Top Level Infrastructure Policy

INTRODUCTION AND DEFINITIONS

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

Definitions

The phrase Infrastructure when italicized in this document, means all of the people and organisations, hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control or support IT services.

The other italicized words used in this document are defined as follows:

- *Policy* is interpreted to include rules, responsibilities and procedures specified in this document together with all those in other documents which are required to exist by stipulations in this document.
- A *participant* is any entity providing, using, managing, operating, supporting or coordinating one or more IT *service*(s).
- A *service* is any computing or software system accessible by *Users* of the Infrastructure.
- The *Management* is the collection of the various boards, committees, groups and individuals mandated to oversee and control the Infrastructure.
- A *User* is an individual who has been given authority to access and use Infrastructure resources.
- A *User Community* is a grouping of *Users*, usually not bound to a single institution, which, by reason of their common membership and in sharing a common goal, are given authority to use a set of *services*.
  - Included in the definition of a *User Community* are cases where *services* are offered to individual *Users* who are not members of an explicitly organised *User Community*.
- The *User Community Management* is the collection of various individuals and groups mandated to oversee and control a *User Community*.

Objectives

This *policy* gives authority for actions which may be carried out by designated individuals and organisations and places responsibilities on all *participants*.

Scope

This *policy* applies to all *participants*. This *policy* augments local *Service* policies by setting out additional Infrastructure specific requirements.

Additional Policy Documents

Additional policy documents required for a proper implementation of this *policy* may be found at a location specific to the Infrastructure [R1].

Approval and Maintenance

This *policy* is approved by the *Management* and thereby endorsed and adopted by the Infrastructure 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 Infrastructure [R1].

ROLES AND RESPONSIBILITIES

This section defines the roles and responsibilities of participants.

The Management

The *Management* provides, through the adoption of this *policy* and through its representations on the various management bodies of the Infrastructure, the overall authority for the decisions and actions resulting from this *policy* including procedures for the resolution of disputes.
The *Management* provides the capabilities for meeting its responsibilities with respect to this policy. The

Management is responsible for ensuring compliance of its participants and can represent them towards third parties with respect to this *policy*.

The *Management* is responsible for appointing a natural or legal person as Data Controller, and for publishing an Infrastructure Privacy Statement compliant with the GEANT Data Protection Code of Conduct [R2] for the Infrastructure. The *Management* must maintain a registry of Privacy Statements of *Services* to which personal data may be released. These Privacy Statements are collected in [R3].

The *Management* is responsible for ensuring that the federation-facing proxy complies with REFEDS R&S criteria and best practices.

The Infrastructure Security Contact

The *Management* must appoint a Security Contact who leads and coordinates the operational security capability of the Infrastructure. This person must support the requirements of the Sirtfi framework on behalf of the Infrastructure. The Security Contact may, in consultation with the *Management* and other appropriate persons, require actions by *participants* as are deemed necessary to protect the Infrastructure from or contain the spread of IT security incidents. The Security Contact also 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 and for reporting potential data breaches to the Data Controller.

The HDF Infrastructure Security Contact is hdf-security@lists.kit.edu.

User Community Management

The *User Community Management* must designate a Security contact point (person or team) that is willing and able to collaborate with affected participants in the management of security incidents.

The *User Community Management* should abide by the Infrastructure policies in the areas of Acceptable Use and Membership Management and all other applicable policies [R1]. Exceptions to this must be handled as in the section on Exceptions. They must ensure that only individuals who have agreed to abide by the Infrastructure AUP [R1] and have been presented with the Infrastructure Privacy Statement are registered as members of the *User Community*. The acceptance of the AUP must be recorded for audit trail and repeated at least once a year, or upon material changes to its content.

User Community Management and *Users* that provide and/or operate services must abide by all applicable policies [R1], including the Sirfti framework [R4].

For services requiring authentication of entities the *User Community Management* must abide by the policy on Acceptable Authentication Assurance [R1].

User Community Management is responsible for promptly investigating reports of *Users* failing to comply with the policies and for taking appropriate action to limit the risk to the Infrastructure and ensure compliance in the future.

Users

Users must accept and agree to abide by the Infrastructure Acceptable Use Policy when they register or renew their registration with a *User Community*.

Users must use services only in pursuit of the legitimate purposes of their *User Community*. They must not attempt to circumvent any restrictions on access to *services*. *Users* must show responsibility, consideration and respect towards other participants in the demands they place on the *Services*.

Users that provide and/or operate *services* must abide by any service oriented policies adopted by the Infrastructure [R1].

For *services* requiring authentication of entities the *Users* must abide by the policy on Acceptable Authentication Assurance [R1].

Users may be held responsible for all actions taken using their credentials, whether carried out personally or not.

No intentional sharing of *User* credentials is permitted.

Service Management

The *Service* must designate a Security contact point (person or team) that is willing and able to collaborate with affected participants in the management of security incidents and to take prompt action as necessary to safeguard services and resources during an incident.

Services must abide by any service oriented policies adopted by the Infrastructure [R1], including the Sirtfi framework [R4].

Services acknowledge that participating in the Infrastructure and allowing related inbound and outbound network traffic increases their IT security risk. *Services* are responsible for accepting or mitigating this risk.

Services must deploy effective security controls to protect the confidentiality, integrity and availability of their services and resources.

For *Services* requiring authentication of entities the *Services* must abide by the policy on Acceptable Authentication Assurance (see [R1])

For *Services* receiving personal data, a Privacy Statement compliant with the GEANT Data Protection Code of Conduct [R2] must be shared with the *Management* and presented to *Users* upon first access to the *Service*. Services are responsible for recording sufficient information such that personal data can be cleansed after the retention period is reached.

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 *User 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 *User 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

Wherever possible, Infrastructure policies and procedures are designed to apply uniformly to all participants. If this is not possible, for example due to legal or contractual obligations, exceptions may be made. Such exceptions should be time-limited and must be documented and authorized by the **Infrastructure Security Contact** and, if required, approved at the appropriate level of the *Management*.

In exceptional circumstances it may be necessary for participants to take emergency action in response to some unforeseen situation which may violate some aspect of this policy for the greater good of pursuing or preserving legitimate Infrastructure objectives. If such a policy violation is necessary, the exception should be minimized, documented, time-limited and authorized at the highest level of the *Management* commensurate with taking the emergency action promptly, and the details notified to the Infrastructure *Security Contact* at the earliest opportunity.

SANCTIONS

Services that fail to comply with this policy in respect of a service they are operating may lose the right to have their services recognized by the Infrastructure until compliance has been satisfactorily demonstrated again.

User Communities who fail to comply with this policy may lose their right of access to and collaboration with the Infrastructure and may lose the right to have their services recognized by the Infrastructure until compliance has been satisfactorily demonstrated again.

Users who fail to comply with this policy may lose their right of access to the Infrastructure, and may have their activities reported to their *User Community* or their home organisation.

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

[R1] https://git.scc.kit.edu/m-team/hdf-info/tree/master/policies

[R2] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

[R3] https://login.helmholtz-data-federation.de/unitygw/VAADIN/files/connected-services.html

[R4] https://aarc-project.eu/policies/sirtfi