Authentication and Authorisation for Research and Collaboration

The WISE Baseline AUP

From the Taipei Accord to a augmentable common AUP

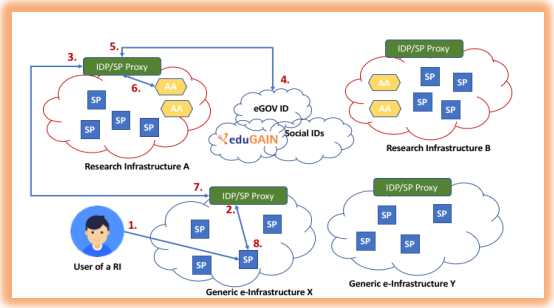
David Groep
Policy and Best Practice coordination lead
based on a lot of work by Ian Neilson, RAL-STFC (UKRI)

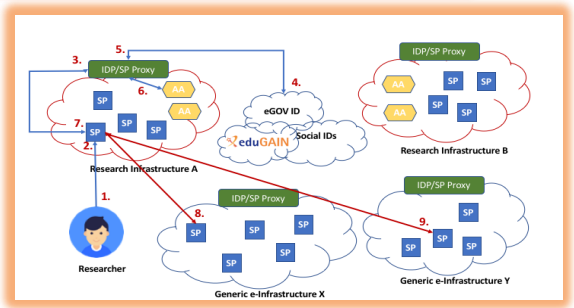
Nikhef

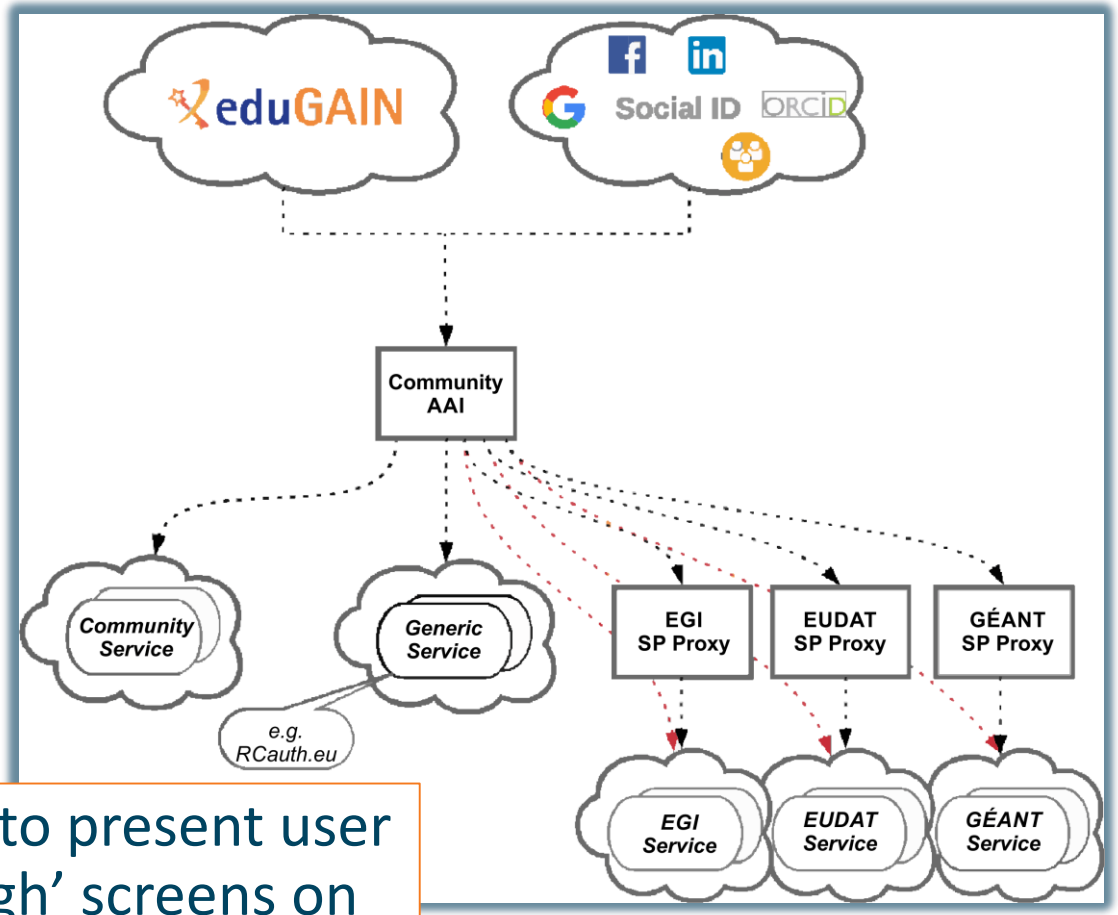
WISE/SIG-ISM Workshop Kaunas
April 2019

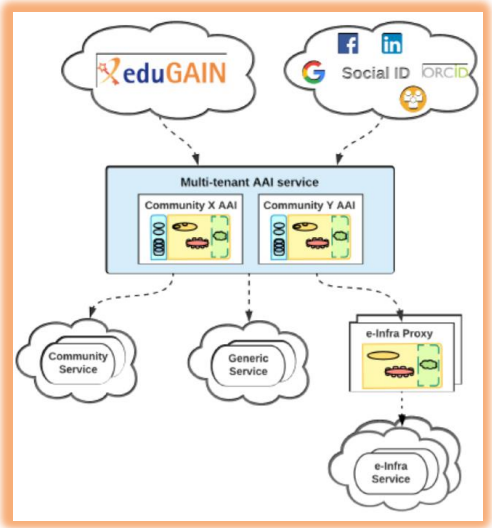
Why a common baseline AUP?

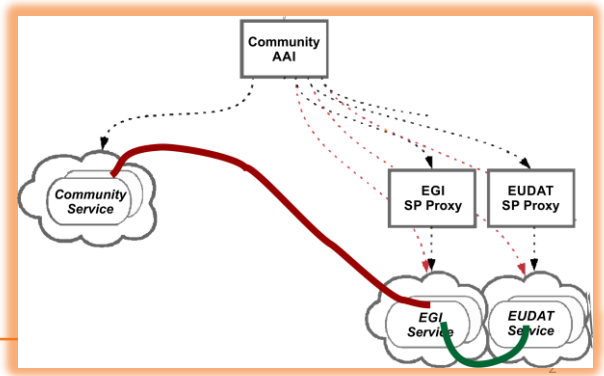
Users move across services – and making them read any AUP is already a hard proposition







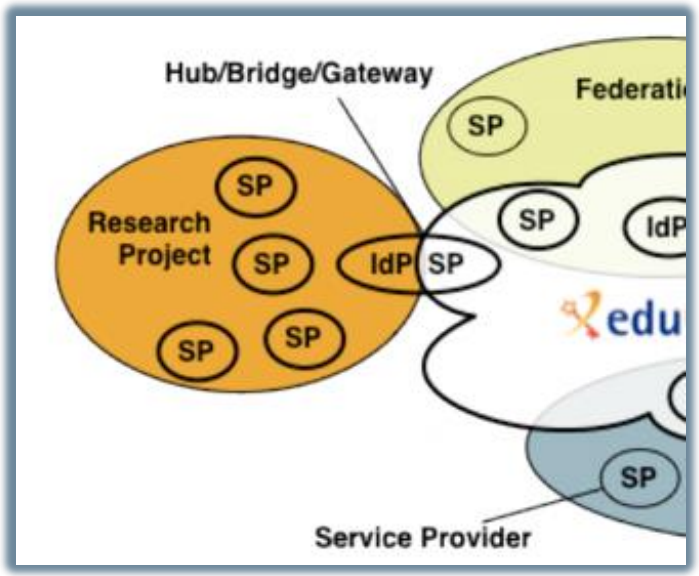




impractical to present user 'click-through' screens on each individual service

A policy framework for service providers groups and proxies

Snctfi - *Scalable Negotiator for a Community Trust Framework in Federated Infrastructures*
Sirtfi - *Security Incident Response Trust Framework for Federated Infrastructures*



graphic IdP-SP bridge: Lukas Hammerle and Ann Harding, SWITCH

igtf.net/snctfi
refeds.org/sirtfi


Snctfi v1.0 AARC

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)

Licia Florio (GÉANT), David Groep (Nikhef), Christos Kanellopoulos (GÉANT), David Kelsey (STFC), Mikael Linden (CSC), Ian Neilson (STFC), Stefan Paetow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (IDRIS-CNR (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and G (SURFsara)

AARC - Version 1.0 - 26 Apr 2017

e-mail: david.kelsey@stfc.ac.uk

Abstract: This paper identifies operational and policy requirem trust between an Infrastructure and identity providers either in an I another Infrastructure, in each case joined via a Service Provider proxy.

Audience: This document is intended for use by the personnel management, operation and security of an Infrastructure and those trustworthiness.

REFEDS

Doc version: 1.0
Date 14.12.2015
Page 1/5

TITLE / REFERENCE: SIRTFI

A Security Incident Response Trust Framework for Federated Identity (Sirtfi)

Authors: T. Barton, J. Basney, D. Groep, N. Harris, L. Johansson, D. Kelsey, S. Koranda, R. Wartel, A. West
Editor: H. Short

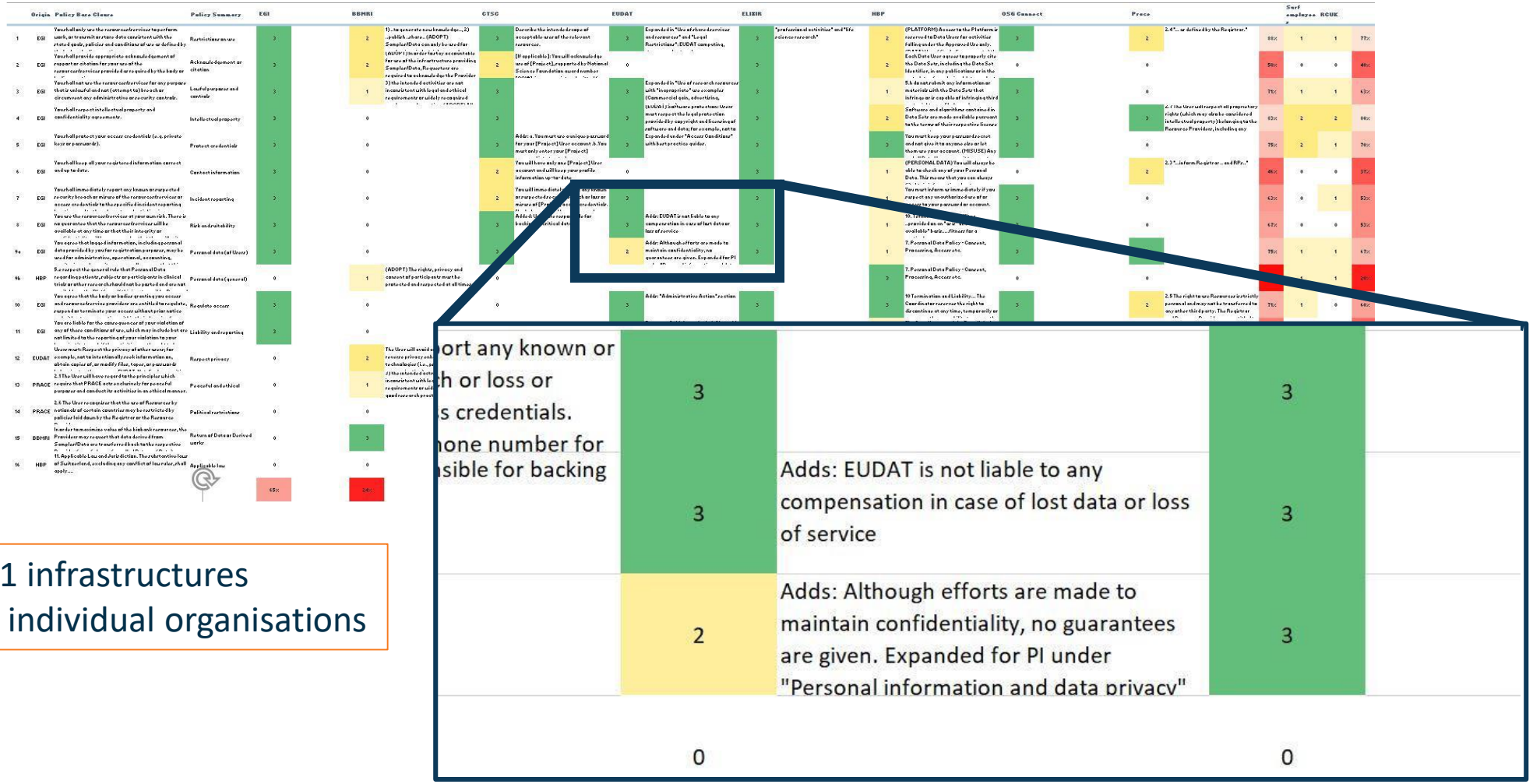
Abstract:
This document identifies practices and attributes of organizations that may facilitate their participation in a trust framework called Sirtfi purposed to enable coordination of security incident response across federated organizations.

Audience:
This document is intended for use by the personnel responsible for operational security of entities that operate within federations, for example Identity Providers, Service Providers and

Derived from **SCI**, the framework on *Security for Collaboration in Infrastructures*
both need the user to adhere to acceptable use policies

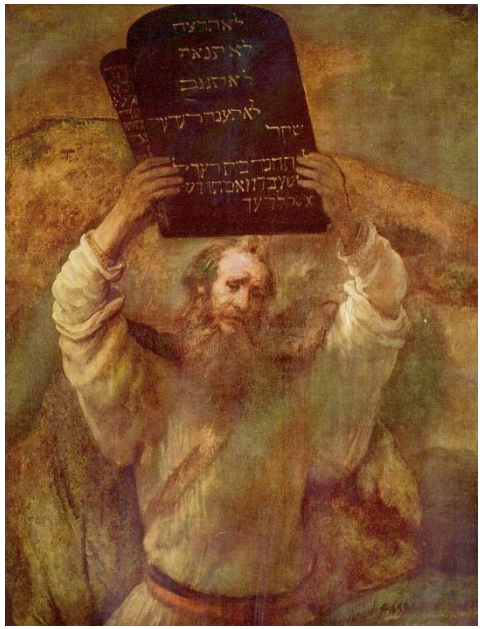
Snctfi is managed for the community by the Interoperable Global Trust Federation IGTF
Sirtfi is managed for the community by the Research and Education Federations group REFEDS

Divergence and convergence – the AUP Alignment Study



ort any known or h or loss or s credentials. hone number for sible for backing	3	3
	3	Adds: EUDAT is not liable to any compensation in case of lost data or loss of service	3
	2	Adds: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI under "Personal information and data privacy"	3
	0		0

11 infrastructures
4 individual organisations



https://docs.google.com/spreadsheets/d/1bg5I9n_DM7QcXdnja_7r0OEpTfjrb72ftq7-xHQxfxM/edit#gid=822235717

Image: Mozes en de tafelen der Wet, Rembrandt van Rijn, 1659

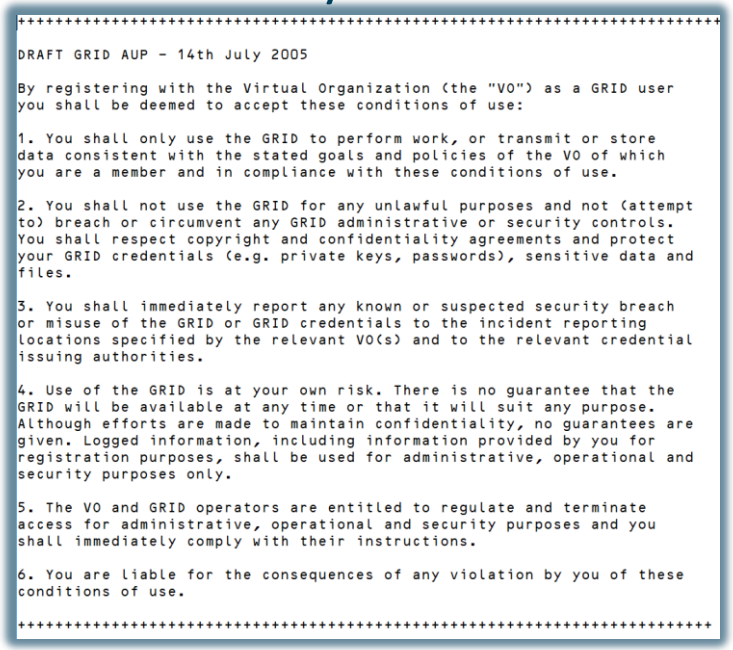
Features of the AUP clusters

Difference between ‘infrastructure’ and ‘organizational’ AUPs is clear

- service provider AUPs in the Infrastructures can limit scope to professional use
- many organization AUPs need ‘non-permissible’ use to govern private use & personal data
- Infrastructure AUPs usually limit liability and place responsibilities on community and user

Yet there is interesting commonality

- many of the Infrastructure AUPs share a common history in the 2005 ‘Taipei Accord’
- focus on permissible use and purpose-binding
- short representation to encourage readability



```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

DRAFT GRID AUP - 14th July 2005

By registering with the Virtual Organization (the "VO") as a GRID user
you shall be deemed to accept these conditions of use:

1. You shall only use the GRID to perform work, or transmit or store
data consistent with the stated goals and policies of the VO of which
you are a member and in compliance with these conditions of use.

2. You shall not use the GRID for any unlawful purposes and not (attempt
to) breach or circumvent any GRID administrative or security controls.
You shall respect copyright and confidentiality agreements and protect
your GRID credentials (e.g. private keys, passwords), sensitive data and
files.

3. You shall immediately report any known or suspected security breach
or misuse of the GRID or GRID credentials to the incident reporting
locations specified by the relevant VO(s) and to the relevant credential
issuing authorities.

4. Use of the GRID is at your own risk. There is no guarantee that the
GRID will be available at any time or that it will suit any purpose.
Although efforts are made to maintain confidentiality, no guarantees are
given. Logged information, including information provided by you for
registration purposes, shall be used for administrative, operational and
security purposes only.

5. The VO and GRID operators are entitled to regulate and terminate
access for administrative, operational and security purposes and you
shall immediately comply with their instructions.

6. You are liable for the consequences of any violation by you of these
conditions of use.

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

But the challenge remains: how to prevent a bazillion AUP clicks?

A new common baseline AUP

*Recommendation for the **content** of an Acceptable Use Policy (AUP)*
to act as a baseline policy (or template) for adoption by research communities
and to enable access to the e-Infrastructure services

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 – enables infrastructure services to have implicit trust coming from the community membership management

WISE Baseline AUP v1 – to be published by WISE/SCI very soon

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 on use of baseline AUP:

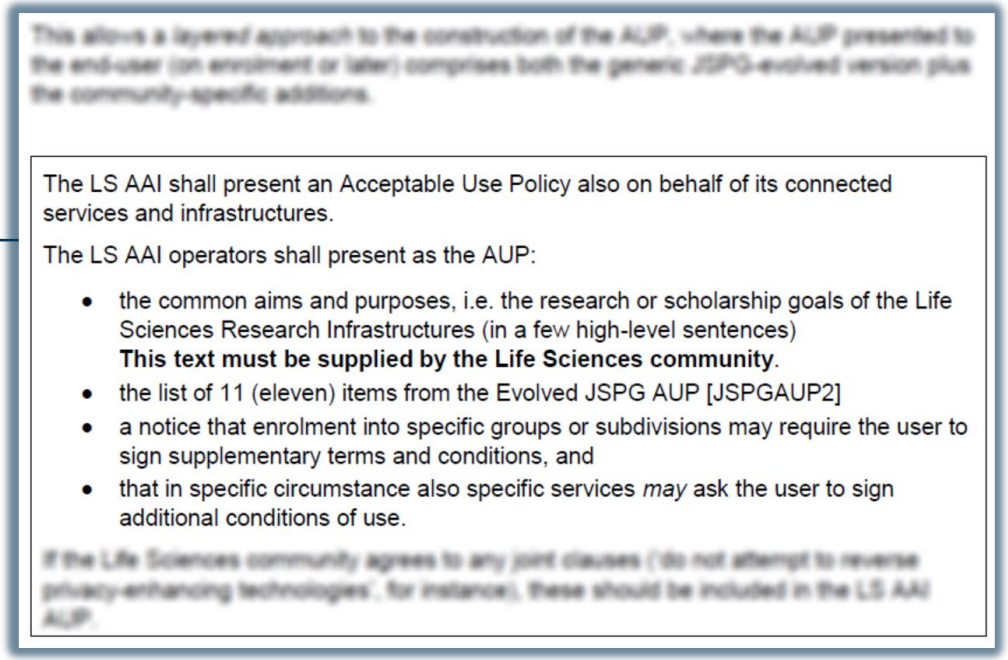
https://aarc-project.eu/guidelines/aarc-i044/

How will this Baseline AUP used?

- Forms part of the information shown to a user **during registration with his/her community**
- AUP provides information on **expected behaviour and restrictions**
- ‘baseline’ text can, **optionally, be augmented** with additional, community or infrastructure specific, clauses as required, but the numbered clauses should not be changed
- Registration point where the user is presented with the AUP may be **operated directly** by the user's research community **or by a third party** on the community's behalf

Scaling Acceptable Use Policy and data release

impractical to present user ‘click-through’ screens on each individual service



This allows a layered approach to the construction of the AUP, where the AUP presented to the end-user (on enrolment or later) comprises both the generic JSPG-evolved version plus the community-specific additions.

The LS AAI shall present an Acceptable Use Policy also on behalf of its connected services and infrastructures.

The LS AAI operators shall present as the AUP:

- the common aims and purposes, i.e. the research or scholarship goals of the Life Sciences Research Infrastructures (in a few high-level sentences) **This text must be supplied by the Life Sciences community.**
- the list of 11 (eleven) items from the Evolved JSPG AUP [JSPGAUP2]
- a notice that enrolment into specific groups or subdivisions may require the user to sign supplementary terms and conditions, and
- that in specific circumstance also specific services *may* ask the user to sign additional conditions of use.

If the Life Sciences community agrees to any joint clauses ('do not attempt to reverse privacy-enhancing technologies', for instance), these should be included in the LS AAI AUP.

Community conditions

Community specific terms & conditions

Community specific terms & conditions

RI Cluster-specific terms & conditions

Common baseline AUP
for e-Infrastructures and Research Communities
(current draft: JSPG Evolved AUP –
leveraging comparison study and joint e-Infrastructure work)

Also picked up by others, e.g. FH VORARLBERG

https://wiki.geant.org/x/P4bWBQ

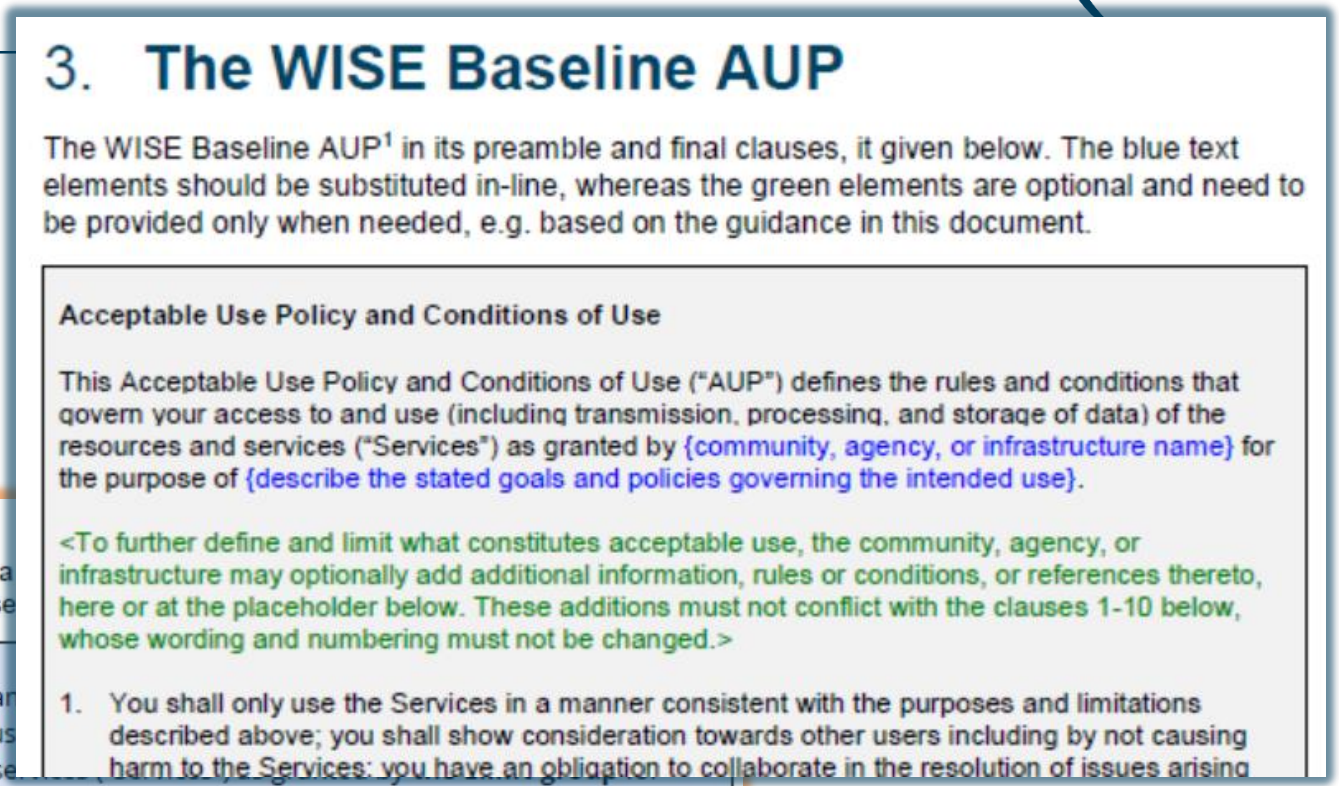
WISE Baseline AUP – and how to apply it for your Infrastructure

https://aarc-project.eu/guidelines/aarc-i044/

AARC-I044

- Includes the final WISE Baseline AUP text
- for both 'community-first' and 'user-first' MMS services (attribute authorities)
- examples make it concrete

Seen rapid take-up
by e-Infras
(both global and national)



3. The WISE Baseline AUP

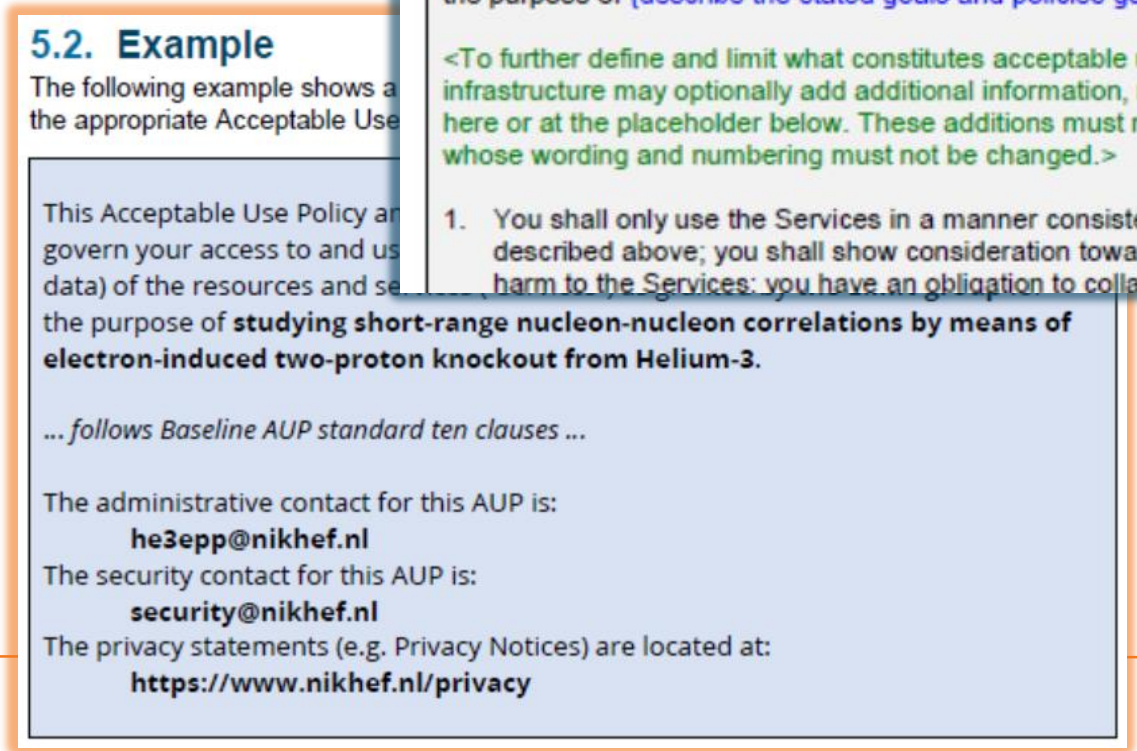
The WISE Baseline AUP[1] in its preamble and final clauses, it given below. The blue text elements should be substituted in-line, whereas the green elements are optional and need to be provided only when needed, e.g. based on the guidance in this document.

Acceptable Use Policy and Conditions of Use

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

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

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



5.2. Example

The following example shows a
the appropriate Acceptable Use

This Acceptable Use Policy ar
govern your access to and us
data) of the resources and se
the purpose of **studying short-range nucleon-nucleon correlations by means of electron-induced two-proton knockout from Helium-3.**

... follows Baseline AUP standard ten clauses ...

The administrative contact for this AUP is:
he3epp@nikhef.nl
The security contact for this AUP is:
security@nikhef.nl
The privacy statements (e.g. Privacy Notices) are located at:
https://www.nikhef.nl/privacy

Next steps

- Publication on the WISE SCI pages and Wiki
- Adoption by the Infrastructures – already happened for EGI & GEANT/eduTEAMS, and will happen in others (WLCG) and for many more through its AEGIS endorsement
- Take-up also in national (R&E) Infrastructures

Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).