Wise Information Security for collaborating e-Infrastructures

The WISE Community and updating baseline policies for collaborating research infrastructures

David Kelsey (STFC-RAL, UK Research and Innovation)

ISGC2021, Virtual Conference, 24 March 2021

In collaboration with and co-supported by EU H2020 EOSC-HUB & GN4-3

https://wise-community.org

Thank you to my WISE collaborators in 2020

My sincere thanks are due to the following for their collaboration:

- Ana Afonso, Tom Barton, Vincent Brillault, Ian Collier, Linda Cornwall, Bob Cowles, David Crooks, Barbara Krašovec, Sven Gabriel, Baptiste Grenier, David Groep, Nicole Harris, Jens Jensen, Urpo Kaila, Daniel Kouril, Maarten Kremers, Mikael Linden, Alf Moens, Ian Neilson, Ralph Niederberger, Mischa Salle, Hannah Short, Uros Stevanovic, Romain Wartel, Chris Weaver, Jule Ziegler
- Colleagues in GridPP, EGI, WLCG, IRIS, GN4-3, EOSC, IGTF, REFEDs, FIM4R, SIG-ISM, Trusted CI
  - And many others in the past
- These individuals have done the work!
  - *And many apologies for any I have missed*

Contents

- The WISE Community
- Current WISE working groups
- Security for Collaborating Infrastructures Working Group (SCI-WG)
  - SCI Version 2 – HowTo & maturity assessment
  - WISE Baseline AUP (reminder)
  - Developing the AARC Policy Development Kit (updating baseline templates)
- WISE & SCI in 2021

- See “WISE” talk at ISGC2019 for more details about AARC PDK and AUP *https://indico4.twgrid.org/indico/event/8/session/10/contribution/37*

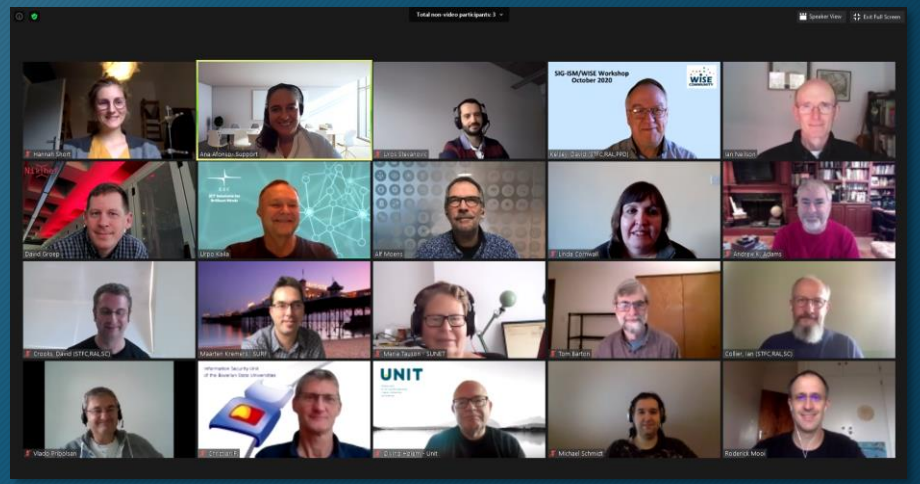
The WISE Community

- Started in October 2015 – Joint - GEANT SIG-ISM & IGTF SCI
- Community members come from e-Infrastructures across the world
- WISE meetings 2019-20
  - LITNET – Kaunas, Lithuania – April 2019 (joint with SIG-ISM)
  - NSF Cybersecurity Summit, San Diego, USA – Oct 2019
  - Two virtual meetings during COVID-19 pandemic
    - April 2020 and Oct 2020
    - Both joint with GEANT SIG-ISM

Some WISE meetings (2018 to 2020)

Abingdon, UK
Feb 2018

Alexandria, VA, USA
Aug 2018



Virtual – Oct 2020
Joint with SIG-ISM

San Diego, CA, USA – Oct 2019
All attendees at NSF Cybersecurity Summit

WISE Mission

- *The WISE Community enhances best practice in information security for IT infrastructures for research.*
- *How? Through membership of working groups and attendance at workshops the members participate in the joint development of policy frameworks, guidelines, and templates.*

WISE Working Groups

Current Working Groups

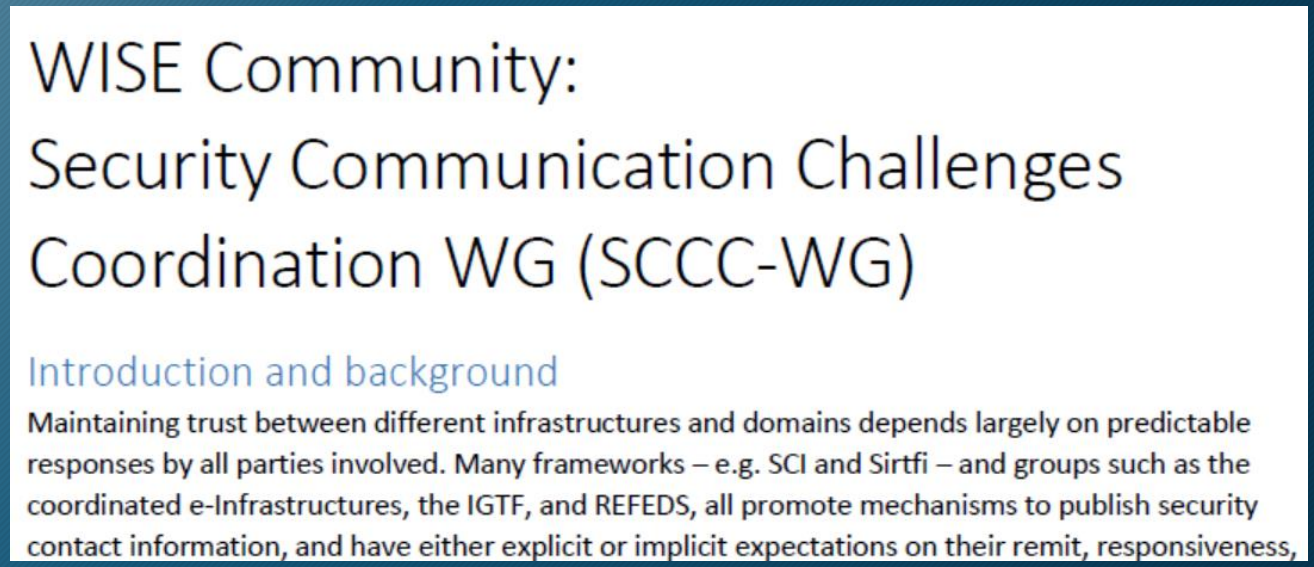
- Trust and policy issues related to the Security for Collaborating Infrastructures trust framework (SCI-WG)
- Security Communications Challenge Coordination Working Group (SCCC-JWG) – joint with SIG-ISM
- Incident Response & Threat Intelligence Working Group (IRTI-WG)
- Risk Assessment WISE (RAW-WG) – joint with SIG-ISM

Still being considered (was proposed at last WISE meeting)

- Best Practices for handling Software Vulnerabilities

Security Communications Challenge Coordination Working Group (SCCC-JWG)

- Many Infrastructures perform regular communication challenges
  - & more sophisticated security challenges
- To build confidence and trust
- Can these be scheduled and coordinated?
- Strengthen Incident Response in eduGAIN
  - eduGAIN security team and Sirtfi-WG
- Promote sharing of CC results



WISE Community:
Security Communication Challenges Coordination WG (SCCC-WG)

Introduction and background

Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have either explicit or implicit expectations on their remit, responsiveness,

https://wiki.geant.org/display/WISE/Communications+Challenge+planning

Other WISE Working Groups

- Risk Assessment Working Group (RAW-WG)
  - Share experiences on risk identification, analysis and evaluation
  - effective security controls
  - Produced a WISE risk assessment template and associated guidelines
- Incident Response & Threat Intelligence Working Group (IRTI-WG)
  - To better handle security incidents - protect services/data & prevent re-occurrence
  - Sharing threat intelligence is growing in importance
  - Security Operations Centres (see talks on SOCs at ISGC2021)

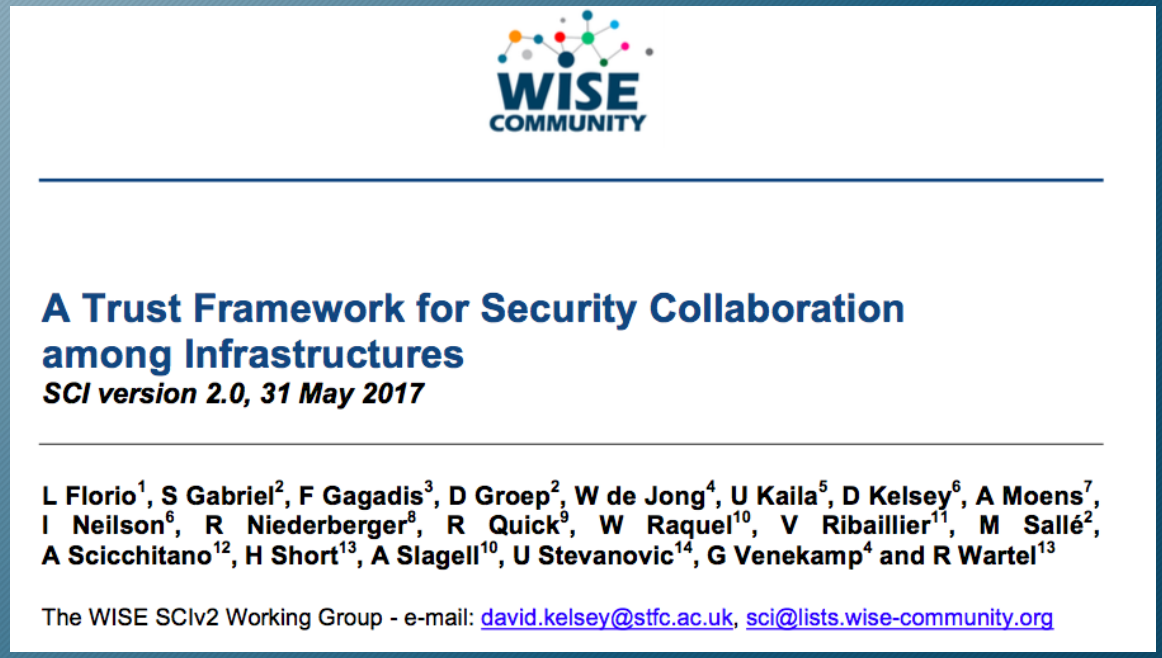
Security for Collaborating Infrastructures …

- SCI Version 2, HowTo and maturity assessment
- WISE Baseline AUP (reminder)
- Developing the AARC Policy Development Kit (updating baseline templates)

SCI-WG - Shared threats & shared users

- Infrastructures are subject to many of the same threats
  - Shared technology, middleware, applications and users
- User communities use multiple e-Infrastructures
  - Often using same federated identity credentials
- Security incidents often spread by following the user
  - E.g. compromised credentials
- e-Infrastructure security teams need to collaborate

SCI Version 2 – published 31 May 2017



WISE COMMUNITY

A Trust Framework for Security Collaboration among Infrastructures

SCI version 2.0, 31 May 2017

L Florio[1], S Gabriel[2], F Gagadis[3], D Groep[2], W de Jong[4], U Kaila[5], D Kelsey[6], A Moens[7], I Neilson[6], R Niederberger[8], R Quick[9], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[10], U Stevanovic[14], G Venekamp[4] and R Wartel[13]

The WISE SCIv2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

Endorsement of SCI Version 2 at TNC17 (Linz)

- 1st June 2017
- *Infrastructures endorse the governing principles and approach of SCI, as produced by WISE, as a medium of building trust between infrastructures, to facilitate the exchange of security information in the event of a cross-infrastructure incident, and the collaboration of e-Infrastructures to support the process. These Infrastructures welcome the development of an information security community for the Infrastructures, and underline that the present activities by the research and e-Infrastructures should be continued and reinforced*
- Endorsements have been received from the following infrastructures; EGI, EUDAT, GEANT, GridPP, MYREN, PRACE, SURF, WLCG, XSEDE, HBP
- https://www.geant.org/News_and_Events/Pages/supporting-security-for-collaborating-infrastructures.aspx

Security for Collaboration among Infrastructures (SCI)

EUGRIDPMA- 2021-02-08

Ian Neilson (STFC-RAL, UK Research and Innovation)

Uros Stevanovic (Karlsruhe Institute of Technology)

https://wise-community.org

In collaboration with and co-supported by EnCo (GN4-3)

SCI requirements

- The document defined a series of numbered requirements in 5 areas
  - Operational Security
  - Incident Response
  - Traceability
  - Participant Responsibilities
  - Data protection

SCI Assessment of maturity

- To evaluate extent to which requirements are met, we recommend Infrastructures to assess the maturity of their implementations
- According to following levels:
  - Level 0: Function/feature not implemented
  - Level 1: Function/feature exists, is operationally implemented but not documented
  - Level 2: … and comprehensively documented
  - Level 3: … and reviewed by independent external body

Assessment spreadsheet

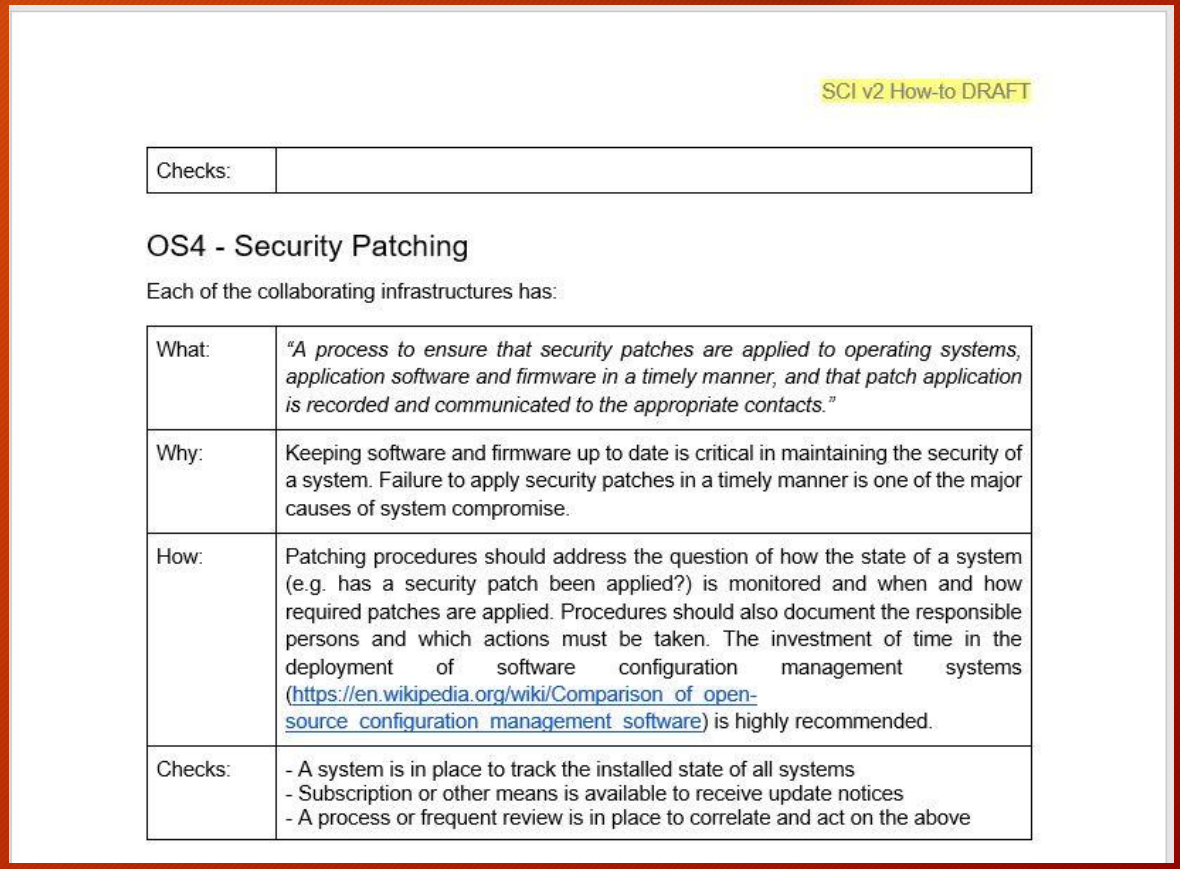
	A	B	C	D	E	F	G	H	I	
1	**Infrastructure Name:**		<insert name>							
2	**Prepared By:**		<insert name>						**On Date:**	<insert date>
3	**Reviewed By:**		<insert name>						**On Date:**	<insert date>
4										
5	**Operational Security [OS]**		**Maturity**				**Evidence**	**Version Number**	**Document Date**	**Document Page**
6			**Value**	**Σ**			**(Document Name and/or URL)**			
7										
8	**OS1 - Security Person/Team**									
9	**OS2 - Risk Management Process**									
10	**OS3 - Security Plan (architecture, policies, controls)**			2.0						
11	OS3.1 - Authentication		3							
12	OS3.2 - Dynamic Response		1							
13	OS3.3 - Access Control									
14	OS3.4 - Physical and Network Security									
15	OS3.5 - Risk Mitigation									
16	OS3.6 - Confidentiality									
17	OS3.7 - Integrity and Availability	Q	1	1.0						
18	OS3.8 - Disaster Recovery									
19	OS3.9 - Compliance Mechanisms									
20	**OS4 - Security Patching**		1	1.0						
21	OS4.1 - Patching Process									
22	OS4.2 - Patching Records and Communication									
23	**OS5 - Vulnerability Mgmt**		1	0.7						
24	OS5.1 - Vulnerability Process									

- https://wiki.geant.org/download/attachments/58131190/SCIv2-Assessment-Chart_V2-US.xlsx?version=1&modificationDate=1554550759208&api=v2

SCI How-to?

- SCI is a framework
  - Sometimes not detailed or prescriptive enough
  - Different understanding of requirements
  - Requirements may vary greatly in scope and complexity

The guidance is intended to assist those implementing SCI and, as such, is not, primarily scoped to 'end users' - members of collections of users. Infrastructure managers, service operators, security officers, the responsibles of collections of users, and others invested in the security of an infrastructure and its services, are the intended audience.



SCI v2 How-to DRAFT

Checks:	

OS4 - Security Patching

Each of the collaborating infrastructures has:

What:	*"A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts."*
Why:	Keeping software and firmware up to date is critical in maintaining the security of a system. Failure to apply security patches in a timely manner is one of the major causes of system compromise.
How:	Patching procedures should address the question of how the state of a system (e.g. has a security patch been applied?) is monitored and when and how required patches are applied. Procedures should also document the responsible persons and which actions must be taken. The investment of time in the deployment of software configuration management systems (https://en.wikipedia.org/wiki/Comparison_of_open-source_configuration_management_software) is highly recommended.
Checks:	- A system is in place to track the installed state of all systems - Subscription or other means is available to receive update notices - A process or frequent review is in place to correlate and act on the above

Security for Collaborating Infrastructures …

SCI Version 2, HowTo and maturity assessment

WISE Baseline AUP (reminder)

Developing the AARC Policy Development Kit (updating baseline templates)

Kelsey/WISE Community

24 March 2021

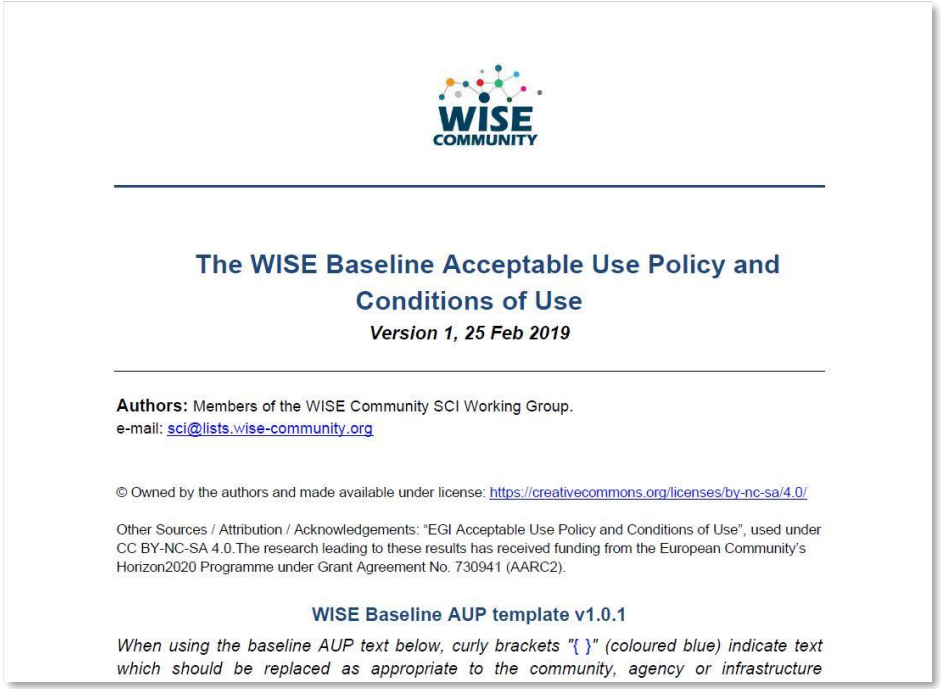
AARC Policy Development Kit
Acceptable Use Policy - *A reminder*

See “WISE” talk at ISGC2019 for more details about AARC PDK and AUP
https://indico4.twgrid.org/indico/event/8/session/10/contribution/37

A common baseline AUP

An agreed Acceptable Use Policy (AUP) to act as a baseline policy (or template) for adoption by research communities

- To facilitate -
  a) a more rapid community infrastructure ‘bootstrap’
  b) ease the trust of users across infrastructures
  c) provide a consistent and more understandable enrolment for users.
- Adoption of a single policy preferred to modifying a template



WISE COMMUNITY

The WISE Baseline Acceptable Use Policy and Conditions of Use

Version 1, 25 Feb 2019

Authors: Members of the WISE Community SCI Working Group.
e-mail: sci@lists.wise-community.org

Other Sources / Attribution / Acknowledgements: “EGI Acceptable Use Policy and Conditions of Use”, used under CC BY-NC-SA 4.0.The research leading to these results has received funding from the European Community’s Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

WISE Baseline AUP template v1.0.1

When using the baseline AUP text below, curly brackets "{ }" (coloured blue) indicate text which should be replaced as appropriate to the community, agency or infrastructure

WISE Baseline AUP v1

https://wise-community.org/wise-baseline-aup/

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 to 10 below, whose wording and numbering must not be changed.>

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.>

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>

AARC Guideline I044 on use of baseline AUP

https://aarc-project.eu/guidelines/#policy

Security for Collaborating Infrastructures …

- SCI Version 2, HowTo and maturity assessment
- WISE Baseline AUP (reminder)
- Developing the AARC Policy Development Kit (updating baseline templates)

Development of AARC PDK by WISE SCI-WG

- Involve the widest experience from many Infrastructures and policy groups (including AEGIS)
  - https://aarc-project.eu/about/aegis/
- Infrastructures using/considering the AARC PDK include
  - EOSC-hub, IRIS(UK), EGI, WLCG, SLATE(USA)
- Policy templates are useful to new Infrastructures and help build trust and interoperability (compliant with SCI Trust Framework)
- WISE SCI will collect feedback from Infrastructures
  - And use this if/when a new version of a template is required
- Unlike AUP, new templates may contain optional components
  - Infrastructures just use the components that work for them

Building on AARC PDK in WISE SCI-WG

https://aarc-project.eu/policies/policy-development-kit/

		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	
Data Protection	Privacy Statement	Defines			Defines	Views
	Policy on the Processing of Personal Data	Defines	Abides by	Abides by	Abides by	
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	

Policy Area	New Template	Lead Participants
Top Level	Infrastructure Policy	IRIS (UK), EOSC-hub
Data Protection	Privacy Statement	WLCG, IRIS
Data Protection	Policy on the Processing of Personal Data	EGI, WLCG
Membership	Community Policy	IRIS, EOSC, GN4-3, IGTF
Membership	Acceptable Authentication Assurance	GN4-3, IGTF
Operational Security	Incident Response	eduGAIN, Sirtfi, GN4-3, EOSC & many opsec groups
Operational Security	Service Operations	EOSC-hub, IRIS

Science and Technology Facilities Council

IRIS Security

Trust Framework and Operational Security

David Crooks
david.crooks@stfc.ac.uk

IAM Users Workshop
January 2021

Science and Technology Facilities Council

iris

IRIS Background

Science Activities

- ALMA
- ATLAS
- CCFE
- CLF
- CMS
- CTA
- DLS
- DUNE
- eMERLIN
- EUCLID
- GAIA
- ISIS
- LHCb
- LIGO
- LSST
- Lux-Zeplin
- SKA

Provider Entities

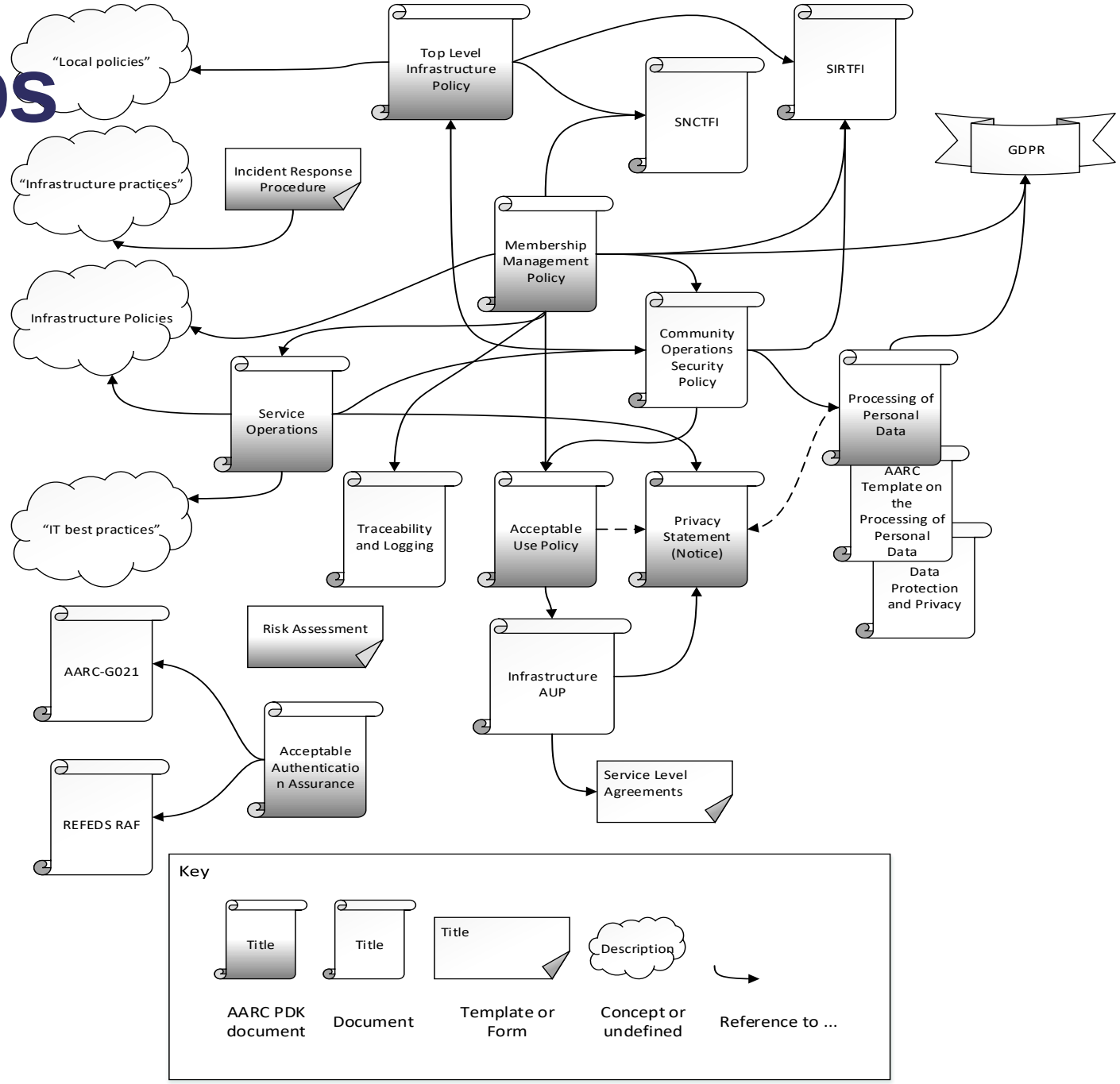
- The Ada Lovelace Centre (ALC)
- DiRAC [HPC]
- GridPP [HTC]
- The Hartree Centre
- STFC Scientific Computing Department
- The DLS Computing Department
- CCFE computing

UKRI Science and Technology Facilities Council

WISE COMMUNITY

Policy Relationships

- Policy map derived from AARC PDK and others in first year of IRIS Trust Framework
- Shows there are many policies, groups, procedures, ‘standards’, notices, agreements, regulations and fuzzy objects in this space.
- Shows relationships between different policy items
- Can be used to inform most useful next steps



IRIS Trust Framework status

- Update on status of policy drafting and approval
- Approved by DB:
  - Infrastructure Security Policy
  - IRIS AUP
  - IRIS IAM Privacy Notice
- In draft:
  - Service Operations Security Policy
  - *Community Policy (following risk assessment currently underway)*

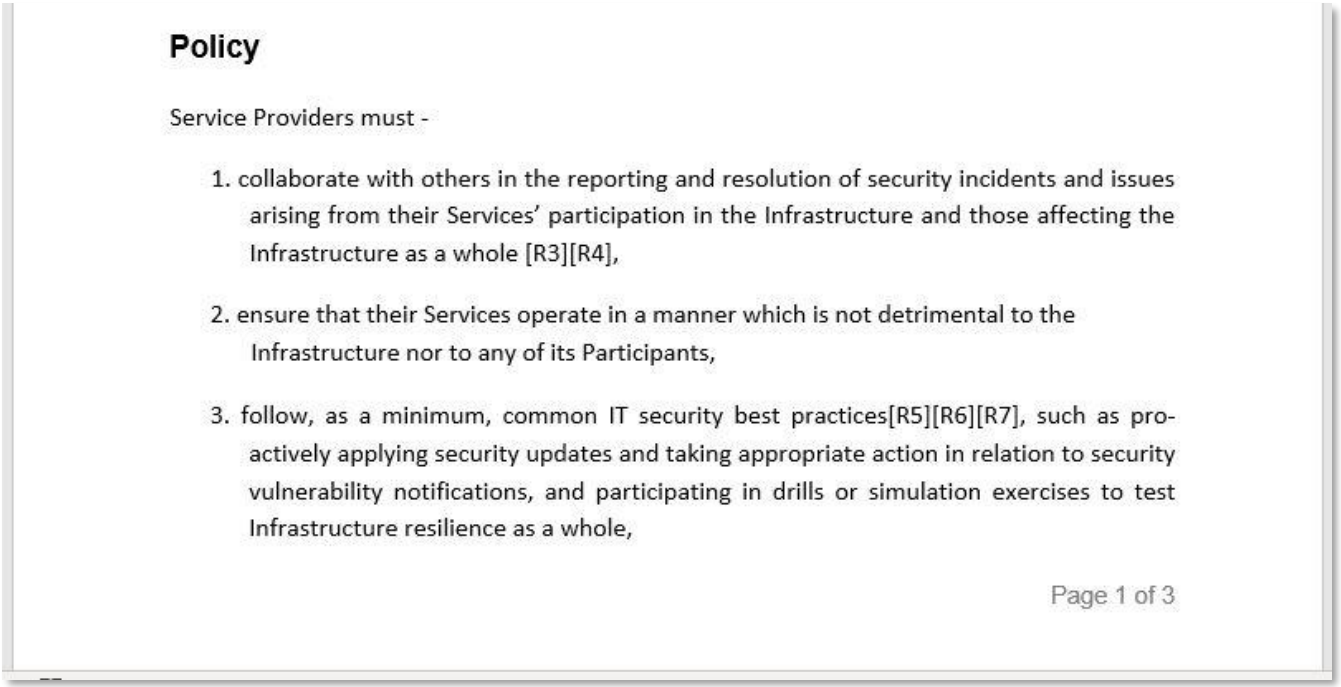
IRIS Service Operations Security Policy (draft)

This DRAFT IRIS Service Operations Security Policy is based on the AARC Policy Development Kit "Service Operations Security Policy".

DRAFT IRIS Service Operations Security Policy

Introduction

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.



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 Infrastructure as a whole [R3][R4],

2. 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[R5][R6][R7], such as pro-actively applying security updates and taking appropriate action in relation to security vulnerability notifications, and participating in drills or simulation exercises to test Infrastructure resilience as a whole,

Page 1 of 3

UKRI Science and Technology Facilities Council

iris

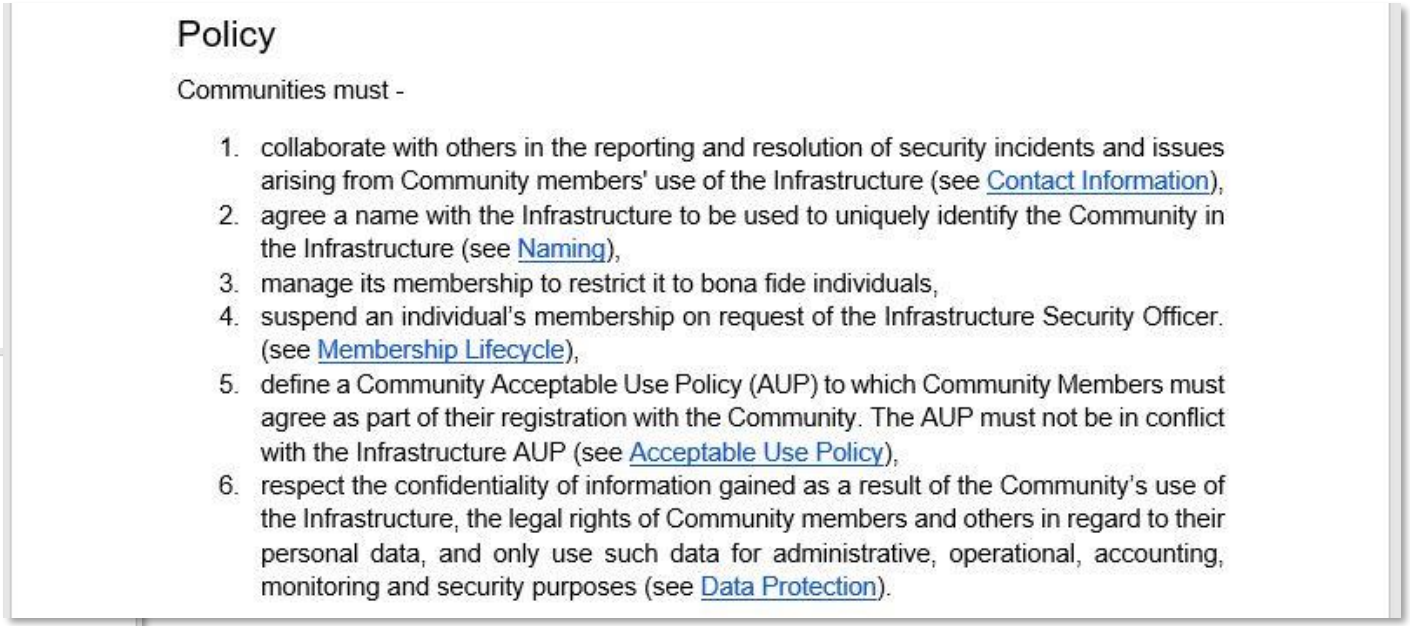
IRIS Community Security Policy (draft)

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.



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).

UKRI Science and Technology Facilities Council

iris

The future: WISE & SCI in 2021

- WISE work continues within the working groups
- SCI-WG
  - Complete the HowTo Guidance on maturity assessment
    - Encourage Infrastructures to perform self-assessment
  - Produce some updated policy templates from AARC PDK
- Full WISE meetings (twice) still to be defined for 2021

- Please join the WISE mail list and the WG lists too (all welcome)
  - *https://lists.wise-community.org/sympa/info/wise*

Questions?

- And discussion ….

Backup slides

WISE and Trusted CI have agreed a joint statement of collaboration

"Trusted CI and WISE share a common goal to support the research mission through the development of appropriate cybersecurity practices. Through close collaboration, the groups will ensure that cybersecurity frameworks, templates, and policies for our international infrastructures for research will grow increasingly aligned and interoperable."

IRIS Trust Framework

- The IRIS Trust Framework is intended to build the security policy required by IRIS
  - Start with foundational and user-facing policies
- Address Incident Response for IRIS
- Parallel to development of Identity and Access Management for IRIS through IRIS-IAM
  - Deployment of INDIGO IAM Identity Proxy
  - In operation, part of UK AMF
  - Follows AARC Blueprint Architecture

UKRI Science and Technology Facilities Council

WISE COMMUNITY