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.

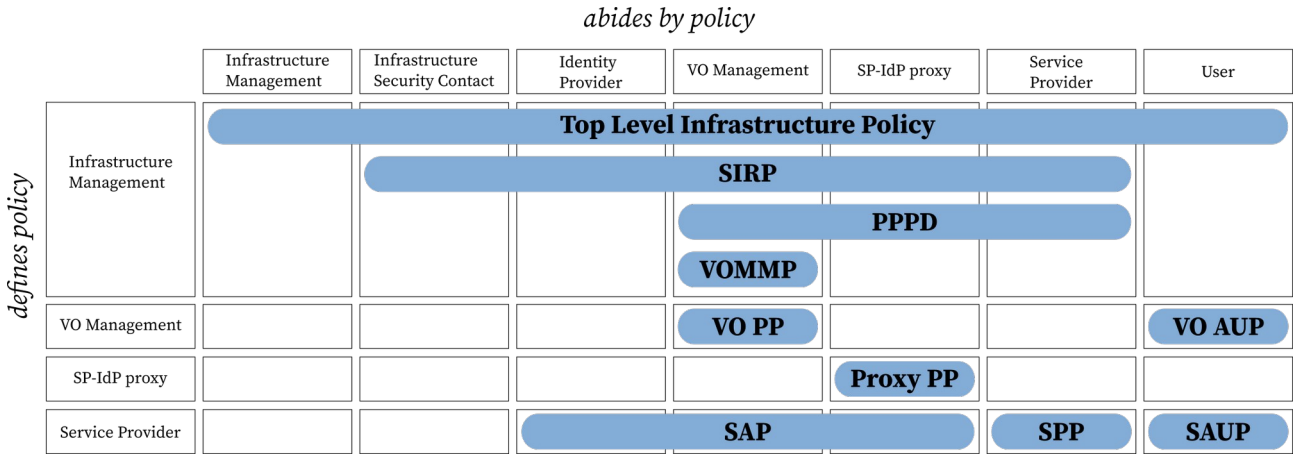

Figure 1: Overview of HIFIS policies, with respect to the Participants involved in defining them, as well as abiding by the specified policies.

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

Virtual Organisation Membership Management Policy

This policy is effective from November 18th, 2020.

1 INTRODUCTION

This policy is designed to establish trust between a Virtual Organisation and other Virtual Organisations, Infrastructures, and the R&E federations. The behaviour of the Virtual Organisation and its Users must be appropriate and facilitate the Virtual Organisation's compliance with the requirements of *Snctfi* [1].

This policy applies to the Virtual Organisation Management and other designated Virtual Organisation management personnel. It places requirements on Virtual Organisations regarding eligibility, obligations and rights of their Users, and it governs their relationships with all Infrastructures with which they have a usage agreement. The Virtual Organisation management personnel must ensure awareness and acceptance, by the Virtual Organisation and its Users, of the responsibilities documented in this policy.

2 DEFINITIONS

Data supplied by the User is defined as follows.

User Data comprises verified information on at least:

- family name(s)
- given name(s)
- the employing organisation's name and address (this is required if the User's membership eligibility derives from his/her institutional affiliation)
- contact telephone number (this is optional, but the Virtual Organisation Management may need to contact the User promptly during investigation of security incidents)

Registration Data — authentication (AuthN) related information:

- *User Data*
- email address
- unique and non-reassigned identifier(s) of the User and the source of authority of each identifier
- registration timestamp

The principles of data protection should apply to any processing of personal data and information concerning an identified or identifiable User.

3 INDIVIDUAL USERS

The Virtual Organisation must define an Acceptable Use Policy (AUP). The AUP must be shown to all persons joining the Virtual Organisation. Acceptance of the AUP by Virtual Organisation members who act as responsible persons towards the Infrastructure must be an explicit action, must be recorded, and must be a prerequisite for registration in the Virtual Organisation. Virtual Organisation procedures must ensure that the User is informed of and explicitly consents to material changes to the AUP, including those that arise out of new collaborative partnerships, as soon as is feasible. The Virtual Organisation is recommended to

ensure that their AUP comprises specific AUPs of the individual Services used by the Virtual Organisation. Experience shows that some Services require different AUPs.

Hosts, Services and/or Robots (automated processes acting on behalf of the Virtual Organisation or a User) may be registered as members of the Virtual Organisation. In the case of such registrations, the *Registration Data* must include the personal details of the individual requesting registration who must assume, as a User, ongoing responsibility for the registered entity, and may be subject to additional policy requirements of the Infrastructure.

All Users are deemed to be acting in a professional capacity when interacting with or using Infrastructure Services that support the Virtual Organisation.

4 VIRTUAL ORGANISATION MANAGEMENT

The Virtual Organisation must define a Virtual Organisation Management role and assign this role to two or more individuals. The Virtual Organisation Management role can be performed only by individuals who can authenticate via an Identity Provider that is part of the Infrastructure. The Virtual Organisation Management is responsible for meeting the requirements of this policy and those of the applicable policies of the Infrastructures, and for implementing the necessary procedures and operational requirements.

The Virtual Organisation Management does not necessarily have to be a member of the Virtual Organisation. The role may be performed by any individual so designated by the Virtual Organisation, including Infrastructure personnel.

The Virtual Organisation Management must implement procedures that ensure the accuracy of individual User *Registration Data* for all Virtual Organisation members who act as responsible persons towards the Infrastructure. The contact information must be verified both at initial collection (registration) and on an ongoing basis (through periodic renewal or review, please refer to the topic *Membership Life Cycle: Renewal*) and only stored and processed in compliance with applicable Data Protection legislation.

Other Virtual Organisation roles, such as additional management personnel and security contacts must be defined and assigned to individuals as required by the Infrastructure.

5 VIRTUAL ORGANISATION

5.1 Aims and Purposes

The Virtual Organisation must define, in its AUP, its collective aims and purposes, i.e., the research or scholarship goals of the Virtual Organisation. In order to allow Infrastructures to make decisions on resource allocation, the Virtual Organisation should make this definition available to them, and subsequently inform them of any material changes therein.

5.2 Membership

The Virtual Organisation Management is responsible for the Virtual Organisation Membership life cycle process of its Users. This responsibility may be devolved to designated personnel in the Virtual Organisation or in the Infrastructure, and their trusted agents (such as Institute Representatives or Service Managers), hereafter collectively called Sponsors.

The Virtual Organisation procedures must:

- unambiguously name the individuals who take responsibility for the validity of the *Registration Data* provided,
- ensure there is a way of contacting the User identified as responsible for an action while using Infrastructure Services as a member of the Virtual Organisation, and
- identify those with the authority to exercise control over the rights of its members to use the Infrastructure Services that support the Virtual Organisation.

The Virtual Organisation must be aware that inappropriate actions by an individual member of the Virtual Organisation may adversely affect the ability of other members of the Virtual Organisation to use an Infrastructure.

5.3 Membership Life Cycle: Registration

Membership Registration is the process by which an applicant joins the Virtual Organisation and becomes a Member. *Registration Data* must be collected at the time of Registration, verified and stored in compliance with the Data Protection and Privacy Policy. Reasonable efforts must be spent to validate the data.

The applicant must agree to abide by the AUP of the Virtual Organisation, and agree to use Services of the Infrastructures exclusively for the Aims and Purposes of the Virtual Organisation.

5.4 Membership Life Cycle: Assignment of Attributes

Assignment of attributes (such as group membership, entitlements, or roles) shall be the responsibility of the Virtual Organisation Management or of designated person(s) responsible for the management of such attributes.

Attribute management may be subject to an assurance profile agreed upon between the Virtual Organisation and the Infrastructures. Attributes shall be assigned only for as long as they are applicable.

5.5 Membership Life Cycle: Changes of Assurance Level

In some cases, it may be necessary to increase the assurance of a User (for example, changing the identity assurance profile from low to medium). This shall be the responsibility of the Virtual Organisation Management and must be done in accordance to the assurance framework in which the statement was made.

5.6 Membership Life Cycle: Renewal

Membership Renewal is the process by which a User remains a member of the Virtual Organisation. Membership Renewal procedures must make a reasonable effort to

- ensure that accurate *Registration Data* is maintained for all eligible Users
- confirm continued eligibility of the User to use Infrastructure Services that support the Virtual Organisation
- confirm continued eligibility of the User to any attributes
- ensure the reaffirmation of acceptance of the AUP of the Virtual Organisation

The maximum time span between Registration and Renewal, and between Renewals, for all Virtual Organisation members who act as responsible persons towards the Infrastructure, shall be one year. The User shall be able to correct and amend their *Registration Data* at any time.

5.7 Membership Life Cycle: Suspension

The Suspension of Virtual Organisation membership is the temporary revocation of full or partial rights and of any attributes. Suspension is done by or on behalf of the Virtual Organisation Management.
A User should be suspended when the Virtual Organisation Management is presented with reasonable evidence that the member's identity or credentials have been used, with or without the User's consent, in breach of relevant Policies.

Suspension can be requested by:

- the Virtual Organisation Management, the Sponsor of the User, those responsible for the assignment of attributes, or the User;
- Officer(s) or operational staff of the Infrastructure designated by the Infrastructure Management;
- Service Providers participating in the Infrastructure.

The Virtual Organisation Management must cooperate fully with the investigation and resolution of security incidents reported by the Security Officer(s) of any Infrastructure, including acting on any requests for suspension without delay.

Unless it is considered detrimental to the investigation and resolution of a security incident, the Virtual Organisation Management should contact the User that was or is about to be suspended. The Virtual Organisation may define a dispute resolution process by which a User can challenge a Suspension.
User's rights shall not be reinstated unless the Virtual Organisation Management has sent timely prior notification to all those who requested Suspension.

5.8 Membership Life Cycle: Termination

The Termination of Virtual Organisation membership is the removal of a member from the Virtual Organisation. Following Termination, the former member is no longer eligible to use Infrastructure Services that support the Virtual Organisation and the Virtual Organisation must no longer assert membership or attributes for the former member.

In absence of overriding reasons, a request by the User for removal must be honored.
The events that shall trigger re-evaluation of the User's membership of the Virtual Organisation include:

- a request by the Sponsor,
- failure to complete a membership Renewal process within the allotted time,
- end of collaboration between the User and the Virtual Organisation,
- end of collaboration between the User's Sponsor and the Virtual Organisation, if applicable,
- end of collaboration between the User and his/her Sponsor, if applicable.

6 PROTECTION AND PROCESSING OF PERSONAL DATA

The Virtual Organisation must have policies and procedures addressing the protection of the privacy of individual Users with regard to the processing of their *Personal Data* collected as a result of their membership in the Virtual Organisation and of their access to Services provided by any Infrastructure.

These policies must be made available in a visible and easily accessible way and Users must explicitly acknowledge acceptance of these policies (through the AUP and registration process).

The Virtual Organisation must inform the User (through the AUP and registration process) of the policies on the processing of *Personal Data* of those Service Providers with which it has entered into agreements and that can access the User's *Personal Data*.

It is recommended that any *Personal Data* stored by the Virtual Organisation is time-stamped in order to determine when it is appropriate to remove data that is no longer necessary for audit, traceability or any legal requirements.

7 AUDIT AND TRACEABILITY REQUIREMENTS

The Virtual Organisation must record and maintain an audit log of all membership lifecycle transactions. This audit log must be kept for a minimum period consistent with the Traceability and Logging Policies of all Infrastructures that provide Services to the Virtual Organisation. Audit logs containing personal *Registration Data* must not be retained beyond the maximum period allowed by the Policy on the processing of *Personal Data* of the Virtual Organisation (e.g. for as long as a member is registered and entitled to use Services and one year after this data is no longer associated with such an active membership or attribute assignment).

Events that must be logged include every request for:

- membership,
- assignment of or change to a member's attributes,
- assignment of or change to a member's assurance information,
- membership renewal,
- membership suspension,
- membership termination or re-evaluation.

Each logged event should record the date and time, the originator, the details of the event, and whether or not it was approved. The identity of the person granting or refusing the request should be recorded, including any verification steps involved and other people consulted, such as Sponsors.

8 REGISTRY AND REGISTRATION DATA

The Virtual Organisation must operate, or have operated on its behalf, a Registry that contains the membership data of the Virtual Organisation. This registry must be operated in a secure and trustworthy manner and in compliance with the security requirements of the Virtual Organisation and of the Infrastructures in terms of authentication, authorisation, access control, physical and network security, security vulnerability handling and security incident handling. The Registry must also be operated in a manner compliant with Sirtfi [2].

The Registry must store at least:

- *Registration Data*, including *Personal Data* of the User
- attributes assigned to members

The types of information recorded must be listed in the Policy on the processing of Personal Data of the Virtual Organisation.

9 REFERENCES

[1] Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi) - https://www.igtf.net/snctfi/
[2] Security Incident Response Trust Framework for Federated Identity (Sirtfi) - https://refeds.org/sirtfi

Security Incident Response Procedure

This procedure applies for any suspected or confirmed security breach with a potential impact on the *Infrastructure* or on other *Infrastructure* participants. Hereinafter, the term "participants" only includes those *Infrastructure* participants that are required to abide by this procedure.

This procedure is effective from November 18th, 2020.

Security Incident Response Procedure for Infrastructure Participants

1. Contain the security incident to avoid further propagation whilst aiming at carefully preserving evidence and logs. Record all actions taken, along with an accurate timestamp.
2. Report the security incident to the Infrastructure Security Contact within one local working day of the initial discovery or notification of the security incident.
3. In collaboration with the Infrastructure Security Contact, ensure all affected participants in the Infrastructure and federation (and, if applicable, in other federations), are notified via their security contact with a "heads-up" and can take action. In the case of a personal data breach, report the security incident to the Controller to ensure compliance with applicable GDPR provisions, and share additional information as necessary with all affected participants to enable them to comply with applicable GDPR provisions as well.
4. Announce suspension of service (if applicable) in accordance with Infrastructure, federation and inter-federation practices.
5. Perform appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
6. Share additional information as often as necessary to keep all affected participants up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
7. Respond to requests for assistance from other participants involved in the security incident within one working day.
8. Take corrective action, restore access to service (if applicable) and legitimate user access.
9. In collaboration with the Security Incident Response Coordinator, produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labeled TLP AMBER [3] or higher.
10. Update documentation and procedures as necessary.

Security Incident Response Procedure for the Infrastructure Security Contact

1. Assist Infrastructure participants in performing appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
2. Report the security incident to their federation security contact point within one local working day of the initial discovery or notification of the security incident.

3. Ensure all affected participants in the Infrastructure and federation (and, if applicable, in other federations) are notified via their security contact with a “heads-up” within one local working day. If other federations are affected, the eduGAIN security contact point must be notified, even if affected participants in all other federations have been contacted directly.
4. Coordinate the security incident resolution process and communication with affected participants until the security incident is resolved.
5. Ensure suspension of service (if applicable) is announced in accordance with Infrastructure, federation and inter-federation practices.
6. Share additional information as often as necessary to keep all affected participants up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
7. Assist and advise participants in taking corrective action, or restoring access to service (if applicable) and legitimate user access.
8. Produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labeled TLP AMBER [3] or higher.
9. Update documentation and procedures as necessary.

Policy on the Processing of Personal Data

This policy is effective from November 18th, 2020.

1 INTRODUCTION

This policy ensures that data collected as a result of the use of the Infrastructure is processed fairly and lawfully by Infrastructure participants. Some of this data, for example that relating to user registration, monitoring and accounting contains "personal data" as defined by the European Union (EU) [GDPR]. The collection and processing of personal data is subject to restrictions aimed at protecting the privacy of individuals.

2 DEFINITIONS

- *Personal Data*: any information relating to an identified or identifiable natural person [GDPR].
- *Processing (Processed)*: any operation or set of operations, including collection and storage, which is performed upon Personal Data [GDPR].
- *Controller*: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data[1] [GDPR] on behalf of an Infrastructure Participant.
- *Processor*: a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller [GDPR].

3 SCOPE

This policy covers Personal Data that is Processed as a prerequisite for or as a result of a User's use of Infrastructure services. Examples of such Personal Data include registration information, credential identifiers and usage, accounting, security and monitoring records.

This policy does not cover Personal Data relating to third parties included in datasets provided by the User or the research community to which they belong as part of their research activity. Examples of such data are medical datasets which may contain Personal Data.[1]

4 POLICY

By their activity in the Infrastructure, Participants:

- Declare that they have read, understood and will abide by the Principles of Personal Data Processing as set out below.

1 The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This policy does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

- Declare their acknowledgment that failure to abide by these Principles may result in exclusion from the Infrastructure, and that if such failure is thought to be the result of an unlawful act or results in unlawful information disclosure, they may be reported to the relevant legal authorities.

5 PRINCIPLES OF PERSONAL DATA PROCESSING

1. The User whose Personal Data is being Processed shall be treated fairly and in an open and transparent manner.
2. Personal Data of Users (hereinafter "Personal Data") shall be Processed only for those administrative, operational, accounting, monitoring and security purposes that are necessary for the safe and reliable operation of Infrastructure services, without prejudice to the Users' rights under the relevant laws.
3. Processing of Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are Processed.
4. Personal Data shall be accurate and, where necessary, kept up to date. Where Personal Data are found to be inaccurate or incomplete, having regard to the purposes for which they are Processed, they shall be rectified or purged.
5. Personal Data Processed for the purposes listed under paragraph 2 above shall not be kept for longer than the period defined in a relevant Infrastructure service policy governing the type of Personal Data record being Processed (e.g. registration, monitoring or accounting).
6. Appropriate technical and organisational measures shall be taken against unauthorised disclosure or Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data. As a minimum, Infrastructure Participants shall:
    a. Restrict access to stored Personal Data under their control to appropriate authorised individuals;
    b. Transmit Personal Data by network or other means in a manner to prevent disclosure to unauthorised individuals;
    c. Not disclose Personal Data unless in accordance with these Principles of Personal Data Processing;
    d. Appoint at least one Data Protection Officer (DPO) to which Users or other Infrastructure Participants can report suspected breaches of this policy;
    e. Respond to suspected breaches of this Policy promptly and effectively and take the appropriate action where a breach is found to have occurred;
    f. Define periodic audit intervals and procedures to ensure compliance to this Policy and make the results of such audits available to other Infrastructure Participants upon their request.
7. Each Infrastructure service interface provided for the User must provide, in a visible and accessible way, a Privacy Policy containing the following elements:
    a. Name and contact details of the Controller responsible for Processing Personal Data;
    b. Description of Personal Data being Processed;
    c. Purpose or purposes of Processing of Personal Data as well as the legal basis for the processing;
    d. Third party recipients of the personal data, if any; as well as the existence or absence of adequacy appropriate or suitable safeguards in case the recipient is not bound to GDPR.
    e. Retention period of the Personal Data Processed;
    f. Explanation of the rights of the Users according to GDPR;
    g. The contact details of the Controller's DPO to which the User should direct requests in relation to their rights above;
    h. Reference to this Policy.
8. Personal Data may only be transferred to or otherwise shared with individuals or organisations where the recipient:

a. has agreed to be bound by this Policy and the set of common Infrastructure policies, or
b. is part of a recognised Computer Incident Response Team framework and as part of an incident investigation to prevent active or suspected misuse of Infrastructure services, or
c. presents an appropriately enforced legal request.

Acceptable Use Policy Template

When using the baseline AUP text below, curly brackets "{ }" (colored blue) indicate text which should be replaced as appropriate to the community, agency or infrastructure presenting the AUP to the user. Angle brackets "< >" (colored green) indicate text which is optional and should be deleted or replaced as indicated. Other text should not be changed.

This policy is effective from {insert date}.

1 Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by {community, agency, or infrastructure name} for the purpose of {describe the stated goals and policies governing the intended use}.

<To further define and limit what constitutes acceptable use, the community, agency, or infrastructure may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1-10 below, whose wording and numbering must not be changed.>

By registering as a user you declare that you have read, understood and will abide by the following conditions of use:

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities.
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organisation or to law enforcement.

<Insert additional numbered clauses here.>

11. You shall provide appropriate acknowledgement of support or citation for your use of the resources/services provided as required by the body or bodies granting you access.

The administrative contact for this AUP is: {email address for the community, agency, or infrastructure name}
The security contact for this AUP is: {email address for the community, agency, or infrastructure security contact}
The privacy statements (e.g. Privacy Notices) are located at: {URL}
Applicable service level agreements are located at: <URLs>

Privacy Policy Template

When using the Privacy Policy template text below, the text colored blue should be replaced with information specific to the Service, in line with the indications in the text. Other text should not be changed.

The Privacy Policy is designed to fulfill the GDPR requirements:

- *Who or what is your Data Controller?*
- *Will your Research Community have a Data Protection Officer?*
- *Which information do you need to collect on the user? Is this minimised?*
- *Specific data collected by each service may vary. Can your Infrastructure provide a template statement for all services?*

This policy is effective from <insert date>.

1 Privacy Policy

1. Name of the Service	SHOULD be the same as mdui:DisplayName
2. Description of the Service	SHOULD be the same as mdui:Description
3. Data Controller and a contact person	You may wish to include the Data Controller defined for the Infrastructure, rather than per-service
4. Data Controller's data protection officer (if applicable)	
5. Jurisdiction and supervisory authority	The country in which the Service Provider is established and whose laws are applied. SHOULD be an ISO 3166 code followed by the name of the country and its subdivision if necessary for qualifying the jurisdiction. How to lodge a complaint to the competent Data protection authority: Instructions to lodge a complaint are available at...
6. Personal data processed and the legal basis	A. Personal data retrieved from your Home organisation: • your unique user identifier (SAML persistent identifier) * • your role in your Home Organisation (eduPersonAffiliation attribute) * • your name * • ... B. Personal data gathered from yourself • logfiles on the service activity * • your profile • ... * = the personal data is necessary for providing the Service. Other personal data is processed because you have consented to it. Please make sure the list A. matches the list of requested attributes in the Service Provider's SAML 2.0 metadata.
7. Purpose of the processing of personal data	Don't forget to describe also the purpose of the log files, if they contain personal data (they usually do).

8. Third parties to whom personal data is disclosed	Notice clause of the Code of Conduct for Service Providers. Are the 3rd parties outside EU/EEA or the countries or international organisations whose data protection EC has decided to be adequate? If yes, references to the appropriate or suitable safeguards.
9. How to access, rectify and delete the personal data and object to its processing	Contact the contact personal above. To rectify the data released by your Home Organisation, contact your Home Organisation's IT helpdesk.
10. Withdrawal of consent	If personal data is processed on user consent, how can he/she withdraw it?
11. Data portability	Can the user request his/her data be ported to another Service? How?
12. Data retention	When the user record is going to be deleted or anonymised? Remember, you cannot store user records infinitely. It is not sufficient that you promise to delete user records on request. Instead, consider defining an explicit period. Personal data is deleted on request of the user or if the user hasn't used the Service for <period of time> (e.g., 18 months).
13. Data Protection Code of Conduct	Your personal data will be protected according to the Code of Conduct for Service Providers [1], a common standard for the research and higher education sector to protect your privacy

REFERENCES

[1] GÉANT Data Protection Code of Conduct - http://www.geant.net/uri/dataprotection-code-of-conduct/v1

Checklists for Infrastructure Participants

This document provides simple checklists of actions for Infrastructure participants, to ensure compliance with the Top Level Infrastructure Policy. This document is meant as a helper and does not guarantee completeness.

1 Infrastructure Management

- Approve the HIFIS Top Level Policy
- Maintain a webserver with up-to-date policies (and templates for AUP and PP)
- Appoint the Data Controller (legal or natural person)
- Specify Infrastructure Security Contact (e.g. mailing list)
- Maintain registry of Privacy Policies for all services and for the Infrastructure itself
- Make sure all participant requirements are met
- Oversee and approve service onboarding process
- Approve VO registration and deregistration

2 Service Providers

- Specify Security Contact
- Provide Privacy Policy
- (optionally) Provide Service Acceptable Use Policy
- (optionally) Provide Service Access Policy:
  - supported / minimal level of assurance
  - additional attributes or entitlements besides the REFEDS R&S attribute bundle
- Cooperate with other participants in case of user misconduct

3 Identity Providers

- Specify Security Contact
- Support REFEDS RAF
- Support REFEDS R&S
- Cooperate with other participants in case of user misconduct
- Ensure that it can supply the attributes defined in the R&S Entity Category
- Ensure that it can supply additional attributes as required by a service's SAP
- Alert users of the AUPs in force in the Federation and commit them to compliance
- Inform users of the data to be transmitted to a Service Provider
- Make bilateral agreements with Service Providers for use of individual services, as necessary

4 Virtual Organisation Management

- Specify two or more VO Managers / Contacts
- Specify VO Security Contact
- Responsible for implementation of procedures on behalf of Virtual Organisation
- Define Acceptable Use Policy (template is provided)
- Define Privacy Policy (template is provided)
- Abide by the Virtual Organisation Membership Management Policy (VOMMP):
  - Manage user membership according to VOMMP

- Keep an appropriate audit trail regarding user management

5 SP-IdP Proxy

- Specify Security Contact
- Provide Privacy Policy
  - (Currently: https://login.helmholtz-data-federation.de/unitygw/VAADIN/files/data-privacy-statement.html)
- Support REFEDS RAF

Virtual Organisation (VO) Life Cycle Management

1 VO Registration

The VO registration procedure is initiated by the VO Manager.

Requirements for VO Manager:

- anyone who can authenticate with assurance level RAF Cappuccino
- employee of a Helmholtz institution

VO registration form:

- VO name
  - naming scheme and other requirements should be mentioned here
- VO description / purpose
  - this is (among others) to avoid duplicate VOs for the same effort
  - the VO Manager must have access to information on existing VOs
- VO AUP
- VO contact information:
  - VO Manager (Name, Postal Address, Email, Telephone)
  - VO Security Contact (Name, Postal Address, Email, Telephone)

Policies to provide (Templates are provided):

- Acceptable Use Policy (AUP) (Template: <insert link>, or use the HIFIS AUP)
- Privacy Policy (Template: <insert link>, or use the Proxy PP)

Policies to read and accept:

- Top Level Infrastructure Policy
- Community Membership Management Policy
- Security Incident Response Procedure
- Policy on the Processing of Personal Data

The VO Supervisor evaluates the registration request and decides whether to accept or reject it.

Acceptance criteria (all must be met):

- there is no existing VO with significantly overlapping goals.
- the VO registration form contains correct and complete data.
- the VO has provided, read and accepted all the required policies.

2 VO Deregistration

The VO deregistration can be initiated by:

- VO Manager
- VO Supervisor
- VO User
- Infrastructure Management

VO deregistration form:

- Role of the requester (from list above)
- Reason for deregistration request
- Proposed timeline for decommissioning
- Assessment of the VO activities in the last 12 months (only if requester is not VO Manager)

The VO Supervisor evaluates the deregistration request and decides whether to accept or reject it. If the requester is the VO Manager, then the request is automatically accepted.

Acceptance Criteria when the requester is not the VO Manager (all must be met):

- the VO has not produced accounting data for more than one year
- the VO Manager has been notified and given a deadline (minimum 1 month) to respond
- the VO Manager has agreed to the deregistration request or the VO Manager has not responded to the request for feedback before the specified deadline