Science and
Technology
Facilities Council

WISE
COMMUNITY

A Tale of 3 Policies

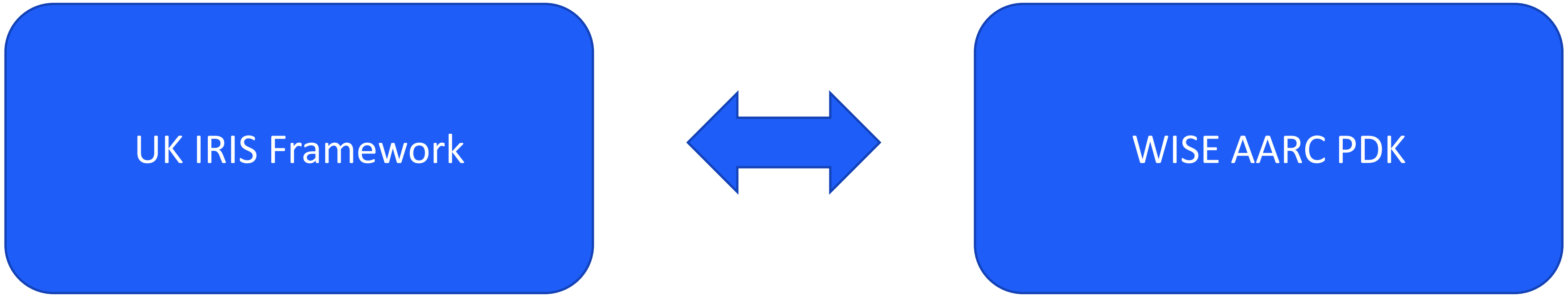
A work in progress

SIG-ISM + WISE virtual workshop, October 2020

Ian Neilson – UKRI-STFC

Objective

- Summarise several strands of policy work



UK IRIS Framework

WISE AARC PDK

- Inform development on both sides

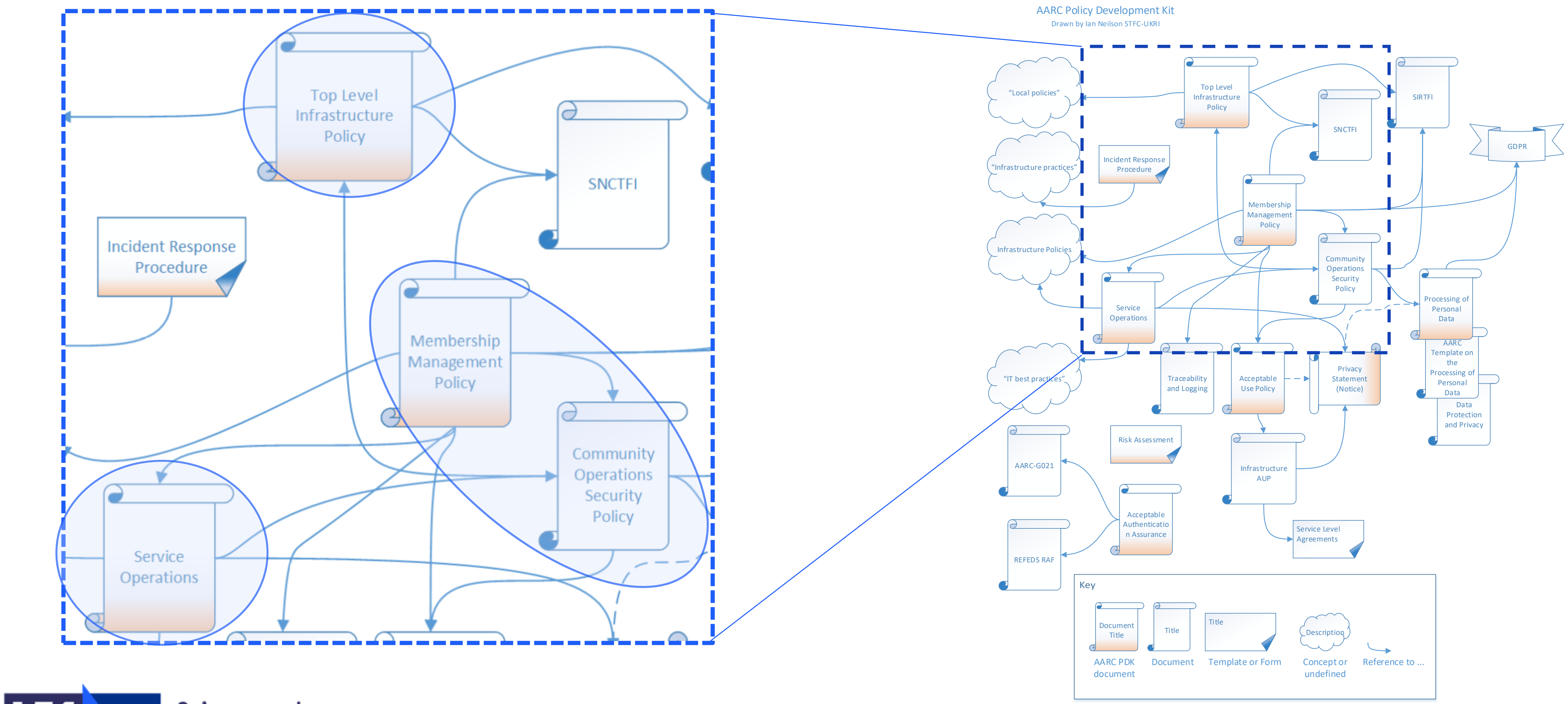
Contents

- Work with 3 AARC PDK policy templates in UK IRIS context

1. Top Level
   - A look at 4 related Top-Level Infrastructure policies:

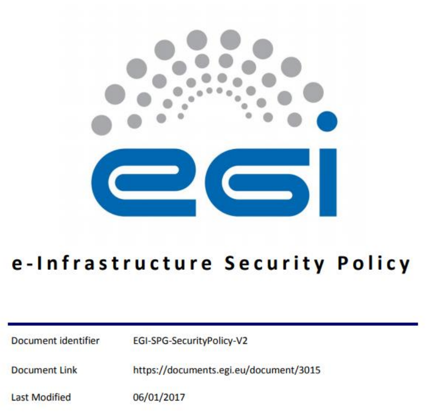
     EGI; EOSC-hub; AARC PDK template; Draft UK IRIS
   - https://docs.google.com/document/d/15-Ef8xUxe7bzOmE9lx1en_-wLsai2_btBFh5S-qSaKI/edit?usp=sharing
2. “Combined” Community
   - Community Operations + Community Membership Management
   - https://docs.google.com/document/d/13x8NtrlY94Afac1MsDcOmaJVuJwA0RsTx4mF9IS9hTw/edit?usp=sharing
3. Service Operations
   - https://docs.google.com/document/d/1nvW6EK9hpSbwv56XFdZTJq7bf5ZZVrKHXuhyFSU8qmI/edit?usp=sharing

AARC PDK context


Top Level Infrastructure Policy
SNCTFI
Incident Response Procedure
Membership Management Policy
Community Operations Security Policy
Service Operations
AARC Policy Development Kit
Drawn by Ian Neilson STFC-UKRI
"Local policies"
"Infrastructure practices"
Infrastructure Policies
"IT best practices"
SIRTFI
GDPR
Processing of Personal Data
AARC Template on the Processing of Personal Data
Data Protection and Privacy
Traceability and Logging
Acceptable Use Policy
Privacy Statement (Notice)
AARC-G021
Risk Assessment
Infrastructure AUP
REFEDS RAF
Acceptable Authenticatio n Assurance
Service Level Agreements
Key
Document Title
AARC PDK document
Title
Document
Title
Template or Form
Description
Concept or undefined
Reference to ...

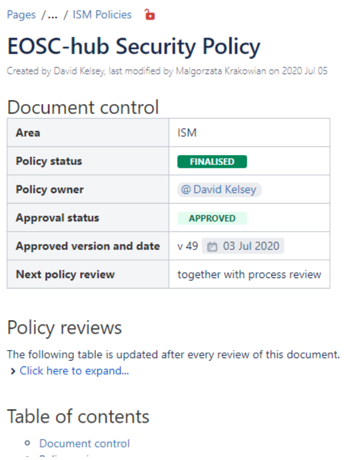
Top Level Policy - 1

- Compare 4 related policies
  - How and why do they differ?
  - How to integrate this back into the AARC PDK?



e-Infrastructure Security Policy

Document identifier	EGI-SPG-SecurityPolicy-V2
Document Link	https://documents.egi.eu/document/3015
Last Modified	06/01/2017



Pages / ... / ISM Policies

EOSC-hub Security Policy

Created by David Kelsey, last modified by Malgorzata Krakowian on 2020 Jul 05

Document control

Area	ISM
Policy status	FINALISED
Policy owner	@ David Kelsey
Approval status	APPROVED
Approved version and date	v 49 03 Jul 2020
Next policy review	together with process review

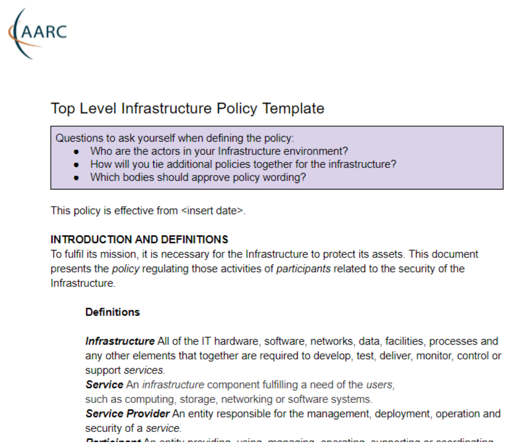
Policy reviews

The following table is updated after every review of this document.

› Click here to expand...

Table of contents

- Document control



AARC

Top Level Infrastructure Policy Template

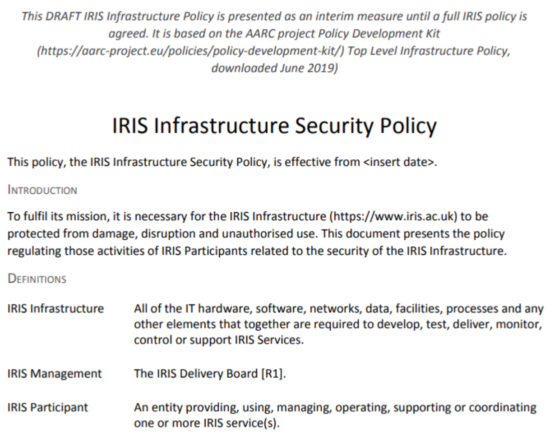
Questions to ask yourself when defining the policy:
- Who are the actors in your Infrastructure environment?
- How will you tie additional policies together for the infrastructure?
- Which bodies should approve policy wording?

This policy is effective from <insert date>.

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

Infrastructure All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support *services*.
Service An *infrastructure* component fulfilling a need of the *users*, such as computing, storage, networking or software systems.
Service Provider An entity responsible for the management, deployment, operation and security of a *service*.
Participant An entity providing, using, managing, operating, supporting or coordinating



This DRAFT IRIS Infrastructure Policy is presented as an interim measure until a full IRIS policy is agreed. It is based on the AARC project Policy Development Kit (https://aarc-project.eu/policies/policy-development-kit/) Top Level Infrastructure Policy, downloaded June 2019)

IRIS Infrastructure Security Policy

This policy, the IRIS Infrastructure Security Policy, is effective from <insert date>.

INTRODUCTION

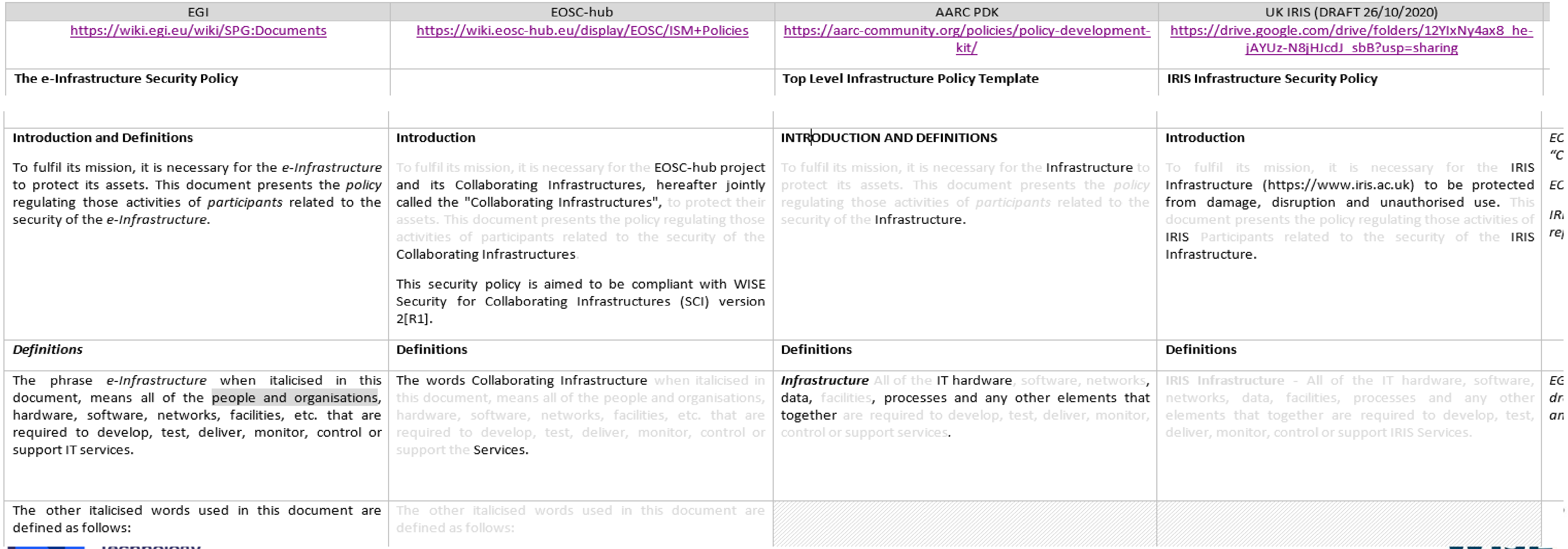
To fulfil its mission, it is necessary for the IRIS Infrastructure (https://www.iris.ac.uk) to be protected from damage, disruption and unauthorised use. This document presents the policy regulating those activities of IRIS Participants related to the security of the IRIS Infrastructure.

DEFINITIONS

IRIS Infrastructure	All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support IRIS Services.
IRIS Management	The IRIS Delivery Board [R1].
IRIS Participant	An entity providing, using, managing, operating, supporting or coordinating one or more IRIS service(s).

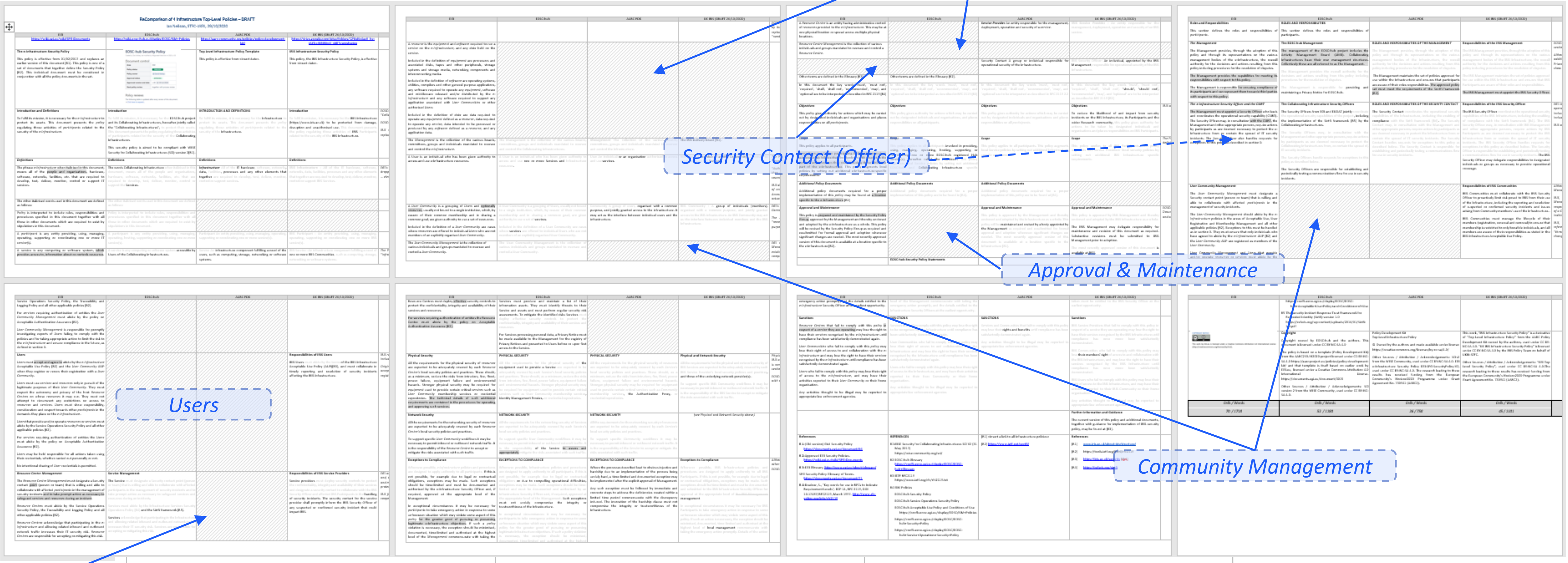
Top Level Policy – 2

- How to compare?
  - Reference against EGI



EGI	EOSC-hub	AARC PDK	UK IRIS (DRAFT 26/10/2020)	
https://wiki.egi.eu/wiki/SPG:Documents	https://wiki.eosc-hub.eu/display/EOSC/ISM+Policies	https://aarc-community.org/policies/policy-development-kit/	https://drive.google.com/drive/folders/12YIxNy4ax8_he-jAYUz-N8jHJcdJ_sbB?usp=sharing	
The e-Infrastructure Security Policy		**Top Level Infrastructure Policy Template**	**IRIS Infrastructure Security Policy**	
Introduction and Definitions To fulfil its mission, it is necessary for the *e-Infrastructure* to protect its assets. This document presents the *policy* regulating those activities of *participants* related to the security of the *e-Infrastructure*.	**Introduction** To fulfil its mission, it is necessary for the EOSC-hub project and its Collaborating Infrastructures, hereafter jointly called the "Collaborating Infrastructures", to protect their assets. This document presents the policy regulating those activities of participants related to the security of the Collaborating Infrastructures. This security policy is aimed to be compliant with WISE Security for Collaborating Infrastructures (SCI) version 2[R1].	**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.	**Introduction** To fulfil its mission, it is necessary for the IRIS Infrastructure (https://www.iris.ac.uk) to be protected from damage, disruption and unauthorised use. This document presents the policy regulating those activities of IRIS Participants related to the security of the IRIS Infrastructure.	*EC* *“C* *EC* *IR* *re*
Definitions	**Definitions**	**Definitions**	**Definitions**	
The phrase *e-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 words Collaborating 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 the Services.	***Infrastructure*** All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support services.	**IRIS Infrastructure** - All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support IRIS Services.	*EG* *dr* *an*
The other italicised words used in this document are defined as follows:	The other italicised words used in this document are defined as follows:	▨	▨	

Top Level Policy – 3



ReComparison of 4 Infrastructure Top-Level Policies – DRAFT

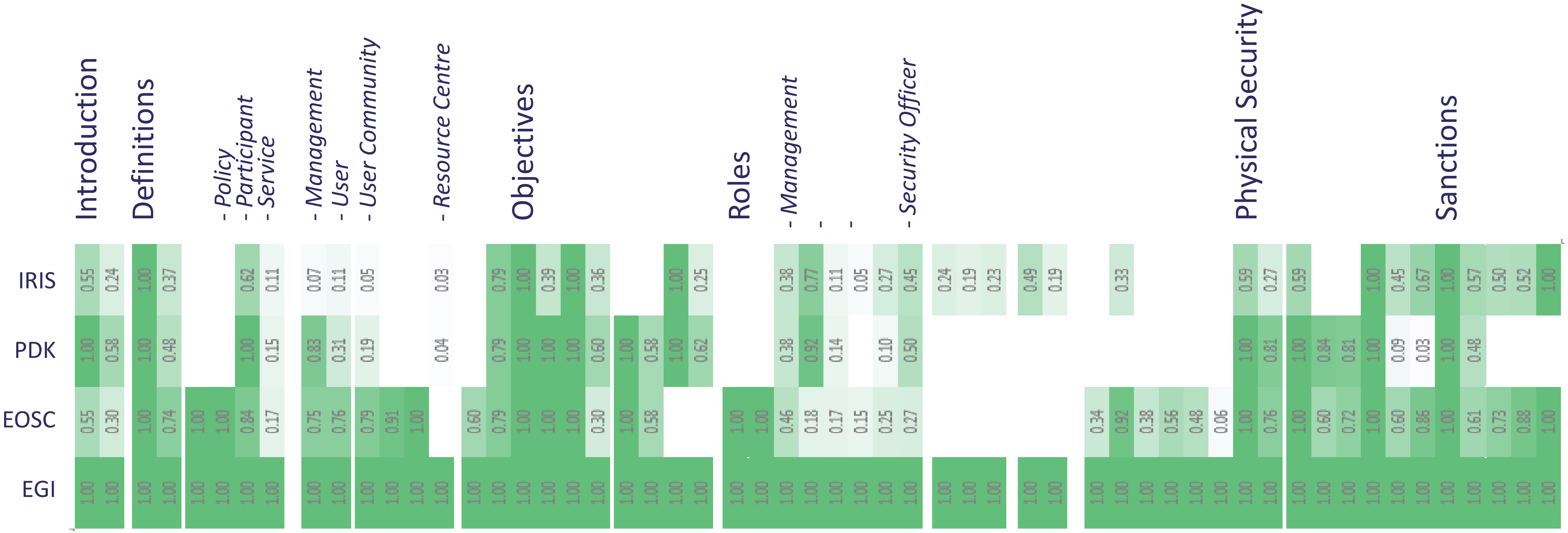
Resource (Service)

Cells / Words	Cells / Words	Cells / Words	Cells / Words
EGI 70 / 1718	EOSC 53 / 1180	PDK 36 / 758	IRIS 45 / 1101

Science and Technology Facilities Council

WISE COMMUNITY

Top Level Policy – 4



	Introduction		Definitions			- Policy	- Participant	- Service	- Management	- User	- User Community			- Resource Centre
IRIS	0.55	0.24	1.00	0.37			0.62	0.11	0.07	0.11	0.05			0.03
PDK	1.00	0.58	1.00	0.48			1.00	0.15	0.83	0.31	0.19			0.04
EOSC	0.55	0.30	1.00	0.74	1.00	1.00	0.84	0.17	0.75	0.76	0.79	0.91	1.00	
EGI	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

			Objectives								Roles		- Management	-
IRIS		0.79	1.00	0.39	1.00	0.36			1.00	0.25			0.38	0.77
PDK		0.79	1.00	1.00	1.00	0.60	1.00	0.58	1.00	0.62			0.38	0.92
EOSC	0.60	0.79	1.00	1.00	1.00	0.30	1.00	0.58			1.00	1.00	0.46	0.18
EGI	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

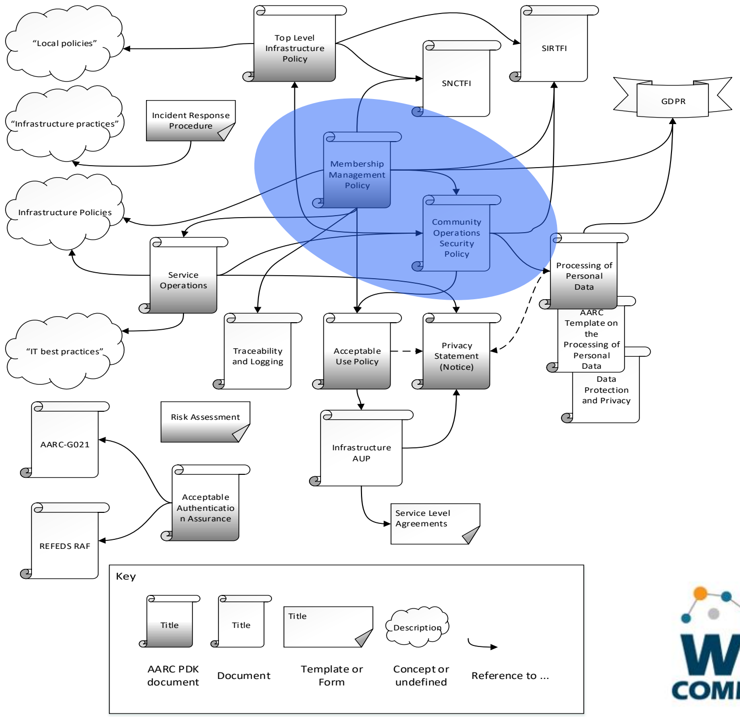
		-		- Security Officer										
IRIS	0.11	0.05	0.27	0.45	0.24	0.19	0.23	0.49	0.19		0.33			
PDK	0.14		0.10	0.50										
EOSC	0.17	0.15	0.25	0.27						0.34	0.92	0.38	0.56	0.48
EGI	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

		Physical Security								Sanctions				
IRIS		0.59	0.27	0.59			1.00	0.45	0.67	1.00	0.57	0.50	0.52	1.00
PDK		1.00	0.81	1.00	0.84	0.81	1.00	0.09	0.03	1.00	0.48			
EOSC	0.06	1.00	0.76	1.00	0.60	0.72	1.00	0.60	0.86	1.00	0.61	0.73	0.88	1.00
EGI	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Cosine similarity measure

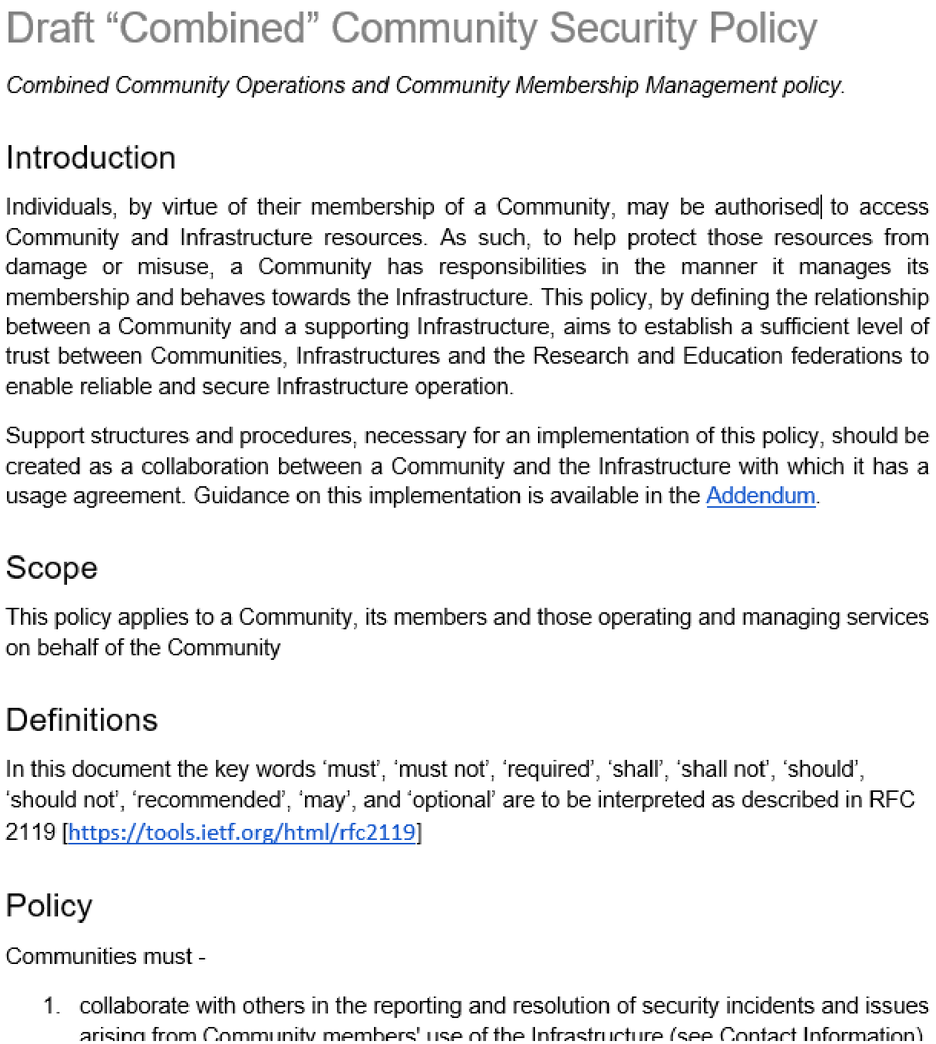
“Combined” Community Policy - 1

- Presentation at virtual WISE meeting, April 2020
  - *https://wiki.geant.org/display/WISE/Virtual+WISE+meeting+21+April+2020*
- Summary
  - Community policy in AARC PDK is incomplete
    - Membership Management ✓ Community Operations ✗
  - Highly interlinked with other policies
  - Internally a complex set of many requirements (~93)
    - Community Managers, Infrastructure Operators …
  - Hard to understand and difficult to implement



“Combined” Community Policy - 2

- IRIS draft
  - input from GEANT GN4-3 Enco
- Community Operations + Membership Management
- Strip out many details
  - But don’t lose them!
- Restructure ongoing
  - Separate into Policy + Guidance Addendum



Draft “Combined” Community Security Policy

Combined Community Operations and Community Membership Management policy.

Introduction

Individuals, by virtue of their membership of a Community, may be authorised to access Community and Infrastructure resources. As such, to help protect those resources from damage or misuse, a Community has responsibilities in the manner it manages its membership and behaves towards the Infrastructure. This policy, by defining the relationship between a Community and a supporting Infrastructure, aims to establish a sufficient level of trust between Communities, Infrastructures and the Research and Education federations to enable reliable and secure Infrastructure operation.

Support structures and procedures, necessary for an implementation of this policy, should be created as a collaboration between a Community and the Infrastructure with which it has a usage agreement. Guidance on this implementation is available in the Addendum.

Scope

This policy applies to a Community, its members and those operating and managing services on behalf of the Community

Definitions

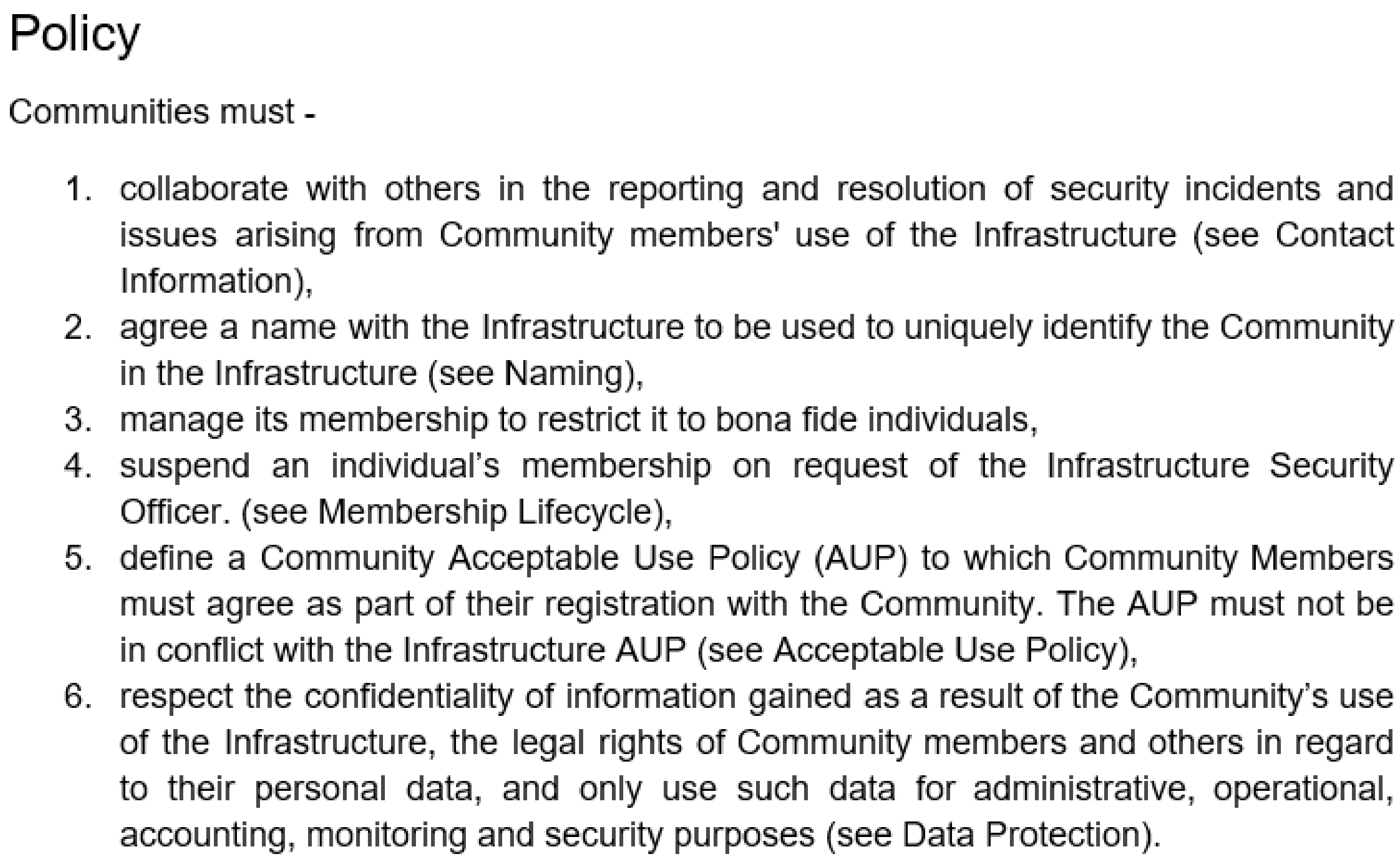
In this document the key words ‘must’, ‘must not’, ‘required’, ‘shall’, ‘shall not’, ‘should’, ‘should not’, ‘recommended’, ‘may’, and ‘optional’ are to be interpreted as described in RFC 2119 [https://tools.ietf.org/html/rfc2119]

Policy

Communities must -

1. collaborate with others in the reporting and resolution of security incidents and issues arising from Community members' use of the Infrastructure (see Contact Information)

“Combined” Community Policy – 3

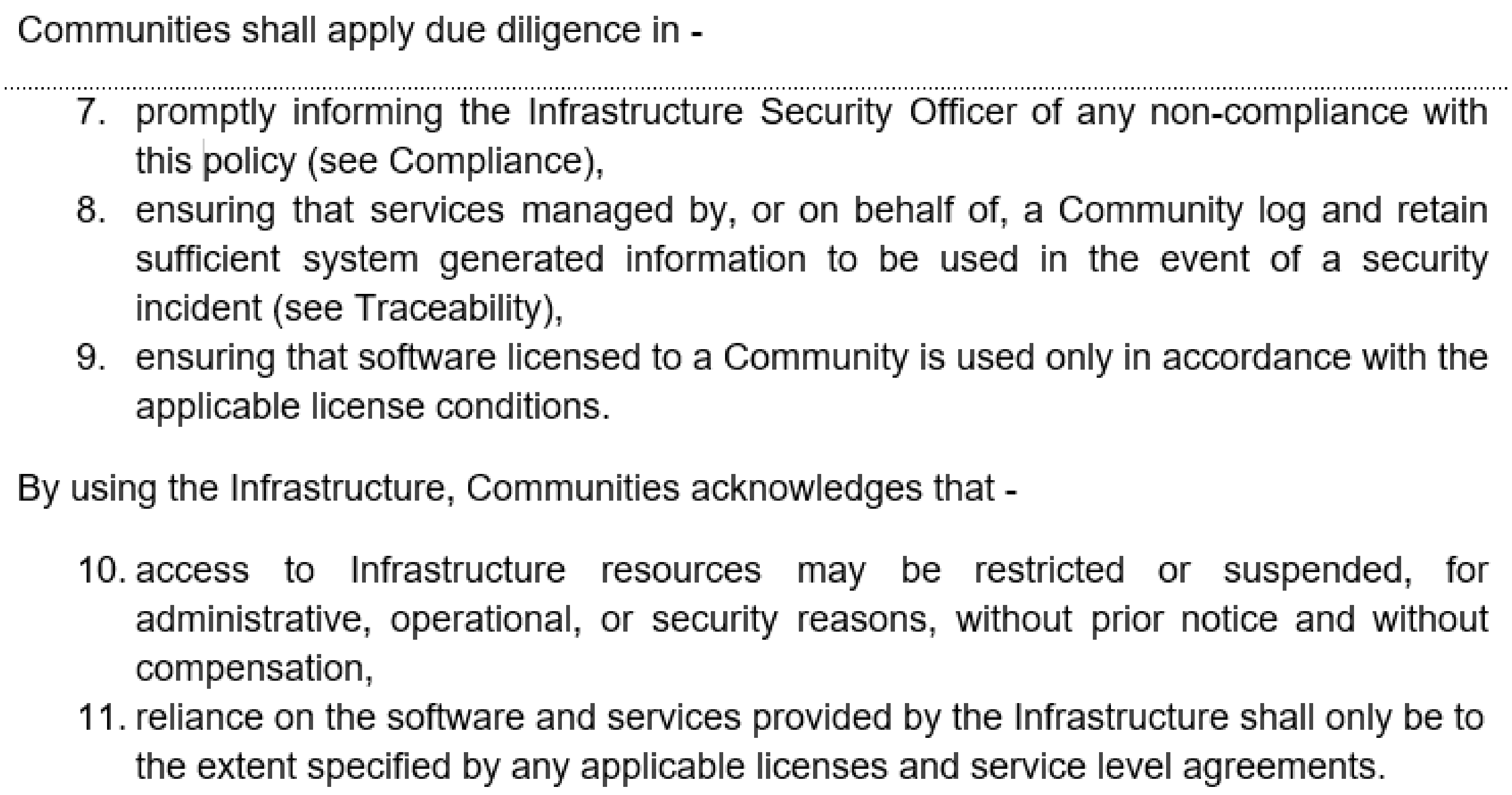


Policy

Communities must -

1. collaborate with others in the reporting and resolution of security incidents and issues arising from Community members' use of the Infrastructure (see Contact Information),
2. agree a name with the Infrastructure to be used to uniquely identify the Community in the Infrastructure (see Naming),
3. manage its membership to restrict it to bona fide individuals,
4. suspend an individual’s membership on request of the Infrastructure Security Officer. (see Membership Lifecycle),
5. define a Community Acceptable Use Policy (AUP) to which Community Members must agree as part of their registration with the Community. The AUP must not be in conflict with the Infrastructure AUP (see Acceptable Use Policy),
6. respect the confidentiality of information gained as a result of the Community’s use of the Infrastructure, the legal rights of Community members and others in regard to their personal data, and only use such data for administrative, operational, accounting, monitoring and security purposes (see Data Protection).

“Combined” Community Policy – 4



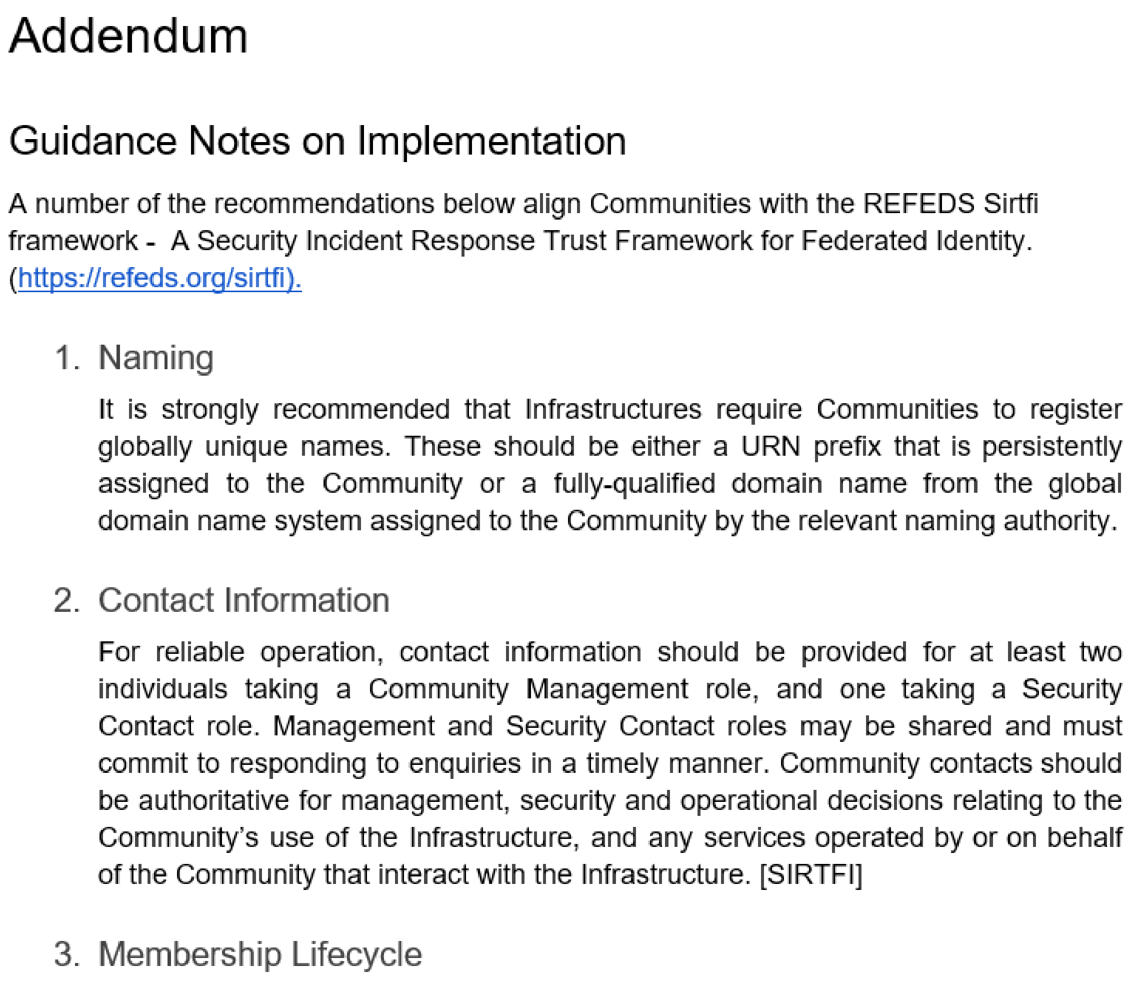
Communities shall apply due diligence in -

7. promptly informing the Infrastructure Security Officer of any non-compliance with this policy (see Compliance),
8. ensuring that services managed by, or on behalf of, a Community log and retain sufficient system generated information to be used in the event of a security incident (see Traceability),
9. ensuring that software licensed to a Community is used only in accordance with the applicable license conditions.

By using the Infrastructure, Communities acknowledges that -

10. access to Infrastructure resources may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation,
11. reliance on the software and services provided by the Infrastructure shall only be to the extent specified by any applicable licenses and service level agreements.

“Combined” Community Policy – 5



Addendum

Guidance Notes on Implementation

A number of the recommendations below align Communities with the REFEDS Sirtfi framework - A Security Incident Response Trust Framework for Federated Identity. (https://refeds.org/sirtfi).

1. Naming

   It is strongly recommended that Infrastructures require Communities to register globally unique names. These should be either a URN prefix that is persistently assigned to the Community or a fully-qualified domain name from the global domain name system assigned to the Community by the relevant naming authority.

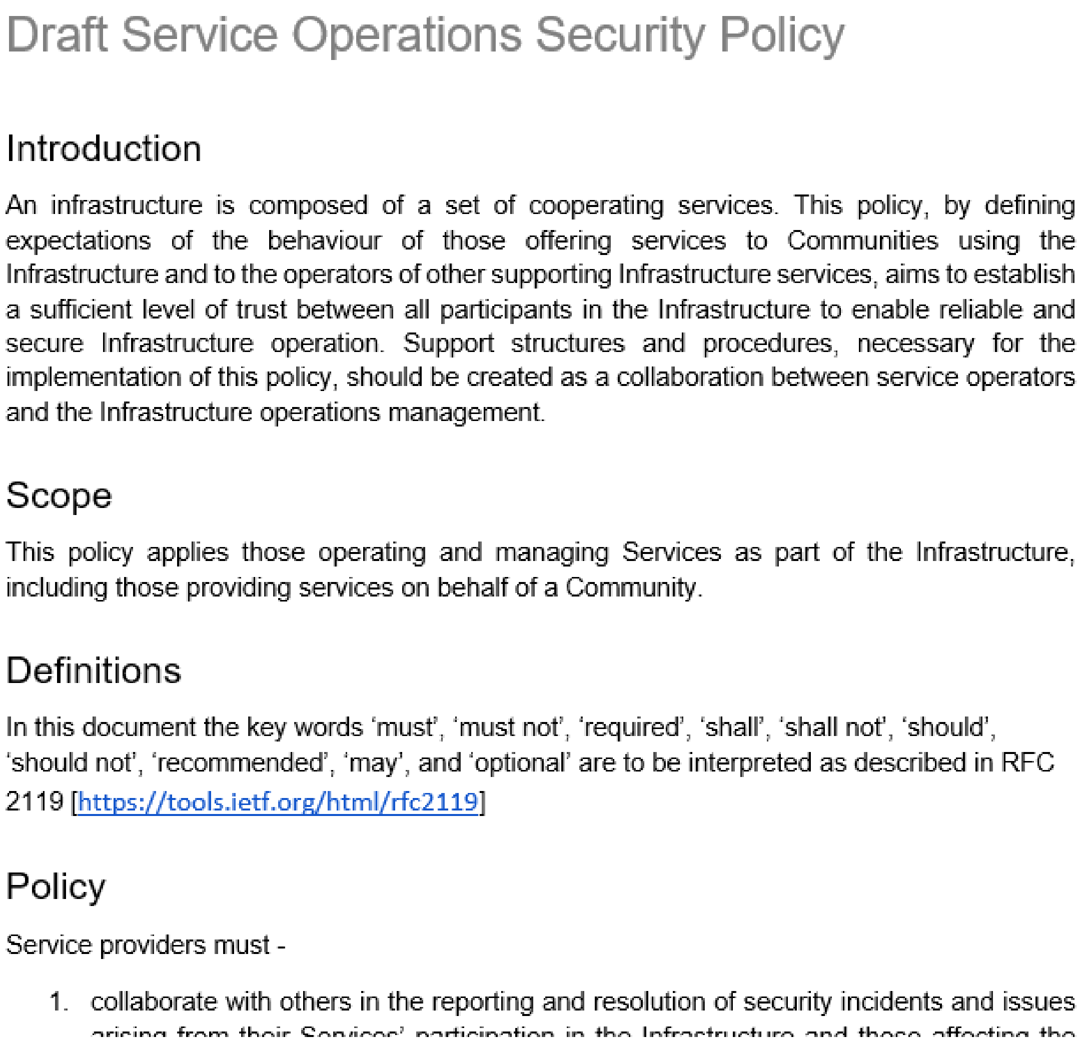
2. Contact Information

   For reliable operation, contact information should be provided for at least two individuals taking a Community Management role, and one taking a Security Contact role. Management and Security Contact roles may be shared and must commit to responding to enquiries in a timely manner. Community contacts should be authoritative for management, security and operational decisions relating to the Community’s use of the Infrastructure, and any services operated by or on behalf of the Community that interact with the Infrastructure. [SIRTFI]

3. Membership Lifecycle

Service Operations Policy - 1

- IRIS draft
  - Based on AARC PDK
  - Reduce policy linkage
- Strip out some details
  - But don’t lose them!
  - Separate into Policy + Guidance Addendum
- Restructure ongoing



Draft Service Operations Security Policy

Introduction

An infrastructure is composed of a set of cooperating services. This policy, by defining expectations of the behaviour of those offering services to Communities using the Infrastructure and to the operators of other supporting Infrastructure services, aims to establish a sufficient level of trust between all participants in the Infrastructure to enable reliable and secure Infrastructure operation. Support structures and procedures, necessary for the implementation of this policy, should be created as a collaboration between service operators and the Infrastructure operations management.

Scope

This policy applies those operating and managing Services as part of the Infrastructure, including those providing services on behalf of a Community.

Definitions

In this document the key words ‘must’, ‘must not’, ‘required’, ‘shall’, ‘shall not’, ‘should’, ‘should not’, ‘recommended’, ‘may’, and ‘optional’ are to be interpreted as described in RFC 2119 [https://tools.ietf.org/html/rfc2119]

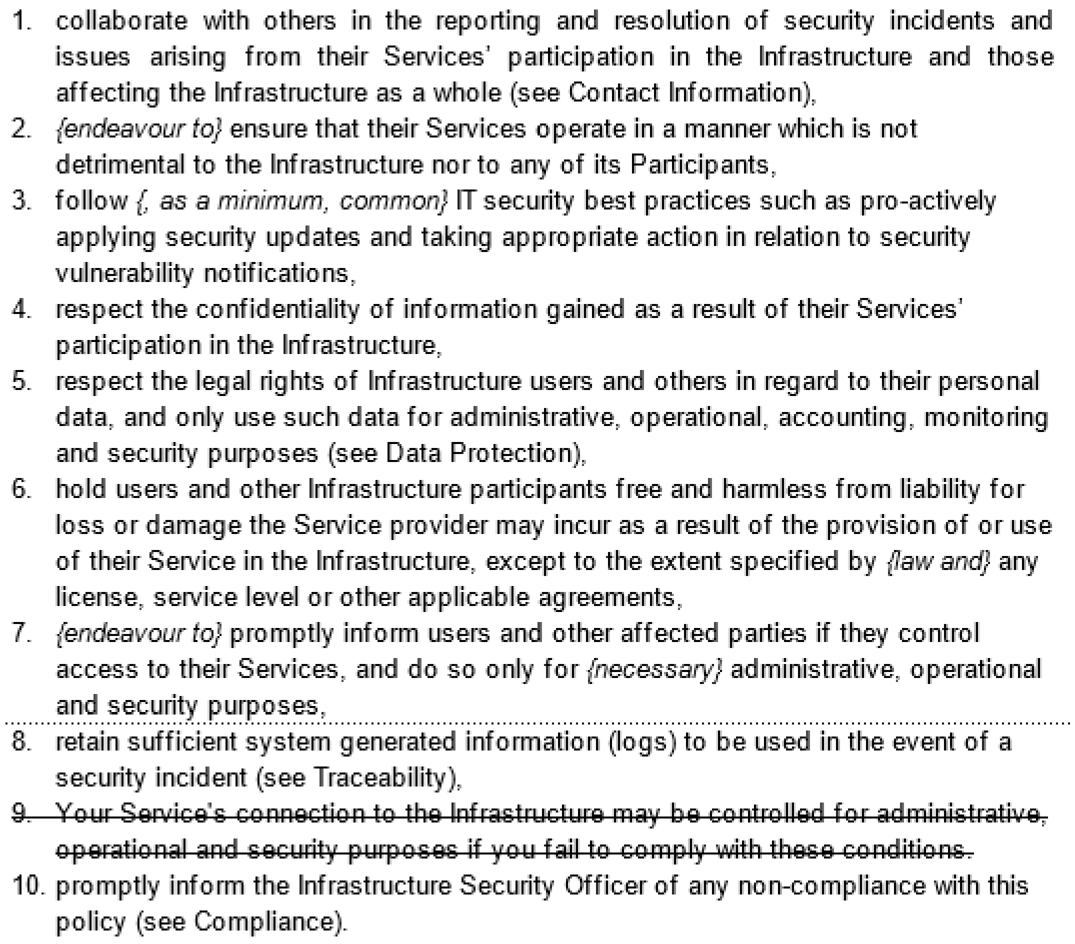
Policy

Service providers must -

1. collaborate with others in the reporting and resolution of security incidents and issues arising from their Services’ participation in the Infrastructure and those affecting the

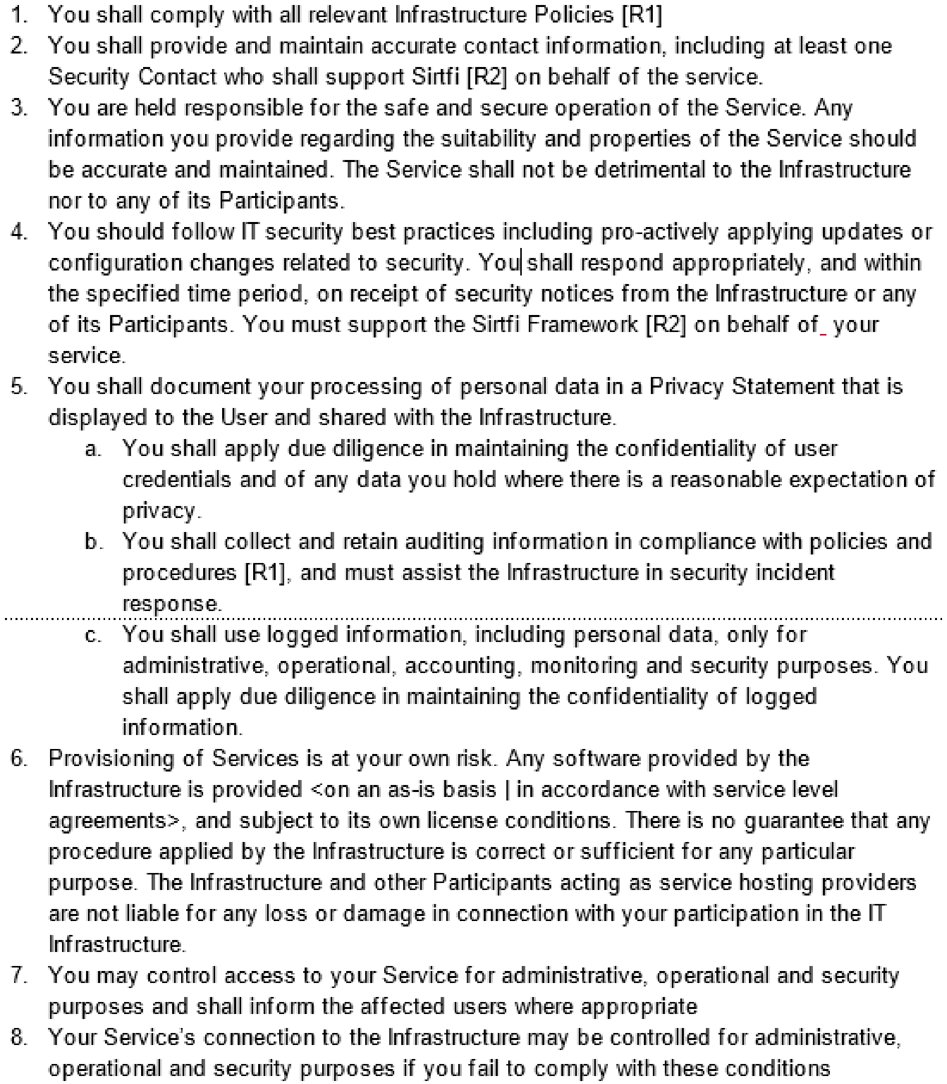
Service Operations Policy - 2

(Very) Draft UK IRIS



1. collaborate with others in the reporting and resolution of security incidents and issues arising from their Services' participation in the Infrastructure and those affecting the Infrastructure as a whole (see Contact Information),
2. *{endeavour to}* ensure that their Services operate in a manner which is not detrimental to the Infrastructure nor to any of its Participants,
3. follow *{, as a minimum, common}* IT security best practices such as pro-actively applying security updates and taking appropriate action in relation to security vulnerability notifications,
4. respect the confidentiality of information gained as a result of their Services' participation in the Infrastructure,
5. respect the legal rights of Infrastructure users and others in regard to their personal data, and only use such data for administrative, operational, accounting, monitoring and security purposes (see Data Protection),
6. hold users and other Infrastructure participants free and harmless from liability for loss or damage the Service provider may incur as a result of the provision of or use of their Service in the Infrastructure, except to the extent specified by *{law and}* any license, service level or other applicable agreements,
7. *{endeavour to}* promptly inform users and other affected parties if they control access to their Services, and do so only for *{necessary}* administrative, operational and security purposes,
8. retain sufficient system generated information (logs) to be used in the event of a security incident (see Traceability),
9. ~~Your Service's connection to the Infrastructure may be controlled for administrative, operational and security purposes if you fail to comply with these conditions.~~
10. promptly inform the Infrastructure Security Officer of any non-compliance with this policy (see Compliance).

PDK



1. You shall comply with all relevant Infrastructure Policies [R1]
2. You shall provide and maintain accurate contact information, including at least one Security Contact who shall support Sirtfi [R2] on behalf of the service.
3. You are held responsible for the safe and secure operation of the Service. Any information you provide regarding the suitability and properties of the Service should be accurate and maintained. The Service shall not be detrimental to the Infrastructure nor to any of its Participants.
4. You should follow IT security best practices including pro-actively applying updates or configuration changes related to security. You shall respond appropriately, and within the specified time period, on receipt of security notices from the Infrastructure or any of its Participants. You must support the Sirtfi Framework [R2] on behalf of your service.
5. You shall document your processing of personal data in a Privacy Statement that is displayed to the User and shared with the Infrastructure.
   a. You shall apply due diligence in maintaining the confidentiality of user credentials and of any data you hold where there is a reasonable expectation of privacy.
   b. You shall collect and retain auditing information in compliance with policies and procedures [R1], and must assist the Infrastructure in security incident response.
   c. You shall use logged information, including personal data, only for administrative, operational, accounting, monitoring and security purposes. You shall apply due diligence in maintaining the confidentiality of logged information.
6. Provisioning of Services is at your own risk. Any software provided by the Infrastructure is provided <on an as-is basis | in accordance with service level agreements>, and subject to its own license conditions. There is no guarantee that any procedure applied by the Infrastructure is correct or sufficient for any particular purpose. The Infrastructure and other Participants acting as service hosting providers are not liable for any loss or damage in connection with your participation in the IT Infrastructure.
7. You may control access to your Service for administrative, operational and security purposes and shall inform the affected users where appropriate
8. Your Service's connection to the Infrastructure may be controlled for administrative, operational and security purposes if you fail to comply with these conditions

So?

- *Top-Level*
  - *EGI is an infrastructure, EOSC-hub is a “federation”, IRIS is an evolving partnership*
  - *One size does not fit all*
- *Community*
  - *“Community”, “Collections”, “Users” and “Members”, “lifecycle” …..*
  - *People arrive with their own context and expectations*
- *Service Operations*
  - *Services exist and then attach to an infrastructure*
  - *Local policies must be respected*
- *And … we haven’t mentioned AUPs or Privacy Notices!*

Comments and input very welcome
Links to googledocs here

UKRI Science and Technology Facilities Council

WISE COMMUNITY

Science and
Technology
Facilities Council

Thank you

ian.neilson@stfc.ac.uk

Facebook: Science and Technology Facilities Council

Twitter:@STFC_matters

YouTube: Science and Technology Facilities Council