*Questions to ask yourself when defining the policy:*

- *Who are the actors in your Collaboration environment?*
- *How will you tie additional policies together for the Collaboration?*
- *Which bodies should approve policy wording?*

**delete this box after completing the policy.*

# Top Level Collaboration Policy

This policy is effective from <insert date>.

## Introduction and Definitions

To fulfil its mission, it is necessary for the 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 services.

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

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

**Service:** A 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 Collaboration.

**User:** An individual authorised to access and use services.

Policy Development Kit
Top Level Collaboration Policy

Other Sources / Attribution / Acknowledgements: SCIv2 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).

*Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.*

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 2.2

## Objectives

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

## Scope

This policy applies to all Service Providers and members of the Community. This policy augments local Service policies by setting out additional 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 the *Management* and thereby endorsed and adopted by the Collaboration as a whole. This *policy* will be maintained and revised by a body appointed by the *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 a location specific to the Collaboration [R1].

## Roles and responsibilities of the management

The *Management* provides, through the adoption of this *policy* and through its representations on the various management bodies of the Collaboration, the overall authority for the decisions and actions resulting from this *policy* including procedures for the resolution of disputes. The 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].



Other Sources / Attribution / Acknowledgements: SCIv2 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).

*Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.*

## Roles and responsibilities of the security contact

The Security Contact coordinates the operational security capabilities of the Collaboration, including the enabling of compliance with the Sirtfi framework [R3]. The Security Contact may, in consultation with the 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 *Community* membership services, the Authentication Proxy, or credential repositories.

## Network security

All the requirements for the networking security of resources are expected to be adequately covered by each *Service's* local security policies and practices.
To support specific *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 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 Collaboration.



Other Sources / Attribution / Acknowledgements: SCIv2 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).

*Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.*

## 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] <Insert a link to all Collaboration policies>

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

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