Top Level Infrastructure Policy

1 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 and availability of the *Infrastructure* governed by this *policy*.

This *policy* is effective from November 18th, 2020.

This *policy* is one of a set of documents that together define the HIFIS Policies [1]. This individual document must be considered in conjunction with all the policy documents in the set.

1.1 Definitions

The terms below, when italicised in this document, are to be interpreted in accordance to their following definitions:

- The phrase *Infrastructure* means all of the natural and legal persons, organisations, hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control, secure or support *Services*.
- *Policy* is interpreted to include rules, responsibilities and procedures. These are 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 *Service(s)*.
- A *Service* is any ICT system or application accessible by *Users* of the *Infrastructure*.
- A *Service Provider (SP)* is any entity offering *Services*.
- The *Infrastructure 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 *Services*.
- A *Virtual Organisation (VO)* is a group of one or more *Users*, not necessarily bound to a single institution, organised with a common purpose, jointly granted access to one or more *Services*. It may serve as an entity which acts as the interface between the individual *Users* and an *Infrastructure*. In general, the members of the *Virtual Organisation* will not need to separately negotiate access with *Service Providers*. A *User* can be member of multiple *Virtual Organisations*.
- The *Virtual Organisation Management* is the collection of various individuals and groups mandated to oversee and control a *Virtual Organisation*.
- The *Virtual Organisation Supervisor* is the collection of various individuals and groups delegated from the *Infrastructure Management* to oversee and approve requests for registration and deregistration of *Virtual Organisations*.
- An *Identity Provider (IdP)* is any system that creates, maintains, and manages identity information for *Users* while offering authentication functionality to relying *Services* and *SP-IdP proxy* within the *Infrastructure*.
- The *Service Provider to Identity Provider proxy (SP-IdP proxy)* [6] — introduced in the AARC Blueprint Architecture [7] used to implement federated access management solutions for international

research collaborations — is a single component that negotiates between *Services* and *IdPs,* thereby shielding the *Infrastructure* from the heterogeneity of global identity federations.
- A *Role* is a property that a *Participant* has. It comprises a set of rights and responsibilities within the *Infrastructure* and determines the *Participant*'s abilities to use and/or manage a *Service, Virtual Organisation* or any other part of the *Infrastructure*. A *Participant* can hold different *Roles* in different contexts. *Roles* are defined by the *Policies*.
- The *Infrastructure Security Contact* is the collection of various individuals and groups mandated by the *Infrastructure Management* to lead and coordinate the operational security capability of the *Infrastructure*.

Other infrastructures, frameworks or standards mentioned in this document are described below:
- *Sirtfi* [2] is a trust framework aiming to enable coordination of security incident response across federated organisations by describing practices and attributes that identify an organisation as being capable of effectively participating in incident response — i.e. is *Sirtfi* compliant.
- The *REFEDS Assurance Framework (RAF)* [3] defines requirements for identity assurance, as well as two assurance profiles based on these requirements. Identity Assurance conveys the level of confidence that an identity belongs to the expected *User*; this includes identity vetting, multi factor authentication and the security provisions of the *Identity Provider* among other factors. The aim is to provide a basis for *SPs* to make decisions on how much to trust assertions made by *IdPs,* and manage risks related to access control to their *Services*.
- The *REFEDS Research and Scholarship (R&S) Entity Category* [4] aims to support the release of attributes by *IdPs* to *SPs* in this category, by defining requirements on both *SPs* and *IdPs,* as well as the attribute bundle that must be supported.
- The *DFN-AAI* [5] is an authentication and authorisation infrastructure operated by the DFN association.
- *DFN-AAI Advanced,* the highest of three levels of assurance within *DFN-AAI,* defines minimum requirements for *IdPs* regarding the reliability and trustworthiness of authentication. Please note that *DFN-AAI* is moving towards *DFN-AAI-+* which makes use of the *REFEDS Assurance Framework* to describe assurance.

1.2 Objectives

This *policy* gives authority for actions as defined in this *policy,* which may be carried out by designated individuals and organisations, and places responsibilities on all *Participants*.

1.3 Scope

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

1.4 Approval and Maintenance

This *policy* is approved by the *Infrastructure Management* and thereby endorsed and adopted by the *Infrastructure* as a whole. This *policy* will be maintained and revised by a collection of various individuals and groups appointed by the *Infrastructure 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* [1].

1.5 Additional Policy Documents

Additional policy documents required for a proper implementation of this *policy* may be found at a location specific to the *Infrastructure* [1], and are listed below:

- Virtual Organisation Membership Management Policy (VOMMP)
- Policy on the Processing of Personal Data (PPPD)
- Security Incident Response Procedure (SIRP)

These *Infrastructure*-defined policies must be complemented by local policies. The following list of policies may need to be specified by *Participants*, depending on which *Infrastructure* components (see section 2.2) are operated.

- Service Privacy Policy (SPP)
- Virtual Organisation Acceptable Use Policy (VO AUP)
- SP-IdP proxy Privacy Policy (Proxy PP)
- Service Acceptable Use Policy (SAUP) — optional
- Service Access Policy (SAP) — optional
- Virtual Organisation Privacy Policy (VO PP) — optional (unless *VOs* process or control personal data)

Templates are provided for Acceptable Use Policies and Privacy Policies [1].

Figure 1 gives an overview of the HIFIS policies, specifying, for each policy, the *Participant* that defines (or should define) the policy, and the *Participant*(s) that must abide by the policy.

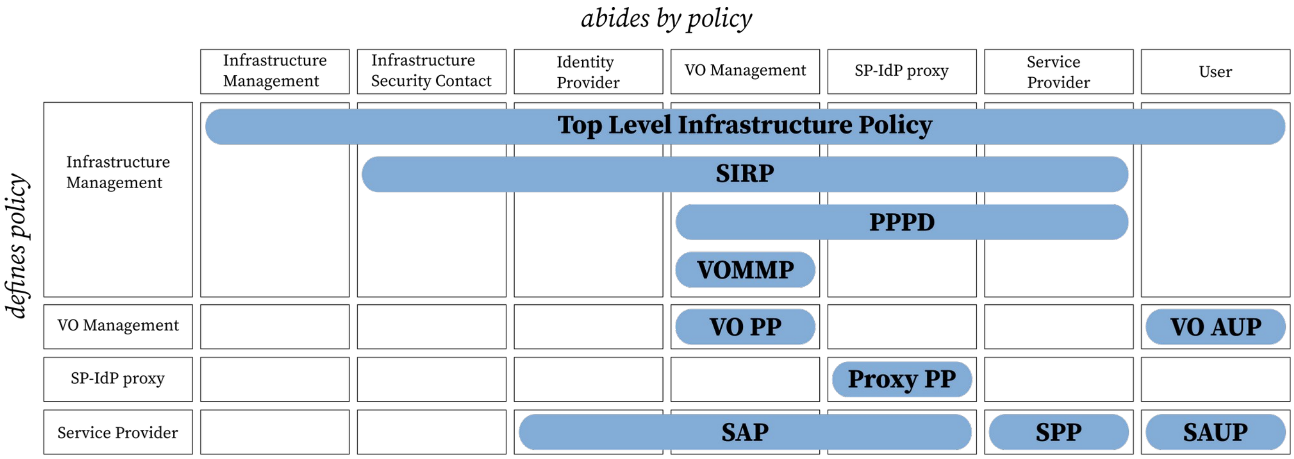

Figure 1: Overview of HIFIS policies, with respect to the Participants involved in defining them, as well as abiding by the specified policies.

2 ROLES AND RESPONSIBILITIES

This section defines the roles and responsibilities of *Participants*.

2.1 Roles

- Infrastructure Management
- Infrastructure Security Contact

- User
- Virtual Organisation Management
- Identity Provider
- Service Provider
- SP-IdP proxy

2.2 Infrastructure

2.2.1 Infrastructure Management

The *Infrastructure 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 *Infrastructure Management* provides the capabilities for meeting its responsibilities with respect to this *policy*. The *Infrastructure Management* is responsible for taking all necessary actions to ensure compliance of its *Participants* and can represent them towards third parties with respect to this *policy*.

The *Infrastructure Management* must maintain a registry of Privacy Policies of *Services* to which personal data may be released.

The *Infrastructure Management* must appoint an *Infrastructure Security Contact* who leads and coordinates the operational security capability of the *Infrastructure*.

2.2.2 Infrastructure Security Contact

The *Infrastructure Security Contact* must support the requirements of the *Sirtfi* framework [2] on behalf of the *Infrastructure*.

The *Infrastructure Security Contact* must, in consultation with the *Infrastructure 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 *Infrastructure Security Contact* also handles requests for exceptions to this *policy* as described in section 5. The *Infrastructure Security Contact* is responsible for establishing periodical tests of a communications flow to all Security Contact Points for use in security incidents.

The *Infrastructure Security Contact* is security@hifis.net.

2.3 Identity Provider

Identity Providers must support / abide by:

- *Sirtfi* [2]

  Identity Providers must comply with the *Sirtfi* framework [2]. *Identity Providers* 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 make it known to the *Infrastructure Security Contact*.

- *REFEDS Assurance Framework (RAF)* [3]

  Identity Providers must abide by the provisions on acceptable authentication assurance in section 3. *Identity Providers* must support the *REFEDS Assurance Framework (RAF)* [3] to describe the levels of assurance of their *Users*.

- *R&S Entity Category* [4]

  Identity Providers must support the *R&S Entity Category* [4] and ensure that they can supply the attributes to *R&S Service Providers* in accordance with the *R&S Entity Category* specification [4].

- Security Incident Response Procedure (SIRP)

- Service Access Policies (SAP)

  The use of each *Service* may require the delivery of additional *User* attributes, such as “entitlements” for authorising the use of specific *Services*. These attributes can be found in the Service Access Policy of the *Service*. *Identity Providers* must ensure the ability to send these additional attributes, and the attributes must be delivered only in agreement with *Service Providers*.

Identity Providers must acknowledge that their mere participation in the *Infrastructure* does not entitle their *Users* to use all the *Services* offered in the *Infrastructure*. The use of the individual *Services* may require bilateral agreements between the organisations of the *Identity Providers* and those of the *Service Providers*.

Identity Providers must provide correct information about their *Users*. Correctness is defined by the *R&S Entity Category* specification [4] and guidelines of the *DFN-AAI* [5]. For additional attributes, the requirements of the respective *Service Provider* apply, as specified in their Service Access Policy (SAP).

Identity Providers must inform *Users* about the data to be transmitted by the *Identity Provider* to the *Service Provider*.

2.4 Virtual Organisation Management

Virtual Organisations must support / abide by:

- *REFEDS Assurance Framework (RAF)* [3]

  The *Virtual Organisation Management* must abide by the provisions on acceptable authentication assurance in section 3. The *Virtual Organisation Management* must support the *REFEDS Assurance Framework (RAF)* [3] to describe the levels of assurance of *Users*.

- Security Incident Response Procedure (SIRP)

The *Virtual Organisation 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, in compliance with the Security Incident Response Procedure (SIRP).

- Virtual Organisation Membership Management Policy (VOMMP)

  The *Virtual Organisation Management* must abide by the Virtual Organisation Membership Management Policy. Exceptions to this must be handled as in section 5.

- Policy on the Processing of Personal Data (PPPD)

  Virtual Organisations that operate their own Registry (containing membership data of the *VO*) must comply with the Policy on the Processing of Personal Data. The Registry must also be operated in a manner compliant with *Sirtfi* [2]. A *Virtual Organisation* may delegate the operation of its Registry to the *SP-IdP proxy*.

Virtual Organisations must define:

- Virtual Organisation Acceptable Use Policy (VO AUP)

  The *Virtual Organisation* must define, and provide to the *Infrastructure*, a Virtual Organisation Acceptable Use Policy (VO AUP), and ensure that its members are aware of and agree to abide by this AUP. The *Virtual Organisation Management* must ensure that only individuals who have agreed to abide by the Virtual Organisation AUP and have been presented with the VO Privacy Policy or SP-IdP proxy Privacy Policy are registered as members of the *Virtual Organisation*. 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.

- Virtual Organisation Privacy Policy (VO PP)

  Virtual Organisations that process or control personal data must define a Virtual Organisation Privacy Policy (VO PP).

The *Virtual Organisation 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.

The *Virtual Organisation Management* is responsible for obtaining support for their *Virtual Organisation* from *Services* (e.g. through MoUs or other types of agreements), and ensuring that all the *Service* requirements placed upon the *Users* are met, including identity assurance.

2.5 SP-IdP Proxy

The *SP-IdP proxy* must support / abide by:

- *Sirtfi* [2]

The *SP-IdP proxy* 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 the *SP-IdP proxy* during an incident and make it known to the *Infrastructure Security Contact*. The Security contact must also support the requirements of the *Sirtfi* framework [2] on behalf of the *SP-IdP proxy*.

- *REFEDS Assurance Framework (RAF)* [3]

  The *SP-IdP proxy* must abide by the provisions on acceptable authentication assurance in section 3.

- *R&S Entity Category* [4]

  The *SP-IdP proxy* must comply with the *R&S Entity Category* [4] criteria and best practices.

- Security Incident Response Procedure (SIRP)

- Policy on the Processing of Personal Data (PPPD)

The *SP-IdP proxy* must define an SP-IdP proxy Privacy Policy (Proxy PP).

The *SP-IdP proxy* must forward entitlements from the home *IdPs* to *SPs*.

2.6 Service Provider

Service Providers must support / abide by:

- *Sirtfi* [2]

  Service Providers must comply with the *Sirtfi* framework [2]. The *Service Provider* 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* during an incident and make it known to the *Infrastructure Security Contact*.

  Service Providers must deploy effective security controls to protect the confidentiality, integrity and availability of their *Services*.

- *REFEDS Assurance Framework (RAF)* [3]

  For *Services* requiring authentication of entities, the *Service Providers* must abide by the provisions on acceptable authentication assurance in section 3.

- *R&S Entity Category* [4]

  Service Providers must comply with the *R&S Entity Category* [4] criteria and best practices. *Service Providers* should limit their data requirements to the bundle of attributes defined in the *R&S Entity Category* [4] specification, but may negotiate for additional data as required, via Service Access Policies.

- Security Incident Response Procedure (SIRP)
- Policy on the Processing of Personal Data (PPPD)

  For *Services* receiving personal data, *Service Providers* must comply with the Policy on the Processing of Personal Data (PPPD).

Service Providers must define, for each *Service*:

- Service Privacy Policy (SPP)

  For each *Service* that processes or controls personal data, a Service Privacy Policy (SPP) must be defined and shared with the *Infrastructure Management*, and presented to *Users* upon first access to the *Service*.

  Service Providers are responsible for recording sufficient information such that personal data can be cleansed after the retention period is reached. The recorded information and the retention period must be specified in the local Service Privacy Policy (SPP).

Service Providers may define, for each *Service*:

- Service Acceptable Use Policy (SAUP)

  For each *Service* provided, *Service Providers* may specify a Service Acceptable Use Policy (SAUP) if the AUPs in force in the *Infrastructure* are not acceptable, and ensure that its *Users* are aware of and agree to abide by this AUP.

- Service Access Policy (SAP)

  For each *Service* provided, *Service Providers* may specify a Service Access Policy (SAP), where supported assurance profiles can be defined, as well as any additional attributes that are required for providing the *Service*.

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

2.7 User

Users must abide by:

- Virtual Organisation Acceptable Use Policy (VO AUP)

  Users must accept and agree to abide by the Virtual Organisation Acceptable Use Policy (VO AUP) when they register or renew their registration with a *Virtual Organisation*, as well as upon changes in this policy.

- Service Acceptable Use Policy (SAUP)

> *Users* must accept and agree to abide by the Service Acceptable Use Policy (SAUP) of each *Service* they use.

Users that have been authorised to use a *Service* by virtue of their membership in a *Virtual Organisation* must use the *Service* only in pursuit of the legitimate purposes of their *Virtual Organisation*.

Users 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 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.

3 ACCEPTABLE AUTHENTICATION ASSURANCE

In line with the *REFEDS Assurance Framework (RAF)* [3], assurance information is expressed by asserting individual assurance components, as well as composite assurance profiles. Assurance profiles can be composed by information derived from several sources in the *Infrastructure*: *Identity Providers, Virtual Organisations, SP-IdP proxy* (see [9] for AARC policy guidelines to effectively implement authentication assurance).

In the HIFIS *Infrastructure,* there is no minimal assurance level. Different assurance levels are supported explicitly. *Identity Providers* should support *RAF* [3]. *Services* should filter *Users* by their assurance level and the *Virtual Organisation Management* can (under specific circumstances) take measures to elevate the assurance of *Users* (e.g. by checking a person's passport according to defined procedures).

Assurance information will be propagated with the *User*'s authentication token for relying *Services* to include in authorisation decisions. Only *Users* conforming to one of the approved authentication assurance profiles shall be granted access to the *Infrastructure*.

4 PHYSICAL AND NETWORK SECURITY

All the requirements for the physical security of *Services* are expected to be adequately covered by each *Service Provider*'s local security policies and practices. The technical details of such additional requirements are contained in the procedures for operating and approving such *Services*.

Networking security of *Services* is expected to be adequately covered by each *Service Provider*'s local security policies and practices.

5 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 authorised by the *Infrastructure Security Contact* and, if required, approved at the appropriate level of the *Infrastructure 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 minimised, documented, time-limited and authorised at the highest level of the *Infrastructure Management* commensurate with taking the emergency action promptly, and the details notified to the *Infrastructure Security Contact* at the earliest opportunity.

6 SANCTIONS

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

Identity Providers who fail to comply with this *policy* may lose their right of access to the *Infrastructure* until compliance has been satisfactorily demonstrated again.

Virtual Organisations who fail to comply with this *policy* may lose their right of access to and collaboration with 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 *Virtual Organisation* or their home organisation.

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

7 FEES

There are no charges for using the *Infrastructure*. The billing of paid *Services* does not fall under the jurisdiction of the *Infrastructure* and may be subject to bilateral agreements between the individual *Participants*.

8 SALVATORY CLAUSE

Should any provision of this *policy* be or become invalid, this shall not affect the validity of the remaining provisions or the agreement as a whole. The provision shall be replaced retroactively by a provision which is legally permissible and whose content comes close to the original provision. The same applies to existing loopholes.

This *policy* is subject to German law and German jurisdiction.

9 REFERENCES

[1] HIFIS Policies - https://hifis.net/policies
[2] Security Incident Response Trust Framework for Federated Identity (Sirtfi) - https://refeds.org/sirtfi
[3] REFEDS Assurance Framework (RAF) - https://refeds.org/assurance
[4] REFEDS Research and Scholarship Entity Category - https://refeds.org/category/research-and-scholarship
[5] DFN-AAI - https://doku.tid.dfn.de/

[6] Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi) - https://www.igtf.net/snctfi/

[7] AARC Blueprint Architecture - https://aarc-project.eu/architecture/

[8] eduGAIN - https://edugain.org/

[9] AARC policy guidelines - https://aarc-project.eu/guidelines/#policy