohibition of duplicate funding.

Pricing shall be based on a documented costing methodology. Component-specific procedures or rate cards shall identify the relevant access units and, where possible, published rates or the basis for calculating costs. CMMI shall maintain appropriate accounting separation between economic and non-economic activities where required to comply with applicable State aid rules and shall ensure that economic activities are not cross-subsidised in breach of legal requirements.

All access must be financially sustainable. In the case of paid access, the user will be charged a fee that is clearly linked to the actual use of the infrastructure itself. For excellence-driven access, costs are normally covered through project funding or institutional support. In specific cases, access may be provided with no direct payment where there is a documented, mutually beneficial arrangement that covers costs and creates value (e.g., data provision to universities with mandatory acknowledgement/citation and promotion of the infrastructure, or co-development of innovative work that can later be exploited for impact and income).

Access fees will abide by the following principles:

- Auditability, including the full economic costs of the activities including space, staff, direct equipment costs, amortization, maintenance, training, and associated technical developments
- traceability to the work done on the infrastructure, including maintaining appropriate records outlining access requests (successful and unsuccessful), reasons for declining access (if relevant), usage data, etc.,
- prohibition of duplicate funding,
- compliance with all relevant national and EU funding terms and conditions and with competition legislation.

Market-driven and proprietary/commercial access will normally be recovered at full commercial rates or at least full economic cost, unless a documented and legally compliant partial-charge, zero-direct-charge or project-funded arrangement is approved for strategic, public-interest or value-creating reasons. The unit of cost depends on the relevant access unit and the component-specific costing methodology.

As the CMMI Research Infrastructure scales, CMMI may introduce a tiered service catalogue and pricing structure to reflect different levels of features, resources, and support. Any tier definitions, eligibility rules, and associated costs will be maintained in component-specific documentation and introduced only once capacity management processes, and the cost model (including full economic costs) are sufficiently mature.

RESTRICTIONS

In conformity with the “As open as possible, as closed as necessary” principle of Open Science, access to the infrastructure may be limited where justified by a structured, risk-based governance mechanism

and applicable laws. Restrictions may arise from research security considerations (including prevention of undesirable knowledge transfer and foreign interference), national security and defence, privacy and confidentiality, commercial sensitivity, intellectual property rights, and ethical considerations. Where restrictions apply, CMMI will implement proportionate safeguards aligned with EU research security expectations, and will document the rationale, measures applied, and (where feasible) routes for compliant access.

Any restriction or exception to access shall be objective, proportionate, documented and linked to the nature of the infrastructure or the proposed use. Examples include safety or protection of critical infrastructure, personal data or confidential information, limited availability of resources, technical limits of equipment, user certification requirements, operation only by specialised CMMI personnel, prioritisation rules, cybersecurity, export control, sanctions/restrictive measures, ethical constraints, IP rights, contractual obligations, and sustainability of operation.

Where access is refused or limited, CMMI shall provide a reasoned decision to the applicant to the extent lawful and compatible with confidentiality, security and third-party rights. Where feasible, CMMI may suggest alternative timing, supervised use, modified scope, remote or virtual access, referral to another RI component, or other proportionate measures.

- Purpose of use: Access to the research infrastructure and data may be restricted to certain research purposes. For example, access may be limited to non-commercial research only.
- Data sharing: The research infrastructure may restrict the sharing of data among users.
- Access duration: The research infrastructure may limit the duration of access for each user. For example, users may be granted access for a limited period of time.
- Usage quotas: The research infrastructure may impose usage quotas on users. For example, users may be limited to a certain amount of data storage or processing time.
- Compliance with policies: The research infrastructure may require users to comply with certain policies, such as data security and privacy policies.

RESEARCH SECURITY AND CONTROLLED ACCESS GOVERNANCE

CMMI is committed to keeping access to its Research Infrastructure open to wider access, while applying precise and proportionate safeguards where risks to research security, integrity, or lawful use are identified. Safeguards are applied based on the sensitivity of the infrastructure component/service, the nature of the proposed activity, and applicable legal and regulatory obligations, not on personal characteristics.

1. Sensitivity classification of RI components

CMMI may classify RI components and services into (i) Standard-access, (ii) Elevated-sensitivity, and (iii) High-sensitivity/Controlled categories. The classification is reviewed periodically and may be updated as technologies, legal requirements, and risk contexts evolve. Access conditions, monitoring, and contractual clauses shall be proportionate to the assigned sensitivity level.

2. Risk-based due diligence and compliance checks (where applicable)

For Elevated-sensitivity and High-sensitivity/Controlled components, CMMI may require additional due diligence prior to granting access, in line with a risk appraisal approach. This may include: (a) screening for applicable restrictive measures and sanctions obligations; (b) export-control and dual-use exposure assessment for goods, software, technology or technical assistance (including intangible transfers); (c) transparency on organisational ownership and beneficial control for market-driven access and commercial engagements; (d) assessment of end-use/end-user risks and links that may increase exposure (e.g., military or intelligence affiliations) where relevant to legal compliance; and (e) review of information security, data protection, and confidentiality arrangements.

These checks are procedural safeguards that support legal conformity, protect institutional integrity, and keep collaboration open and safe.

3. Controlled access measures

Where justified, controlled access measures may include: need-to-know and role-based access controls, user identity verification and authentication (including multi-factor authentication for digital services), secure environments for processing sensitive data, segmentation of networks and datasets, logging and audit trails, and specific contractual terms on publication, data sharing, and dissemination.

4. Escalation and decision-making

Requests involving Elevated-sensitivity or High-sensitivity/Controlled components may be escalated for internal review (e.g., Legal/Compliance, Information Security, Ethics/Safety, and Research Leadership). Where required by EU or national frameworks, security-sensitive projects may be subject to additional procedures (e.g., security self-assessment and handling rules for classified or security-sensitive information). Decisions, conditions, and reasons for restrictions will be recorded for auditability and transparency.

5. Alignment with CMMI frameworks

This policy is aligned with the CMMI Open Science Policy and shall be implemented consistently with CMMI's research security governance instruments (e.g., a Research Security Framework/roadmap) once formally adopted. Open access remains the default. Controlled access is applied proportionately where justified.

ACCESS GOVERNANCE, ACCOUNTABILITY AND MONITORING

CMMI has a designated RI Access Manager who oversees the implementation of this Policy. The Policy does not depend on a single named individual; names, email addresses and telephone numbers may be maintained in CRI entries, website pages and component-specific procedures so they can be updated without a formal policy amendment.

Each major RI component or service made available to external users has an Access Contact Point. The contact point supports enquiries, guides users to the correct application route, coordinates completeness checks, and liaises with scientific, technical, legal, safety, data protection, finance and research-security functions where needed.

CMMI has established a RI infrastructure components Access Committee to collectively assess the demand, complexity, sensitivity or capacity constraints of access to CMMI-based RI. This committee may provide scientific, technical, feasibility, safety, ethics, data/IP, pricing or research-security input, although final authority follows CMMI's internal delegations of authority.

For transparency and accountability, CMMI maintains records of access requests, approvals, conditional approvals, refusals, reasons for decisions, response times, access units used, incidents, deviations, user feedback, outputs and revenues, subject to confidentiality, data protection and commercial-sensitivity requirements.

CMMI shall monitor, where applicable, the number of access requests, number of external users, infrastructure use time or access units, collaborations with enterprises or public organisations, publications and other outputs, revenue from services, use of public-interest access, and any other indicators required for internal KPIs or national reporting.

CMMI periodically reviews the accuracy of information published on its website and on CRI. Component owners will provide updates when infrastructure capabilities, availability, pricing basis, contact points, access conditions or restrictions materially change.

USER RIGHTS AND RESPONSIBILITIES

Acknowledgement and co-authorship

Users should acknowledge the contribution of the Research Infrastructure in any output (i.e. publication, patent, data, etc.) deriving from research conducted within its realms. In accordance with good scientific practice, Users are encouraged to offer co-authorship to those working at the Research Infrastructure and having made genuine scientific contributions to their work.

More specifically:

- Proper acknowledgement of the research infrastructure (including where appropriate acknowledgement of the support that enabled the RI acquisition) should be included in all dissemination forms, including publications, presentations, and articles, to recognize the support and resources provided by the infrastructure.
- The research infrastructure will provide training and resources to users on intellectual property rights and responsibilities, including best practices for acknowledging and giving credit to data and resource providers. This may include organizing workshops, seminars, and other communication channels to facilitate collaboration and knowledge sharing between users and resource providers.

- Users who significantly contribute to the development of the research infrastructure may be eligible for co-authorship, based on the extent of their contribution and intellectual input. This provides recognition for the user's contributions to the infrastructure's development and enhances their own professional reputation.

Ethical conduct and research integrity

Research Infrastructures and Users should undertake the necessary actions to adhere to the standard codes of conduct and ethical behaviour in scientific research and to research integrity.
More specifically:
- All users are required to comply with ethical guidelines and standards for research.
- The Research Infrastructure will provide training and education on ethical conduct and research integrity to all users. The training will cover topics such as data sharing, data management, storage, and responsible authorship. The training may include instructions on anonymization, encryption, and backup procedures.
- The Research Infrastructure will ensure that all research conducted by users adheres to applicable laws and regulations.
- All users will be required to implement appropriate measures to protect against data breaches or other security incidents.
- The Research Infrastructure will encourage users to engage in responsible and transparent research practices, such as pre-registering study designs, ensuring that data and methods are available for independent review, and sharing results openly and promptly.

User instruction

CMMI will provide the Users with instructions for effective, efficient and safe access to the research infrastructure, including mandatory induction/training and signed risk assessments where applicable.
More specifically the research infrastructure will:
-Require and offer user training on the safe and efficient use of the infrastructure resources, ensuring that users can utilize the infrastructure effectively.
-Develop and provide user manuals, risk assessments and other instructional materials to supplement the training provided which will be easily accessible by all users for future reference.
-Require users to use the infrastructure and its services in a responsible and ethical manner, adhering to the standards of conduct and ethical behaviour in scientific research and research integrity. Users must not undertake activities that may put the infrastructure or its services at risk or jeopardize the safety or privacy of other users or stakeholders.

Quality assurance

1. Purpose
The purpose of this Quality Assurance (QA) Section is to establish guidelines and best practices to ensure the high quality, accuracy, and reliability of data, research outputs, and services provided through the CMMI Research Infrastructure (RI). By fostering a culture of continuous improvement,

collaboration, and excellence, this section aims to uphold the standards of the CMMI community and its contributions to the research and innovation ecosystem.

2. Scope

This QA Section applies to all users, collaborators, employees, and third parties who access, manage, or contribute to the CMMI RI. The scope encompasses all activities conducted within or utilizing the infrastructure, ensuring compliance with quality standards and alignment with institutional goals.

3. Quality Assurance Principles

a. Commitment to Quality: All individuals and organizations engaging with the CMMI RI must strive for excellence and maintain high-quality standards by adhering to established guidelines, policies, and best practices.
b. Continuous Improvement: Users and stakeholders are encouraged to actively identify and pursue opportunities for innovation and improvement. Feedback, lessons learned, and adapting to challenges are key components of this principle.
c. Collaboration and Communication: Effective communication and collaboration among users, staff, and stakeholders are essential for ensuring the infrastructure's effectiveness. Users are encouraged to share expertise, seek guidance, and work together to uphold quality standards.

4. Quality Assurance Guidelines

a. Data Quality: Users must ensure the accuracy, reliability, and completeness of data generated, processed, or shared within the infrastructure. This includes verifying data sources, validating processing methods, and transparently documenting any limitations or uncertainties.

b. Research Outputs Quality: Research activities conducted within the CMMI RI must adhere to rigorous methodologies, ethical standards, and best practices. Outputs should be transparent, reproducible, and where applicable, subjected to peer review.

c. Software Quality: Software developed or utilized within the infrastructure must meet high standards of reliability, security, efficiency, and usability. This includes adherence to software development processes, thorough testing and validation, and prompt resolution of identified vulnerabilities.

d. Service Quality: Services provided through the infrastructure, including technical support, training, and consulting, must be professional, responsive, and aligned with user needs and expectations.

5. Quality Assurance Monitoring and Evaluation

a. Performance Metrics: CMMI will establish and monitor key performance indicators to

evaluate the quality of its infrastructure, including data, research outputs, software, and services.

b. Feedback and Reviews: Users are encouraged to provide constructive feedback and participate in periodic reviews of the infrastructure, identifying areas for enhancement and ensuring adherence to quality standards.

c. Audits and Assessments: CMMI will conduct regular audits and assessments, both internally and through external experts, to ensure compliance with this QA Section and to identify opportunities for improvement.

6. Enforcement and Sanctions

CMMI insists that all users and stakeholders comply with the QA guidelines. Violations of these standards may result in:

- Suspension or termination of access to the CMMI RI.
- Disciplinary actions, including legal consequences where applicable.
- Other sanctions as deemed appropriate by CMMI leadership.

By adhering to these quality assurance measures, the CMMI RI ensures its infrastructure remains a safe, reliable and effective resource for advancing research, innovation, and collaboration.

Safety rules for using the infrastructure

1. Purpose

The purpose of this Safety Rules Section is to establish comprehensive guidelines and best practices for ensuring the safe and secure use of the CMMI Research Infrastructure (RI). This section aims to prevent accidents, minimize risks, and promote a culture of safety and responsibility among all users, collaborators, employees, and third parties engaging with the infrastructure.

2. Scope

This Safety Rules Section applies to all individuals and organizations accessing or utilizing the CMMI RI, including its physical facilities, hardware, software, networks, and digital platforms. It covers all aspects of infrastructure use to ensure safety, security, and adherence to established protocols.

3. General Safety Guidelines

a. Compliance with Laws and Regulations: Users must adhere to all applicable health, safety, environmental, and regulatory standards when accessing the CMMI infrastructure. This includes compliance with institutional policies and relevant industry best practices.

b. Training and Awareness: Users are required to complete mandatory safety training sessions and remain informed about relevant guidelines, procedures, and updates provided by CMMI. They must complete (and sign) approved risk assessments for the activities they are to undertake.

c. Incident Reporting: Any accidents, injuries, or safety hazards must be reported promptly to the appropriate CMMI authority, following the procedures outlined in the safety protocol.

d. Personal Responsibility: Users are responsible for ensuring their safety and taking precautions to minimize risks to others while using the infrastructure. This includes acting in accordance with provided training and exercising vigilance during all activities.

4. Specific Safety Rules

a. Workspace Safety: Users must maintain a clean and hazard-free workspace, ensuring proper organization and adherence to ergonomic practices. Potential hazards, such as obstructed pathways or improperly stored equipment, should be addressed immediately.

b. Electrical Safety: Electrical systems must be used responsibly, following guidelines such as avoiding overloaded power outlets, using surge protectors, and refraining from using damaged cables or equipment.

c. Equipment Safety: Infrastructure equipment, including hardware and peripherals, must be handled carefully and responsibly. Users should follow manufacturer guidelines and CMMI policies to prevent damage and ensure safety.

d. Network and Data Security: Users must comply with CMMI's data security policies, which include using strong passwords, keeping software updated, and safeguarding against unauthorized access and cyber threats. Any suspicious activity must be reported immediately.

e. Emergency Procedures: All users must familiarize themselves with emergency protocols and evacuation plans specific to their location. In the event of an emergency, users are expected to act promptly and in accordance with established procedures.

5. Enforcement and Sanctions

CMMI is committed to enforcing these safety rules to ensure the well-being of all individuals and the integrity of the infrastructure. Violations may result in:

- Immediate suspension or termination of access to the infrastructure.
- Disciplinary actions, including legal consequences where applicable.
- Other sanctions as deemed appropriate by CMMI management.

DATA MANAGEMENT, FAIR PRINCIPLES, GDPR AND PUBLICATION CONDITIONS

CMMI will define, in the applicable access agreement or component-specific procedure, the ownership of results, rights to use data, rights to publish, confidentiality obligations, permitted use of CMMI data or models, third-party IP restrictions and acknowledgement requirements.

For non-proprietary/open research access, users will normally be required to acknowledge the RI and, where lawful and appropriate, disseminate results and manage data in line with FAIR principles. Proprietary/commercial access may restrict publication or data sharing where justified by confidentiality, IP, contractual or commercial considerations.
Personal data must be processed in accordance with applicable data protection law, including GDPR where applicable. Requests involving personal data, sensitive data, secure data environments or confidential datasets may require a data processing agreement, data management plan, access controls, anonymisation/pseudonymisation, secure transfer method, retention rules and breach-reporting obligations.
Embargo periods, confidentiality periods and restrictions on dissemination must be documented and proportionate. They must not be used to undermine open access principles where non-proprietary/open research access has been granted, but they may be necessary for legitimate IP protection, publication timing, privacy, safety, research security or commercial confidentiality.

Management of intellectual property rights

1. Purpose
The purpose of this section is to establish guidelines for the proper handling, protection, and sharing of intellectual property (IP) created or used within the CMMI Research Infrastructure (RI). It seeks to foster innovation, collaboration, and responsible data use while safeguarding the rights of creators, contributors, and third parties.

2. Scope
This section applies to all users, collaborators, employees, and third parties accessing, managing, or sharing data and intellectual property within the CMMI RI. It encompasses all types of intellectual property, including copyrights, patents, trademarks, trade secrets, know-how, and other proprietary rights.

3. Ownership and Attribution
a. Ownership: Intellectual property generated within the CMMI RI will be governed by applicable laws, regulations, and agreements between involved parties. Ownership terms must be explicitly stated in agreements to avoid disputes.

b. Attribution: Users are required to attribute all intellectual property and data to their rightful creators or sources, following the citation standards established by CMMI and the relevant research community. Proper attribution fosters recognition and accountability, ensuring respect for the contributions of others.

4. Licensing and Sharing of Intellectual Property
a. Open Access: Users are encouraged to make intellectual property accessible through open access licenses, which promote collaboration and innovation. These licenses allow public use and sharing, provided appropriate attribution is given and conditions outlined in the license are met.

b. Licensing Agreements: Users must ensure they possess the necessary rights and permissions before sharing intellectual property through the CMMI RI. Licensing agreements should clearly define the terms and conditions for use, ensuring compliance with applicable legal and regulatory frameworks.

c. Third-Party Intellectual Property: Users must respect the intellectual property rights of third parties, adhering to licensing terms, restrictions, and usage conditions. Unauthorized use of third-party intellectual property is prohibited and may result in legal and institutional repercussions.

5. Protection and Enforcement of Intellectual Property Rights
a. Protective Measures: Users are encouraged to take proactive steps to protect their intellectual property. This may include registering copyrights, securing patents, or implementing other legal protections to safeguard their contributions.

b. Reporting Infringement: Users must report any suspected or confirmed cases of intellectual property infringement to the appropriate CMMI authority. Timely reporting allows CMMI to investigate and address issues effectively, maintaining the integrity of the research environment.

c. Remedies and Sanctions: Violations of intellectual property rights within the CMMI RI may lead to disciplinary actions, including the suspension or termination of access, legal consequences, or other appropriate measures. These actions aim to protect the rights of creators and uphold institutional integrity.

Confidentiality

1. Purpose
The purpose of this section is to establish responsibilities and obligations for the management, sharing, and handling of sensitive data within the CMMI Research Infrastructure (RI). This policy ensures the protection of confidential information while enabling its appropriate accessibility and usability for research, collaboration, and innovation. By maintaining high standards of confidentiality, CMMI fosters trust, integrity, and responsible data usage among all participants.

2. Scope
This Confidentiality Section applies to all users, collaborators, employees, and third parties interacting with data or resources within the CMMI RI. It encompasses a broad range of data types and information, including but not limited to:

Proprietary research data, Personal information, Experimental results, Technical specifications, Equipment and operational records, Documentation derived from facility use, and any other sensitive information shared or generated within the infrastructure.

3. Confidentiality Obligations
To uphold the integrity of the research ecosystem, all parties accessing the CMMI RI must adhere to the following obligations:

a. Protect Sensitive Data: Users are required to ensure the secure handling, storage, and management of sensitive information, employing measures such as encryption, restricted access controls, and secure storage methods.

b. Limit Disclosure: Disclosure of confidential information must be restricted to authorized individuals with a legitimate need for access, strictly for research, collaboration, or operational purposes.

c. Compliance with Legal and Regulatory Standards: Users must comply with all relevant laws and regulations governing data protection, privacy, and confidentiality. This includes adhering to local, national, and international frameworks as applicable.

d. Reporting Breaches: Any suspected or confirmed breaches of confidentiality, such as unauthorized access or data leaks, must be promptly reported to the appropriate CMMI authority. This enables swift action to mitigate risks and address the breach.

4. Open Access and Confidentiality Balance
CMMI is committed to balancing the principles of open access with the need for confidentiality. While promoting data sharing and collaboration, measures must be taken to protect sensitive information:
Users are encouraged to anonymize or aggregate sensitive data wherever feasible, enabling safe sharing without compromising confidentiality.
Any restrictions on data sharing, such as embargo periods or limited access, must be clearly communicated and justified based on the nature of the data.
This balance ensures that the infrastructure remains a secure yet collaborative environment, fostering innovation and knowledge sharing responsibly.

5. Violations and Sanctions
Breaches of confidentiality undermine the integrity of the CMMI RI and its research community. Violations may result in:

- Immediate suspension or termination of access to the infrastructure.
- Disciplinary actions, including potential legal consequences where applicable.
- Other sanctions as deemed appropriate by CMMI management.

By adhering to this confidentiality policy, all participants contribute to a secure and trustworthy research ecosystem, upholding the principles of responsible data management and collaboration.

ACCESS PROCEDURES

CMMI has implemented a minimum access workflow for publicly funded RI components made available to external users. This workflow includes: (1) public information on the infrastructure, service or equipment; (2) an application or enquiry route; (3) completeness and eligibility screening; (4)

technical, scientific, financial, legal, safety, ethics, data protection and/or research-security assessment as applicable; (5) a reasoned decision with clear conditions; (6) an access agreement or accepted terms of use; (7) booking, delivery and logging of actual use; and (8) closure of the request, including outputs, feedback, invoicing where applicable and KPI recording.

Baseline response standards are published for each RI component. Unless a component-specific procedure provides a different published timeframe justified by the nature of the service, CMMI's default targets are: acknowledgement of receipt within five (5) working days; initial completeness/eligibility screening within ten (10) working days; decision on standard requests within twenty (20) working days from receipt of a complete application; and decision on complex, controlled, multi-party, commercial or elevated-sensitivity requests within forty (40) working days from receipt of a complete application. If a target cannot be met, the applicant shall be informed of the reason and the revised expected timeframe.

Urgent public-interest, safety, civil-protection or regulatory requests may be accelerated where feasible, subject to availability, legality and safety. Component-specific procedures may define shorter service levels for standardised services or longer published timeframes for complex access requiring external review, legal negotiation, security assessment, export-control assessment, ethics approval or specialised scheduling.

Objectivity and transparency is supported through published access criteria, documented assessment of feasibility and resource availability, conflict-of-interest management for evaluators where relevant, separation of advisory input and final decision-making where practical, and use of independent or external review where demand exceeds capacity or excellence-based competitive access is applied.

A reasoned decision will be communicated to the applicant. Decisions may be approved, conditionally approved, deferred, redirected to a different access route or refused. The decision will state the main conditions, indicative timing, pricing basis, required training, safety or data/IP conditions, and any restrictions that can lawfully be disclosed.

Applicants may request clarification or procedural reconsideration of a refusal or condition within ten (10) working days of receiving the decision, unless a component-specific procedure states another published period. Reconsideration is limited to procedural error, material misunderstanding, newly available material information, or inconsistency with the published criteria; it does not create an automatic right to access where capacity, legality, safety, confidentiality or funding conditions prevent access.

Overall, access to the different components of CMMI Research Infrastructure (RI) is governed by structured procedures designed to ensure equitable, transparent, and efficient utilization of resources. These procedures encompass the application process, user agreements, orientation and training, and access tiers, each tailored to facilitate seamless integration and optimal use of the infrastructure's capabilities. For Elevated-sensitivity and High-sensitivity/Controlled components, the procedure may include additional risk-based due diligence and legal compliance checks (e.g., sanctions/restrictive measures, export-control/dual-use exposure, information security and confidentiality requirements) to keep access open and safe while ensuring legal conformity. The following paragraphs describe the main principles of the procedure but specific documents and procedures for individual infrastructure components prevail.

Application Process

Prospective users are required to submit a comprehensive access request detailing their research objectives, the specific resources needed, and the intended duration of use. This request should include a clear outline of the proposed work, methodologies, and anticipated outcomes. The application undergoes a thorough review to assess its alignment with the RI's mission, resource availability, and compliance with ethical and legal standards. This evaluation ensures that the infrastructure supports high-quality and impactful research endeavours.
At a minimum, an access request shall include applicant/user details, organisation and contact details where relevant, description of the proposed project or service need, requested RI component/service/equipment/dataset, technical requirements, expected duration or access units, preferred timing, funding source or cost-covering arrangement, expected outputs, and any safety, ethics, data protection, confidentiality, IP, research-security, training or certification information required by the applicable component-specific procedure.

Component-specific procedures may require additional information, such as sample or data specifications, logistics, storage, remote access needs, secure-environment needs, export-control/end-use information, purchase order or quotation acceptance, proof of insurance, user certification, risk assessments, ethics approval, data management plan, NDA requirements or evidence of authority to bind the applicant organisation.

User Agreements

Upon approval, users must enter into formal agreements that delineate the terms of access, usage policies, compliance requirements, and respective responsibilities. These agreements cover critical aspects such as intellectual property rights, confidentiality obligations, data management protocols, and adherence to safety and ethical guidelines. By formalizing these terms, both the user and the RI establish a mutual understanding that safeguards the interests of all parties and promotes responsible use of resources.
The access agreement, accepted quotation, service order or terms of use shall, therefore, include, where applicable: terms of use; safety, security and training obligations; maximum duration or access units; rights and obligations of CMMI and the user; pricing, invoicing and payment terms; cancellation/no-show rules; confidentiality; intellectual property and data ownership/use rights; publication, embargo and acknowledgement rules; GDPR and personal-data obligations; restrictions on commercial use where relevant; liability, insurance and damage responsibilities; incident reporting; sanctions for misuse; and closure/reporting requirements.

Orientation and Training

To ensure users can effectively and safely utilize the RI, comprehensive orientation and training sessions are provided. These sessions cover operational procedures, safety protocols, data management practices, and the ethical conduct expected within the RI. The training is tailored to the specific resources and facilities the user will engage with, ensuring proficiency and compliance with institutional standards. This preparation is crucial for maintaining the integrity and safety of the research environment.

REVIEW AND MAINTENANCE

This Policy will be reviewed at least annually, and more frequently where required by changes to the national framework, legal or regulatory requirements, funding conditions, state-aid rules, safety or research-security requirements, significant incidents, audit findings, user feedback, or material changes to CMMI RI components or services. Following approval of any amendment, CMMI will update the public version of the Policy, relevant website pages, CRI entries and component-specific procedures as appropriate.

REFERENCES

[1] Revised Charter for Access to Research Infrastructures to foster open science, innovation, and research security - European Commission
https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/revised-charter-access-research-infrastructures-foster-open-science-innovation-and-research-security-2024-11-27_en
[2] Deputy Ministry of Research, Innovation and Digital Policy (Republic of Cyprus), "*National Policy of the Republic of Cyprus for Open Science Practices*,"
https://www.gov.cy/media/sites/13/2025/03/National-OS-policy.pdf
[3] EUR-Lex - 32021H2122 - EN - EUR-Lex
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.431.01.0001.01.ENG
[4] Council Recommendation of 23 May 2024 on enhancing research security (C/2024/3510) – EUR-Lex
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AC_202403510
[5] EU Grants guidance: How to handle security-sensitive projects (incl. EUCI, misuse and security self-assessment) – European Commission
https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-handle-security-sensitive-projects_en.pdf
[6] Deputy Ministry of Research, Innovation and Digital Policy (Republic of Cyprus), "Πλαίσιο Πολιτικής Ανοικτής Πρόσβασης σε Δημόσια Χρηματοδοτούμενες Ερευνητικές και Τεχνολογικές Υποδομές (ΔΧΕΥ)," 29 April 2026.
[7] Deputy Ministry of Research, Innovation and Digital Policy (Republic of Cyprus), Circular to Research Organisations on Institutional Open Access Policies for Research Infrastructures, 30 April 2026.