AARC Policy Development Kit

Task Plan & Notes: https://wiki.geant.org/display/AARC/Policy+Development+Kit
Author list: U. Stevanovic, H. Short, D. Groep, I. Neilson, I. Mikhailava

Abstract

Accessing, using, and operating services for research in today’s world, as a rule, is inherently distributed, where users are expecting to access resources not located in their Home Organization. In this complex environment, the question of trust for both users and resource providers, or Infrastructures, becomes paramount.

In order to regulate and facilitate this trust, a set of policies is necessary. These policies, which are essentially a set of documents, outline the operation and operational measures undertaken by the Infrastructure to properly provide services. As such, the policies cover, among others, security measures, users’ management, data protection.

The policies adopted and followed by the Infrastructure are required for the Infrastructure to properly function. They can be used to show legal compliance, demonstrate to the users suitable operational and technical measures, and govern the Infrastructure operation

The policies outlined here are not to be used as a legal advice.

Introduction

This material provides new or evolving Research Communities with the guidance they need to develop a complete policy suite supporting Federated Identity Management. It is designed to support those making operational or management decisions for Research Communities. This work is based on the Snctfi Trust Framework, developed by AARC and the wider community.

As Research Communities seek to increase their interaction with external identities, such as those from identity federations or social providers, certain provisions should be made for Data Protection, Membership Management and Security Incident Response. The policies presented here aim to take trust, assurance and governance aspects into account whilst providing a coherent set of documents to be adopted by interested parties. Research Communities may manage their own Infrastructure, or a generic e-Infrastructure may provide computing for multiple Research Communities; the word Infrastructure is used throughout this material and intends to cover both scenarios.

Policies are essential for setting expectations for participants in an Infrastructure, stretching from the Infrastructure management to the researchers themselves. Conversely, a violation of policy may be classified as a security incident and may warrant, and give grounds for, investigation to protect the Community. Policy decisions may or may not be enforced on a technical level; the

Infrastructure themselves will be best placed to define the permitted usage of their resources through a combination of technology and documentation.

When incorporating external identities into their ecosystem, Infrastructures are faced with new questions, including but not limited to:

- Which policies do we need to legally receive attributes contained in federated identities?
- What is a reasonable expectation of the level of assurance of incoming identities?
- How can I ensure that all my users are covered by an incident response capability?
- What checks and measures should I put in place when managing the users of my community services, or members of virtual organisations?

The material provided here aims to address these concerns by highlighting current best practices and reusable policy material. These policies should be approved by High Level Management, who should be included early in the decision making process.

Scope

The policies presented are relevant for an Infrastructure operating a Service Provider Proxy that represents the bound set of services in an identity federation. The policies are to be adopted by the Infrastructure itself and, where appropriate, additional policies are suggested for Infrastructure participants such as Services, User Community Management or Users. The Infrastructure may be for the sole use of a single Research Community, or may provide computing services to multiple Research Communities; the policies presented are designed to be flexible.

Policy Impact on Infrastructure Operation

Policy should be thought about early in the design phase of a project. Although it is tempting to view them as an additional layer on top of an architecture, the technical implications of policy can have considerable impact on design decisions. Some possible points to highlight are:

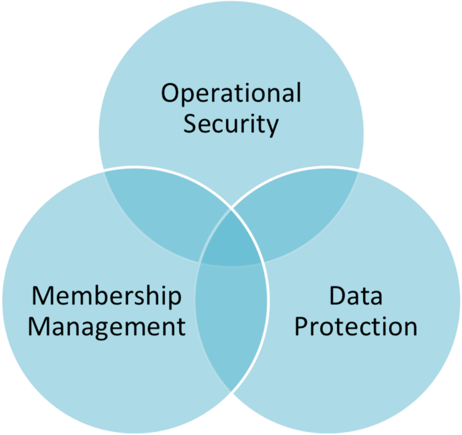
- The ability to display policy documents (such as privacy statements and Acceptable Use Policies) to users during workflows
- Limiting usage to user credentials with appropriate assurance
- Data minimisation, storage, retrieval and deletion, including fine grained access control
- Traceability across infrastructure services
- The capability to suspend users and revoke credentials
- The ability to announce suspension of services

This does not represent an exhaustive list and you will certainly discover additional technical impacts as you review your policy set.

Infrastructure Policies and Frameworks

As exposed by the research carried out in the AARC project [AARC-BLUEPRINT], Infrastructures typically deploy Service-Provider-Proxies that group federated Services behind a single entry point. Snctfi, the Scalable Negotiator for a Community Trust Framework in Federated Infrastructures, is a framework to ensure that such an entry point exposed to an identity federation is capable of representing all the internal services with regards to their adoption of policies. The key policies needed for compliance with the framework are:

1. Policies to stipulate requirements for Data Protection and Privacy
2. Policies to regulate the behaviour of the management of collections of users
3. Policies to coordinate the implementation of operational security practices and incident response

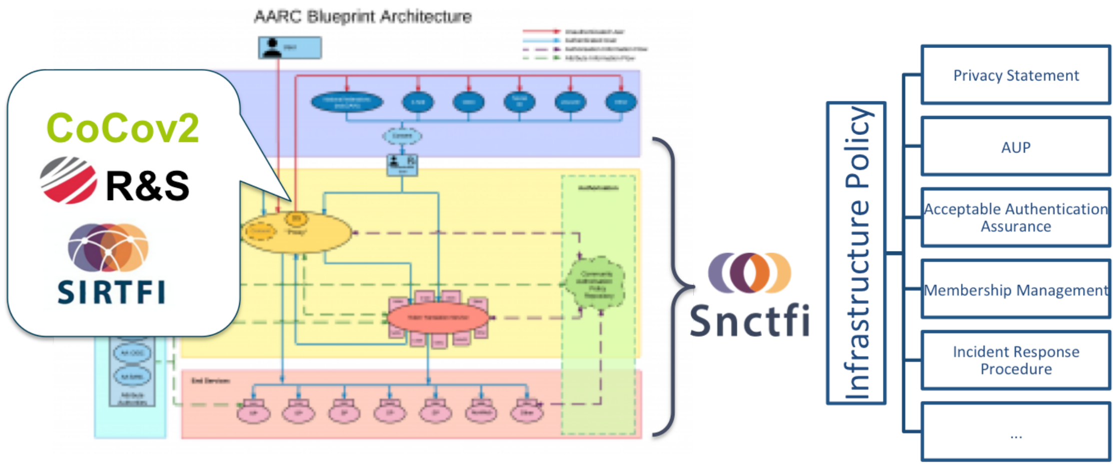


These three areas are expanded below, with template policies provided. Once the relevant policies have been put in place, it is recommended that Infrastructures perform a self-assessment against the Snctfi Framework itself. More information on Snctfi can be found at [AARC-SNCTFI].

In addition to the policies expected by Snctfi, several frameworks are encouraged by the wider Federated Identity Community. The frameworks aim to support responsible data handling and promote trust between federated organisations. It is suggested that these frameworks be adopted and asserted by the proxy on behalf of the Infrastructure.

1. The GEANT Data Protection Code of Conduct (CoCov2)
2. The Research and Scholarship Entity Category (R&S)
3. The Security Incident Response Framework for Federated Identity (Sirtfi)

Armed with the recommended policy documents, and complying with best-practice community frameworks, an Infrastructure is able to support their users' activities in a federated environment.


AARC Blueprint Architecture
CoCov2
R&S
SIRTFI
Snctfi
Infrastructure Policy
Privacy Statement
AUP
Acceptable Authentication Assurance
Membership Management
Incident Response Procedure
...

Frameworks

The following frameworks are considered best practice for Research Communities enabling federated access. They enable trust and promote attribute release from the wider identity federation.

Sirtfi Trust Framework

What is this for? Sirtfi demonstrates that an organisation complies with baseline expectations for operational security and incident response in the context of identity federations
Does my Infrastructure need it? All Service Providers and Identity Providers in Identity Federations are encouraged to support Sirtfi. To mitigate risk, your Infrastructure may choose to restrict its interactions to only those federated organisations who are able to comply with the framework. As well as the Infrastructure itself supporting Sirtfi, it is highly recommended that each connected service should support Sirtfi by providing their Security Contact and abiding by Sirtfi requirements. Your Infrastructure should keep track of Security Contacts for connected services, ensure that participants are aware of the Security Incident Response Procedure and test preparedness for such a procedure regularly.
What do I need to do? Follow the training at [GEANT MOODLE] Further information can be found at https://aarc-project.eu/policies/sirtfi/

Research and Scholarship Entity Category

What is this for? The Research and Scholarship Entity Category identifies federated services that are operated for the purpose of supporting research and scholarship activity. Identity Providers demonstrate their support for research and scholarship by releasing a pre-defined set of attributes for a user, including their name, email address and additional low-risk information that may be useful for their activities.

Does my Infrastructure need it? Yes. Many Identity Providers will not release user attributes to a service that does not publish the Research and Scholarship Entity Category.
What do I need to do? An application should be made to your federation operator, who will check whether your Infrastructure proxy complies with a basic set of requirements. More information is available at https://refeds.org/category/research-and-scholarship

GÉANT Data Protection Code of Conduct

What is this for? The Data protection Code of Conduct (DPCoCo) describes an approach to meet the requirements of the EU Data Protection Directive and with the upcoming General Data Protection Regulation (GDPR) in federated identity management. The Data protection Code of Conduct defines behavioral rules for Service Providers which want to receive user attributes from the Identity Providers managed by the Home Organisations.
Does my Infrastructure need it? Most likely, yes. As said, DPCoCo will provide a scalable and harmonised approach when processing of users' personal data by the service providers is needed for accessing said services. In short, whenever users are accessing services, facilitated by the release of users' information and its subsequent processing by the service providers, which is the most common scenario in federated environment, there needs to be a legal basis for such processing. DPCoCo aims to provide such basis.
What do I need to do? For now, follow the current status of the DPCoCo process, which is still in the process of consultation. However, once the final version of the document is submitted for consideration by Data Protection Authorities (national Data Protection Agency or EU one), we strongly recommend for all IdPs and all SPs to adopt it and adhere to it.
More information can be found here (home page of the overall effort) and here (new DPCoCo version). Explanatory memorandum offers more explanation about the reasons for CoCo and its approach.

Policies

The following policies are a recommended minimum to satisfy the Snctfi framework. The top level Infrastrastructure Policy serves to bind the entire policy set and stipulates requirements on each of the participants; Management, Infrastructure Security Contact, User Community Management, Service Management (including the Proxy Operator) and the User. The top policy identifies additional policy documents; in this case the five that are mandatory for Snctfi compliance.

Your Infrastructure may wish to define additional policies, such as Service Eligibility, Disaster Recovery, or Data Management; these policies should be linked into the Infrastructure Policy to ensure a coherent Policy set.

		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	Abides by
Data Protection	Privacy Statement	Defines			Defines	Views
Membership Management	Community Membership Management Policy	Defines		Abides by		
	Acceptable Use Policy	Defines		Defines		Abides by
	Acceptable Authentication Assurance	Defines		Abides by	Abides by	
Operational Security	Incident Response Procedure	Defines	Abides by		Abides by	

Top Level

Infrastructure Policy

What is this for? Infrastructure proxies represent multiple participants, Research Services and User Community Management services being key elements, in addition to end users and the management bodies responsible for the Infrastructure itself. For the Infrastructure to adequately protect its assets, it is essential that the authorised behaviour of these participants be defined

and communicated. A high level Infrastructure Policy defines the roles and responsibilities of the participants, and points to additional policies as required. It serves to bind the policies together.
Does my Infrastructure need it? It is highly recommended. Whilst defining this policy we encourage Infrastructures to consider additional policies they may need due to the specific activity of their Services or Users, such as traceability, accounting or virtual machine management.
What do I need to do? The template below provides a starting point for an Infrastructure Policy but it should not be used without thorough analysis, amendment and approval from suitable Management bodies.

Data Protection

Why Data Protection?

Operating and using the infrastructure inevitably involves collection and processing of data that may contain personal information of people residing in EU. Such data must be processed lawfully, in accordance to national laws and especially in accordance with the General Data Protection Regulation (GDPR) [GDPR].

Implications of the GDPR

As a Regulation, it is legally valid in all EU countries, without the need for the ratifications by the national parliaments. However, certain liberty is left to the states to further define and regulate in a number of areas, which may cause certain inconsistencies in applying the GDPR.
An additional effect of the GDPR is the expanded territorial scope, where now the GDPR applies to all persons (natural/legal) processing the personal data of people residing in the EEA, regardless of the said persons location. Penalties have been increased, and the conditions for consent are strengthened. Furthermore, additional requirements are introduced: Breach notification, Right to access, Privacy by design, Data portability, Data Protection Officers (DPO), among others.

Which actions are required?

All organisations must conduct an internal review to check whether they are processing personal data in compliance with the GDPR. That could mean that there is a need to change their current practices to comply, for e.g., Privacy by design. There would also probably exists a need to conduct a Data Privacy Impact Assessment (DPIA).

Privacy Statement

What is this for? Privacy notices are used to inform the users about how their data are processed. Information that is needed to provide to the users must be concise and easily accessible, written in clear and plain language, and free of charge [ICO-PRIV-NOT]. Privacy statements are required for each service to which personal data is released, this includes services accessed by a User directly and services where personal data is transferred.
Does my Infrastructure need it? Yes, both for the Infrastructure itself and on a per-Service basis. All data controllers, i.e. any entity receiving personal information, must inform the users that their personal data are being processed.

What do I need to do? Each service doing data processing must provide a privacy policy to the users. The template below should be used carefully, and modified to fit the needs, requirements, and actual processing activities that are applied. The Infrastructure may choose to provide a pre-filled template to Services.

Risk Assessment

What is this for? The GDPR is envisioning a procedure for assessing the risks for the users when processing their personal data. This procedure is called Data Protection Impact Assessment (DPIA). In order to assess whether conducting a DPIA is mandatory, a certain risk assessment procedure has to be performed. The process of estimating risks for the users is not a policy per se, however the process and its conclusions should be documented. As mentioned by the European Data Protection Board (EDPB) the DPIA, and by extension the risk assessment, can be understood and used as a method of showing compliance with the GDPR.
Does my Infrastructure need it? As mentioned, a DPIA itself may not be necessary. But, conducting a risk assessment (that, among others, demonstrate why "official" DPIA is not necessary) is highly recommended. This procedure may show, among others, how is Infrastructure processing and protecting personal data of its users.
What do I need to do? The Infrastructure must know all its data processing functions that are taking place. For each of these, a risk assessment "for the rights and freedoms of the natural persons" should be conducted. These will then provide with more information whether an actual DPIA should be conducted. Depending on the processing, that might not be necessary. For example, the [AARC-G042] guideline is arguing that processing personal data for providing an access to a service does not meet the need for a DPIA. However, others types of personal data processing may require a DPIA. EDPB has issued a preliminary opinion which processing operations may merit an actual DPIA.

Membership Management

The Community membership management is administered via several policies, those mandatory for Snctfi compliance are the Community Membership Management Policy, Acceptable Use Policy, and Acceptable Authentication Assurance. These policies are needed to establish and foster trust between Infrastructures and Communities, and to demonstrate and instruct the proper behaviour of the User and User Communities. The Infrastructure and Community must ensure that the users are aware that they have certain responsibilities and roles delineated in these policies.

We strongly encourage the adoption of these policies to direct and regulate the Community membership management. Naturally, when one creates and adopts these policies, data protection and privacy consideration must be taken into account.

Community Membership Management Policy

What is this for? This policy is designed to establish trust between a Community and other Communities, Infrastructures, and the R&E federations. The behaviour of the Community and its users must be appropriate and facilitate the Community's compliance with the requirements of the Infrastructure's policies, especially Infrastructure top-level policy. It introduces definitions and roles which Community users and management must fulfill. It also provides rules for managing the membership life cycle, including but not limited to, registration, renewal, suspension. Additionally, this policy may contain provisions for proper protection and processing of personal data.

Does my Infrastructure need it? Yes. The Infrastructure should define a Community Membership Management policy that all User Communities must adopt.

What do I need to do? The Infrastructure should create a policy that details how Communities must manage their users. A Template is provided here, however, it should be used in accordance with the community requirements and careful consideration of Infrastructure needs should be taken into account.

Acceptable Use Policy

What is this for? An acceptable use policy provides end users with rules and regulations to which they must conform when accessing a service. A breach of the acceptable use policy may constitute an incident and give grounds for suspension or further investigation.

Does my Infrastructure need it? It is highly recommended that an Acceptable Use Policy be put in place. The Acceptable Use Policy is typically displayed to users upon registration and is consequently provided by the Research Community.

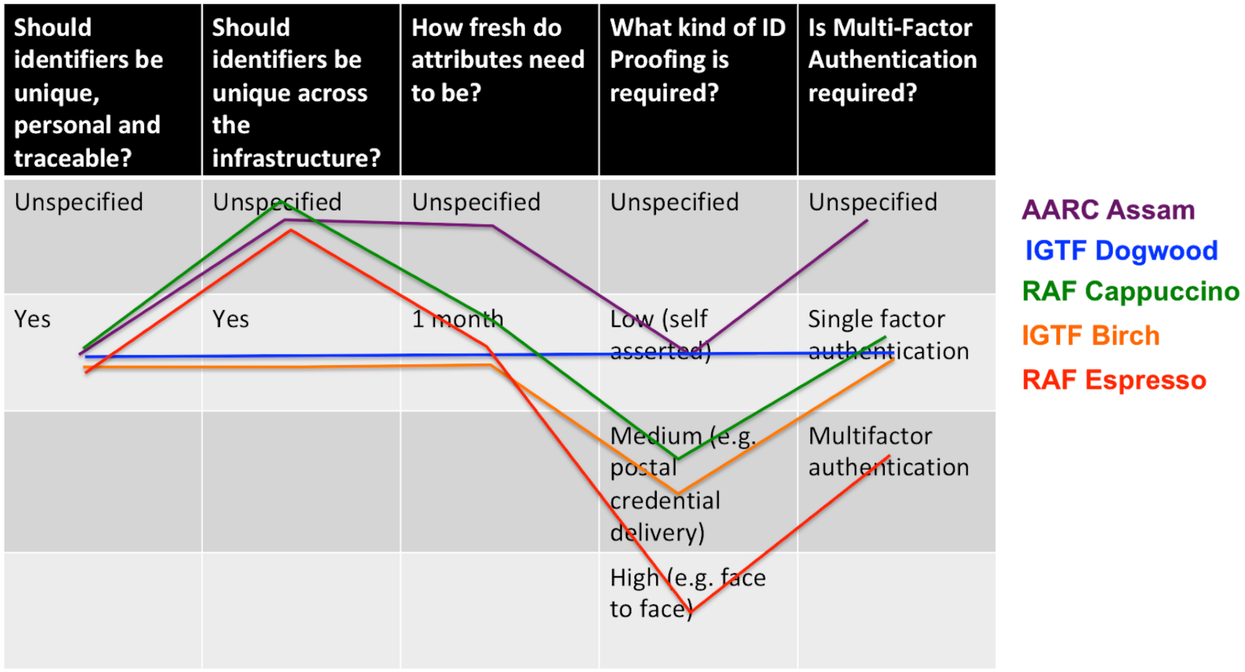
What do I need to do? The template below provides a starting point for an Acceptable Use Policy but it should not be used without thorough analysis, amendment and approval from suitable Management bodies. A Research Community operating on a generic Infrastructure may wish to add additionally restrictive clauses to the Infrastructure AUP.

Acceptable Authentication Assurance

What is this for? Assurance Information conveys the level of confidence about the users' Identity; this includes controls on identifier uniqueness, identity proofing, attribute freshness and multi factor authentication among other factors. Identity Providers, Attribute Authorities and Service Provider Proxies may all contribute to the Level of Assurance (LoA) of an identity that is passed to a Research Service. The wider community has evolved several standardised means of expressing LoA to enhance interoperability between Research Services and Infrastructures. Typically the proxy will issue identity assertions that include the LoA of the credential. Certain critical research services may require higher LoA than others and may choose to restrict access based on the LoA standard expressed.

Does my Infrastructure need it? It is strongly suggested that an acceptable minimum assurance profile be defined for the Infrastructure, or a subset of its services, and provisions put in place to ensure that only approved users can access critical services. This may include measures such as supporting identity vetting, or restricting access to only certain Identity Providers.

What do I need to do? To get a first approximation of the LoA profile appropriate for a service or set of services, use this diagram to match your needs to a standard profile from AARC Guideline 21 [AARC-G021 Exchange of specific assurance information between Infrastructures]. Assurance profiles should be read thoroughly and adopted according to the guidelines.



Should identifiers be unique, personal and traceable?	Should identifiers is unique across the infrastructure?	How fresh do attributes need to be?	What kind of ID Proofing is required?	Is Multi-Factor Authentication required?
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Yes	Yes	1 month	Low (self asserted)	Single factor authentication
			Medium (e.g. postal credential delivery)	Multifactor authentication
			High (e.g. face to face)	

The chosen profile, or profiles, should be included in the template for Infrastructure Acceptable Authentication Assurance that should be adopted by Infrastructure elements contributing to assurance, typically Attribute Authorities and the Proxy. The template here provides a starting point for an Infrastructure Acceptable Authentication Assurance Policy but it should not be used without thorough analysis, amendment and approval from suitable Management bodies. In particular, it is up to the Infrastructure to decide which Assurance Profiles are suitable, how controls will be implemented and how the LoA will be communicated to Services.

Operational Security

Best practices in Operational Security for Research Communities encourage assertion of compliance with the Sirtfi Trust Framework by the SP Proxy, and the adoption of an Incident Response Procedure

Incident Response Procedure

What is this for? An Incident Response Procedure allows organisations to respond to security incidents in a consistent and considered manner and stipulates the steps to ensure an incident is fully resolved. In an Infrastructure this is particularly important since there are multiple participants who must collaborate. Fundamental to Incident Response is the role of an Incident Coordinator, it is suggested that the Infrastructure nominate an Security Contact to play this role and to interact with external identity federations.

Does my Infrastructure need it? Yes. An incident response procedure is a requirement of the Sirtfi framework. Your Infrastructure should ensure that it is able to respond to security incidents as part of a demonstration of its security capability. Data Protection regulations require that appropriate security measures be in place to mitigate risk and a security incident response procedure plays a crucial role in an Infrastructure's ability to recover.

What do I need to do? The template below is provided as a starting point. Your Infrastructure should identify a central Infrastructure Security Contact, whether that be an individual or an established team. In addition, each Service must nominate a Security Contact. The infrastructure should ensure that the Incident Response Procedure is known by all participants.

Policy Templates

Top Level Infrastructure Policy Template

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

The following template is based on work by EGI.eu, licensed under a Creative Commons Attribution 4.0 International License.
https://documents.egi.eu/public/RetrieveFile?docid=3015&version=3&filename=EGI-SPG-SecurityPolicy-V2.pdf

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 italicised 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 italicised 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*. □

Other terms are defined in the Glossary [R3]. □In this document the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' are to be interpreted as described in RFC 2119 [R4] □2.2

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

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.

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.
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.
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 [R1].
For *Services* receiving personal data, a Privacy Statement compliant with the GEANT Data Protection Code of Conduct 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 authorised 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 minimised, documented, time-limited and authorised 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 recognised 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 recognised 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] <Insert a link to all Infrastructure policies>

Membership Management Policy Template

- Which information do you need to collect on your users? Name, contact information, nationality?
- How long is membership valid?
- How often do your users need to sign an AUP?

The following is based on the EGI Community Membership Management policy.
Taken from:
https://docs.google.com/document/d/1vPcAja1EyTp-kJPvJpwu3NSd8e1aVcytY3nSGthWNLU/edit#

This policy is effective from <insert date>.

INTRODUCTION

This policy is designed to establish trust between a Community and other Communities, Infrastructures, and the R&E federations. The behaviour of the Community and its users must be appropriate and facilitate the Community's compliance with the requirements of the Snctfi document [ref]. The identifiers of requirements from the Snctfi document are provided herein for ease of reference.

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

DEFINITIONS

A Community is a set of one or more groups of persons (Users), organised with a common purpose, with a Community Management willing to take responsibility for all sub-groups, jointly granted access to one or more Infrastructures. It may serve as an entity which acts as the interface between the individual Users and an Infrastructure. In general, the members of the Community will not need to separately negotiate access with Service Providers or Infrastructures (hereafter jointly called Infrastructures).

Examples of Communities include, but are not limited to: User groups, Virtual Organisations, Research Communities, Research Infrastructures, Virtual Research Communities, Projects, Communities authorised to use particular portals or gateways, and geographically organised communities.

Other terms are defined in the Glossary [ref].

INDIVIDUAL USERS

The Community must define an Acceptable Use Policy (AUP) [ref]. The AUP must be shown to all persons joining the Community. Acceptance of the AUP by Community 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 Community [ref]. The AUP must address at least the following areas:

- The aims and purposes, and the basis of membership of the Community
- Acceptable use
- Non-acceptable use
- Maintenance of user registration data
- Protection and use of credentials
- Data protection and privacy

The Community may rely on an Infrastructure AUP to address one or more of these requirements, provided that acceptance of such an Infrastructure AUP, in addition to the Community AUP, by the User is a prerequisite for registration. The Community AUP must not be in conflict with the referenced Infrastructure AUPs.

The data protection and privacy section of the AUP must address the relationship with the Infrastructure policies on the Processing of Personal Data, Security Traceability and Logging, and Service Operations Security.

Community 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 [ref], as soon as is feasible.

Hosts, Services and/or Robots (automated processes acting on behalf of the Community or a User) may be registered as members of the Community. 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 Resources assigned to the Community.

COMMUNITY MANAGER AND OTHER ROLES

The Community must define a Community Manager role and assign this role to two or more individuals. The Community Manager 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 [ref].

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

The Community Manager must implement procedures that ensure the accuracy of individual user registration data for all Community 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) [ref] and only stored and processed in compliance with applicable Data Protection legislation.

Other Community roles, such as additional management personnel and security contacts must be defined and assigned to individuals as specified in the Community Operations Security Policy [ref] or as required by the Infrastructure.

COMMUNITY

Aims and Purposes

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

Membership

The Community Manager is responsible for the Community Membership life cycle process of its Users [ref]. This responsibility may be devolved to designated personnel in the Community or in the Infrastructure, and their trusted agents (such as Institute Representatives or Resource Centre Managers), hereafter collectively called Sponsors.

The Community procedures must

- unambiguously name the individuals who take responsibility for the validity of the Registration Data provided [ref],
- ensure there is a way of contacting the User identified as responsible for an action while using Infrastructure services as a member of the Community [ref], and
- identify those with the authority to exercise control over the rights of its members to use the Infrastructure Resources assigned to the Community.

The Community must be aware that inappropriate actions by an individual member of the Community may adversely affect the ability of other members of the Community to use an Infrastructure [ref].

Membership Life Cycle: Registration

Membership Registration is the process by which an applicant joins the Community 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 [ref]. Reasonable efforts must be spent to validate the data.

The applicant must agree to abide by the AUP of the Community, and agree to use Resources of the Infrastructures exclusively for the Aims and Purposes of the Community.

Membership Life Cycle: Assignment of Attributes

Assignment of attributes (such as group membership, entitlements, or roles) shall be the responsibility of the Community Manager 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 Community and the Infrastructures. Attributes shall be assigned only for as long as they are applicable.

Membership Life Cycle: Renewal

Membership Renewal is the process by which a User remains a member eligible to use Infrastructure Resources assigned to the Community. Membership Renewal procedures must make a reasonable effort to

- ensure that accurate Registration Data is maintained [RC4,RC5] for all eligible Users
- confirm continued eligibility of the User to use Infrastructure Resources assigned to the Community
- confirm continued eligibility of the User to any attributes
- ensure the reaffirmation of acceptance of the AUP of the Community

The maximum time span between Registration and Renewal, and between Renewals, for all Community members who act as responsible persons towards the Infrastructure, shall be <INSERT RENEWAL TIMESPAN>. The User shall be able to correct and amend their Registration Data at any time.

Membership Life Cycle: Suspension

The Suspension of Community membership is the temporary revocation of full or partial rights and of any attributes. Suspension is done by or on behalf of the Community Manager.

A User should be suspended when the Community Manager 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 Community Manager, the Sponsor of the User, those responsible for the assignment of attributes, or the User
- Security Officer(s) or designated operational staff of the Infrastructure
- Resource Centres participating in the Infrastructure

The Community Manager must cooperate fully with the investigation and resolution of security incidents reported by the Security Officer(s) of any Infrastructure [ref], including acting on any requests for suspension without delay.

Unless it is considered detrimental to the investigation and resolution of a security incident, the Community Manager should contact the User that was or is about to be suspended. The Community may define a dispute resolution process by which a User can challenge a Suspension.

User's rights shall not be reinstated unless the Community Manager has sent timely prior notification to all those who requested Suspension.

Membership Life Cycle: Termination

The Termination of Community membership is the removal of a member from the Community. Following Termination, the former member is no longer eligible to use Infrastructure Resources assigned to the Community and the Community 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 honoured.

The events that shall trigger re-evaluation of the User's membership of the Community 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 Community,
- end of collaboration between the User's Sponsor and the Community, if applicable,

- end of collaboration between the User and his/her Sponsor, if applicable.

PROTECTION AND PROCESSING OF PERSONAL DATA

The Community 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 Community and of their access to resources 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 [ref] (through the AUP and registration process).

The Community must inform the User (through the AUP and registration process) of the policies on the processing of Personal Data of those providers with which it has entered into agreements and that can access the User’s Personal Data [ref].

The Policy on the processing of Personal Data of the Community [ref] shall address at least the items in A.5 section 7 of the Template Policy on the Processing of Personal Data of the AARC Recommendations and template policies for the processing of personal data [Ref], as amended from time to time.

It is recommended that any personal data stored by the Community 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.

AUDIT AND TRACEABILITY REQUIREMENTS

The Community 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 resources to the Community. 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 Community (e.g. for as long as a member is registered and entitled to use resources 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,
- 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.

REGISTRY AND REGISTRATION DATA

The Community must operate, or have operated on its behalf, a Registry that contains the membership data of the Community. This registry must be operated in a secure and trustworthy manner and in compliance with the security requirements of the Community and of the

Infrastructures [OS1] 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 REFEDS Sirtfi version 1 [Ref] [OS3].

The Registry must store at least:

- Registration data, including personal data of the User
- attributes assigned to members
- <Add or delete lines as required>

The Registration data for a User comprises verified information on at least:

- family name(s)
- given name(s)
- the employing organisation name and address
- any applicable Sponsor identity
- a professional email address
- unique and non-reassigned identifier(s) of the User and the source of authority of each identifier
- <Add or delete lines as required>

and is recommended to contain:

- professional contact telephone number so as to inform the User promptly during the investigation of security incidents and of lifecycle events
- other contact information, as voluntarily provided and maintained by the User.

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

Acceptable Authentication Assurance Policy Template

- Which identity providers are acceptable for your infrastructure? SAML Identity Federation IdPs? Social providers such as Google, Facebook etc?
- How much certainty does your community require of the identity? How will you validate this for each identity provider?
- How can you ensure that each user is covered by a security incident response capability at their home organisation?
- Do your services, or a subset, require step-up (multi-factor) authentication?

Taken from
https://documents.egi.eu/public/RetrieveFile?docid=2930&version=4&filename=EGI-SPG-AuthNAssurance-V1.pdf

INTRODUCTION

In order to protect its assets, the Infrastructure needs to authenticate, identify, and trace *Users* granted access to its *Services*. The authentication and identification must be sufficient to meet the requirements of the Security Policy and any ancillary Specific Policies, bearing in mind the nature of data stored within the Infrastructure and the heterogeneous authentication options.

DEFINITION OF APPROVED AUTHENTICATION ASSURANCE SOURCES

<Enter the details of the Assurance profiles relevant for your infrastructure, as defined in AARC-G021>

OPERATIONAL MATTERS

<Authentication Assurance 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.>

MORE-SPECIFIC POLICIES

For specific cases, a risk evaluation and assessment having been completed, different authentication assurance policies may apply. The Infrastructure shall maintain a registry of such specific policies and their area of applicability.

Acceptable Use Policy Template

- What are your Research Community's aims and purposes?
- Can your infrastructure be used for commercial purposes?
- Do you guarantee any availability of your services to your users?
- Do you need to require citation of the infrastructure in published works?

Taken from https://wiki.geant.org/pages/viewpage.action?pageId=97945151

RESEARCH COMMUNITY AIMS AND PURPOSES

This Research Community is operated for the purpose of <insert a brief description>. Individual services within the Infrastructure may present additional Acceptable Use Policies.

USER DECLARATION

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 resources/services to perform work, or transmit or store data consistent with the stated goals, policies and conditions of use as defined by the body or bodies granting you access.
2. 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.
3. You shall not use the resources/services for any purpose that is unlawful and not (attempt to) breach or circumvent any administrative or security controls.
4. Youshallrespectintellectualpropertyandconfidentialityagreements.

5. You shall protect your access credentials (e.g. private keys or passwords).
6. You shall keep all your registered information correct and up to date.
7. You shall immediately report any known or suspected security breach or misuse of the resources/services or access
8. credentials to the specified incident reporting locations and to the relevant credential issuing authorities.
9. You use the resources/services at your own risk. There is no guarantee that the resources/services will be available
10. at any time or that their integrity or confidentiality will be preserved or that they will suit any purpose.
11. You agree that logged information, including personal data provided by you for registration purposes, may be used
12. for administrative, operational, accounting, monitoring and security purposes. You agree that this logged information may be disclosed to other authorised participants via secured mechanisms, only for the same purposes and only as far as necessary to provide the services.
13. You agree that the body or bodies granting you access and resource/service providers are entitled to regulate, suspend or terminate your access without prior notice and without compensation, within their domain of authority, and you shall immediately comply with their instructions.
14. You are liable for the consequences of your violation of any of these conditions of use, which may include but are not limited to the reporting of your violation to your home institute and, if the activities are thought to be illegal, to appropriate law enforcement agencies.

Privacy Policy Template

- 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?

Name of the Service	SHOULD be the same as mdui:DisplayName

Description of the Service	SHOULD be the same as mdui:Description
Data controller and a contact person	You may wish to include the Data Controller defined for the Infrastructure, rather than per-service
Data controller’s data protection officer (if applicable)	
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..._
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.
Purpose of the	Don’t forget to describe also the purpose of the log files, if they

processing of personal data	contain personal data (they usually do)
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.
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.*
Withdrawal of consent	If personal data is processed on user consent, how can he/she withdraw it?
Data portability	Can the user request his/her data be ported to another Service? How?
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 18 months*
Data Protection Code of Conduct	*Your personal data will be protected according to the Code of Conduct for Service Providers, a common standard for the research and higher education sector to protect your privacy*

Risk Assessment

An actual template for a risk assessment is not provided, since it heavily relies on the type of processing that is taking place. However, the following questions and table can be used as an input into conducting a risk assessment, or even a full DPIA. The table below provides possible risk sources, and how can they be considered and mitigated. More information is provided in WP29 opinions [WP29-WP248rev.01] and AARC guideline [AARC-G042].

- What type of processing involving personal data do you conduct?
- What are the risks associated with these processing activities?
- What are the mitigation procedures? Review of processing activities?
- Is the documentation about all processing activities relevant and up-to-date?

Risks	Impacts on data subjects	Main risk sources	Main threats	Existing or planned measures	Severity	Likelihood
Illegitimate access to personal data						
Unwanted change of data						
Disappearance of data						

Incident Response Procedure

- Where will you store the security contact details of the Infrastructure and its participants?
- Does your Research Community need to set up a secure data store for evidence gathered during Incident Response?
- Can your Research Community establish secure communication between its participants, management and the wider community?
- Will your infrastructure have a dedicated Computer Security Incident Response team?
- Do you have established practices to announce suspension of services?

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 point within one local working day of the initial discovery or notification of the security incident.

3. In collaboration with the Security Incident Response Coordinator (identified by 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.
4. Announce suspension of service (if applicable) in accordance with infrastructure, federation and interfederation 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 labelled 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 interfederation 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 labelled TLP AMBER [3] or higher.
9. Update documentation and procedures as necessary.

Additional Policies of Interest

Your Infrastructure may wish to define additional policies beyond those recommended in this material.

Policy	**Examples**
Service Eligibility	ELIXIR https://docs.google.com/document/d/1cJ3mR8lqfZKRMvSFalSmPbqd1OPU-L6YcUFIRnh1rhQ/edit#heading=h.4gk94slczirb
Traceability & Logging	EGI Security Traceability and Logging Policy (Updated 14 Nov 2016)
Disaster Recovery	CTSC Disaster Recovery Policy Template
Service Operations	EGI Service Operations Security Policy (Updated 1 June 2013)
Asset Management	CTSC Asset Management Policy Template

References

GDPR - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
ICO-PRIV-NOT - https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/
SIRTFI - https://aarc-project.eu/policies/sirtfi/
SNCTFI - https://aarc-project.eu/policies/snctfi/
AARC-G042 - https://aarc-project.eu/guidelines/aarc-g042/
WP29-WP248rev.01 - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236