

PLEASE NOTE: THIS POLICY IS A DRAFT AND SUBJECT TO REVISION

01. Top Level CADRE Collaboration Policy

This policy is effective from 20 January 2025.

The Coordinated Access for Data, Research and Environments (CADRE) is a Five Safes Implementation Framework for sensitive data in the Humanities, Arts, and Social Sciences and related disciplines in Australia.

The CADRE platform provides the means to improve Australian researcher access to sensitive data by operationalising the Five Safes framework. The platform has been developed to fill a gap in national research infrastructure, remove barriers and enhance data access processes.

The CADRE collaboration provides the basis for platform partners to engage in, manage and support the development and maintenance of the CADRE platform for CADRE's Australian and international user community.

Introduction and Definitions

To fulfil its mission, it is necessary for the CADRE Collaboration to protect its assets. This document presents the policy regulating those activities of participants related to the security of the Collaboration.

Definitions

Collaboration: All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support the CADRE platform and its services.

Policy Development Kit
Top Level Collaboration Policy

© Owned by the authors and made available under license:

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCLv2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Community: A group of users, organised with a common purpose, and jointly granted access to the CADRE Collaboration. It may act as the interface between individual users and the CADRE Collaboration.

Management: The collection of the various boards, committees, groups and/or individuals mandated to oversee and control the CADRE Collaboration.

Service: A CADRE Collaboration component fulfilling a need of the users, such as computing, storage, networking or software systems.

Service Provider: An entity responsible for the management, deployment, operation and security of a service.

Security Contact: A group or individual responsible for operational security of the CADRE Collaboration. This includes the Collaboration Security Contact and nominated Security Contacts within, or operating on behalf of, a Service Provider.

User: An individual authorised to access and use services.

In this document the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' are to be interpreted as described in RFC 2119.

Objectives

This policy gives authority for actions which may be carried out by designated individuals and organisations, and assigns responsibilities. [SEP]

Scope

This policy applies to all Service Providers and other members of the CADRE Community. This policy augments local Service policies by setting out additional CADRE Collaboration specific requirements.

Additional Policy Documents

Additional policy documents required for a proper implementation of this policy are to be found at [R1].

Approval and Maintenance

This policy is approved by CADRE Management and thereby endorsed and adopted by the Collaboration as a whole. This policy will be maintained and revised by a body

Policy Development Kit
Top Level Collaboration Policy

© Owned by the authors and made available under license:

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCLv2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

appointed by CADRE Management as required and resubmitted for formal approval and adoption whenever significant changes are needed. The most recently approved version of this document is available at [R1].

Roles and responsibilities of the management

CADRE Management provides, through the adoption of this policy and through its representations on the various management bodies of the CADRE Collaboration, the overall authority for the decisions and actions resulting from this policy including procedures for the resolution of disputes. CADRE Management maintains the set of policies approved for use within the Collaboration and ensures that participants are aware of their roles and responsibilities. The approved policy set must meet the requirements of the Snctfi framework [R2].

Roles and responsibilities of the security contact

The CADRE Security Contact coordinates the operational security capabilities of the CADRE Collaboration, including the enabling of compliance with the Sirtfi framework [R3]. The Security Contact may, in consultation with the CADRE Management and other appropriate persons, require actions by Service Providers as are deemed necessary to protect the Collaboration from or contain the spread of IT security incidents. The Security Contact handles requests for exceptions to this policy as described below. The Security Contact is responsible for establishing and periodically testing a communications flow for use in security incidents.

Physical security

All the requirements for the physical security of resources are expected to be adequately covered by each Service's local security policies and practices. These should, as a minimum, reduce the risks from intruders, fire, flood, power failure, equipment failure and environmental hazards. Stronger physical security may be required for equipment used to provide certain critical services such as CADRE Community membership services, the Authentication Proxy, or credential repositories.

Network security

All the requirements for the network security of resources are expected to be adequately covered by each Service's local security policies and practices.

Policy Development Kit
Top Level Collaboration Policy
© Owned by the authors and made available under license:
<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCLv2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

To support specific CADRE Community workflows, it may be necessary to permit inbound or outbound network traffic. It is the responsibility of the Service to accept or mitigate the risks associated with such traffic.

Exceptions to compliance

Where the processes described lead to obvious injustice and hardship due to an implementation of the process being unduly hard, a time-limited and documented exception may be implemented after the explicit approval of CADRE Management.

Any such exception must be followed by immediate and concrete steps to address the deficiencies created within a limited time period commensurate with the discrepancy induced. The invocation of the hardship clause must not compromise the integrity or trustworthiness of the CADRE Collaboration.

Sanctions

Services and Communities that fail to comply with this policy may lose their rights and benefits until compliance has been satisfactorily demonstrated again.

Any activities thought to be illegal may be reported to appropriate law enforcement agencies.

[R1] <https://documentation.cadre.ada.edu.au/policies>

[R2] <https://www.igtf.net/snctfi/>

[R3] <https://refeds.org/wp-content/uploads/2022/08/Sirtfi-v2.pdf>

Policy Development Kit

Top Level Collaboration Policy

© Owned by the authors and made available under license:

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SC1v2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).