AARC Authentication and Authorisation for Research and Collaboration

Baseline AUP Study

e-Researcher-centric policies (NA3.3)

Ian Neilson

STFC – UK Research and Innovation

Science & Technology Facilities Council | UK Research and Innovation

Joint EOSC-hub/AARC2/EGI/EUDAT/WLCG Security Policy Workshop / CERN

April 2018

Context

- AARC2 - e-Researcher-centric policies (NA3.3)
- Inventory of high-assurance identity requirements from the AARC2 use cases
  - Milestone Document AARC2-MNA3.5 (submitted Jan 2018) referencing wiki page with requirements identified from use-cases. Further requirements may be added if identified during the project.
- Acceptable Use Policy alignment study
  - https://wiki.geant.org/pages/viewpage.action?pageId=86736956
  - Presented AARC2 All-hands, Athens, April 2018
  - Updated EUGridPMA, Karlsruhe, May 2018
    - https://wiki.geant.org/pages/viewpage.action?pageId=108007315
  - Today's objectives
    - Brief review of the AUP task (based on Athens slides)
    - Discussion and integration of feedback

Motivation

To make a recommendation for the content of an Acceptable Use Policy (AUP) to act as a baseline policy (or template) for adoption by research communities.

- To facilitate -

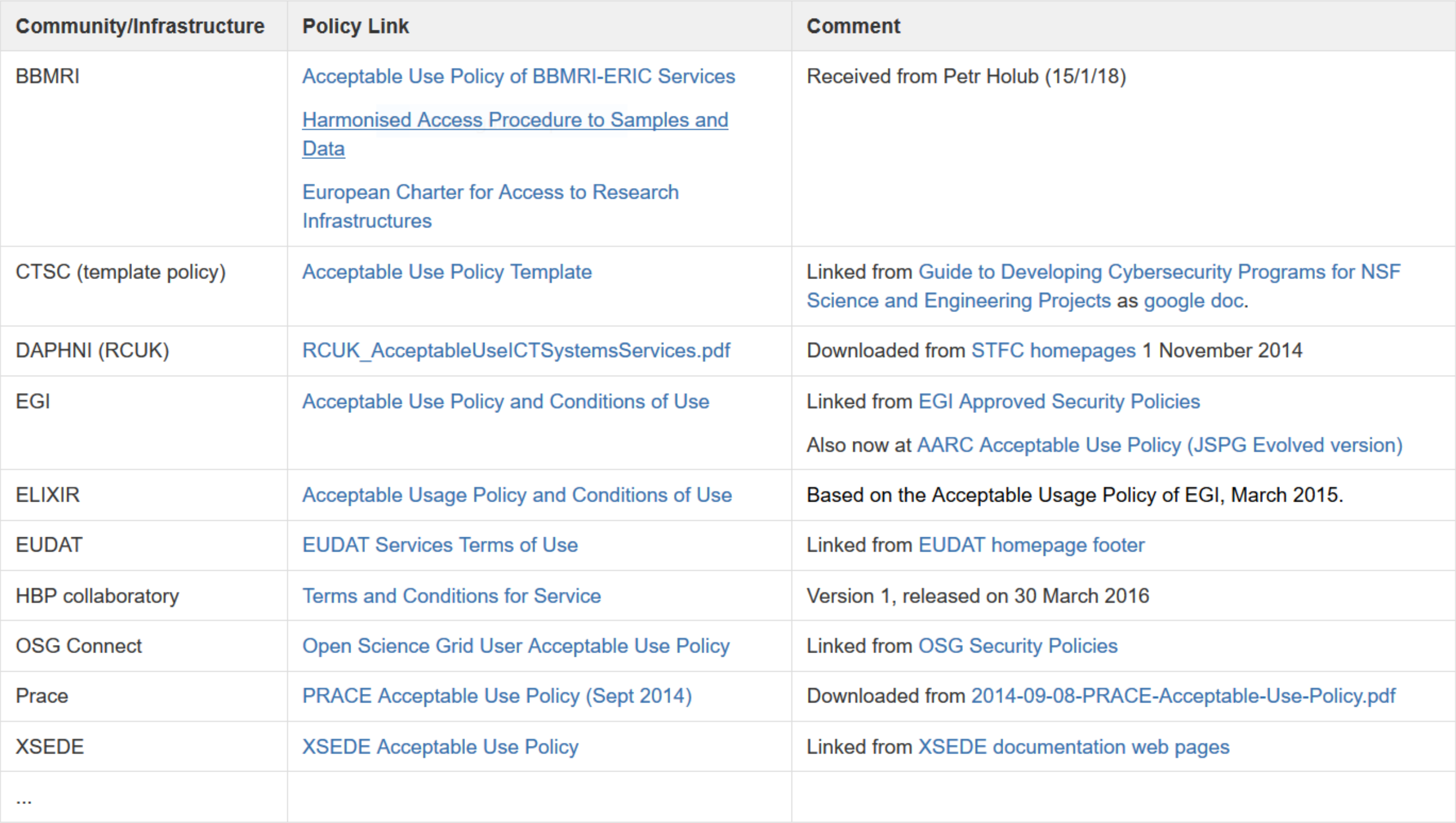
  a) a more rapid community infrastructure ‘bootstrap’

  b) ease the trust of users across infrastructures

  c) provide a consistent and more understandable enrolment for users.

- Adoption of a policy preferred to template

Inputs

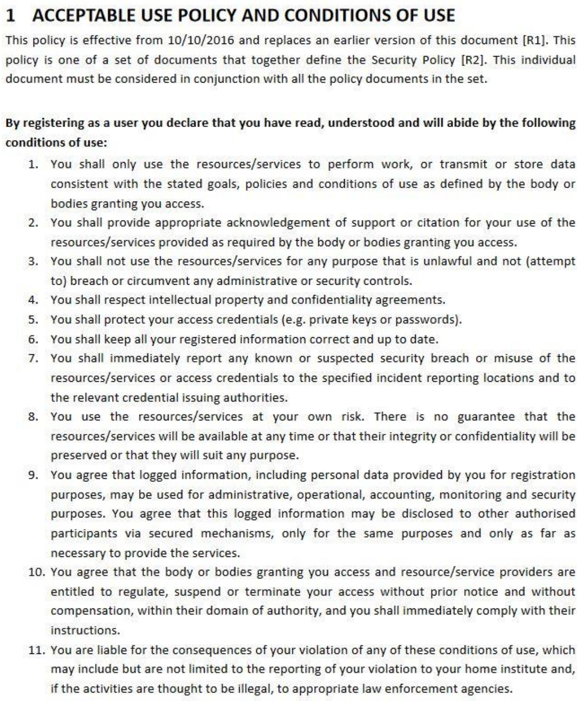


Community/Infrastructure	Policy Link	Comment
BBMRI	Acceptable Use Policy of BBMRI-ERIC Services Harmonised Access Procedure to Samples and Data European Charter for Access to Research Infrastructures	Received from Petr Holub (15/1/18)
CTSC (template policy)	Acceptable Use Policy Template	Linked from Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects as google doc.
DAPHNI (RCUK)	RCUK_AcceptableUseICTSystemsServices.pdf	Downloaded from STFC homepages 1 November 2014
EGI	Acceptable Use Policy and Conditions of Use	Linked from EGI Approved Security Policies Also now at AARC Acceptable Use Policy (JSPG Evolved version)
ELIXIR	Acceptable Usage Policy and Conditions of Use	Based on the Acceptable Usage Policy of EGI, March 2015.
EUDAT	EUDAT Services Terms of Use	Linked from EUDAT homepage footer
HBP collaboratory	Terms and Conditions for Service	Version 1, released on 30 March 2016
OSG Connect	Open Science Grid User Acceptable Use Policy	Linked from OSG Security Policies
Prace	PRACE Acceptable Use Policy (Sept 2014)	Downloaded from 2014-09-08-PRACE-Acceptable-Use-Policy.pdf
XSEDE	XSEDE Acceptable Use Policy	Linked from XSEDE documentation web pages
...		

Comparators

- Compare to clauses of “JSPG Evolved”
  - Joint Security Policy Group (EGEE, WLCG, OSG, …….)
  - Current EGI AUP & Conditions of Use
- Why choose this?
  - Common ancestor with several existing AUPs
    - Functional since 2005
  - Deliberately brief and broadly focussed
    - “Easy” to compare
  - Maintained

1. Restrictions on use
2. Acknowledgement or citation
3. Lawful purposes and controls
4. Intellectual property
5. Protect credentials
6. Contact information
7. Incident reporting
8. Risk and suitability
9. Personal data
10. Regulate access
11. Liability and reporting



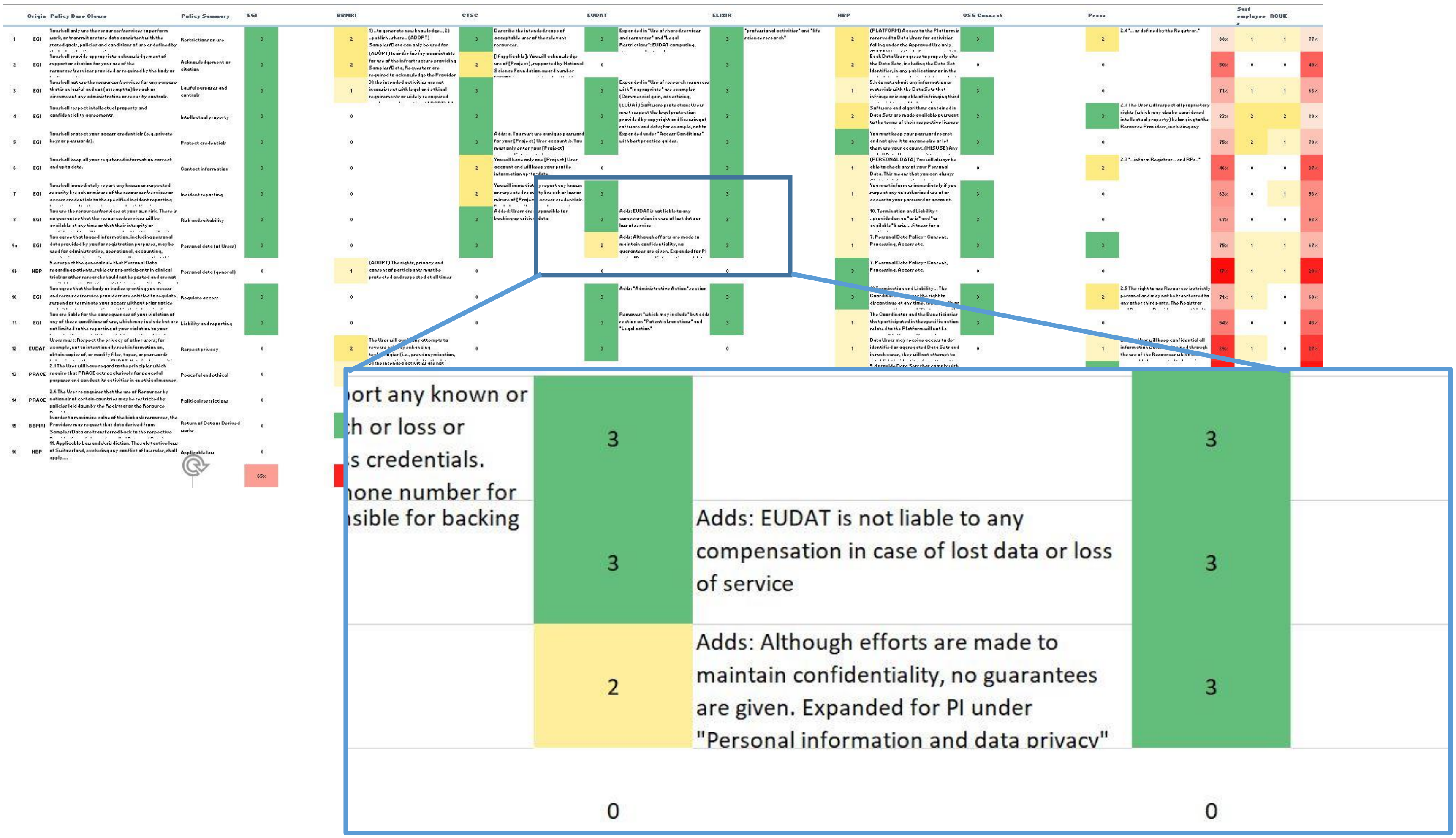
1 ACCEPTABLE USE POLICY AND CONDITIONS OF USE

This policy is effective from 10/10/2016 and replaces an earlier version of this document [R1]. This policy is one of a set of documents that together define the Security Policy [R2]. This individual document must be considered in conjunction with all the policy documents in the set.

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. You shall respect intellectual property and confidentiality agreements.
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 credentials to the specified incident reporting locations and to the relevant credential issuing authorities.
8. You use the resources/services at your own risk. There is no guarantee that the resources/services will be available at any time or that their integrity or confidentiality will be preserved or that they will suit any purpose.
9. You agree that logged information, including personal data provided by you for registration purposes, may be used 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.
10. 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.
11. 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.

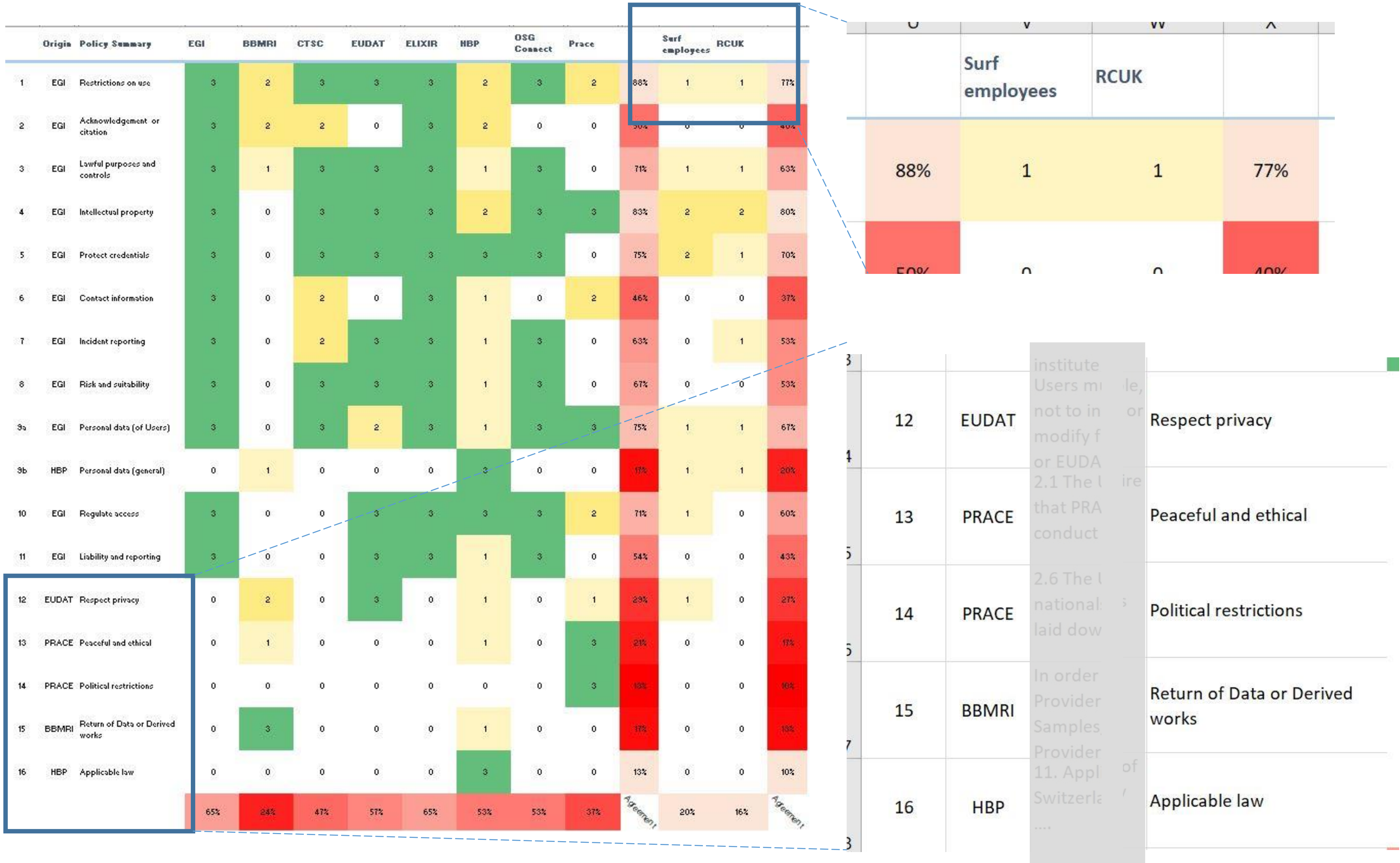
Method - tabulate, compare, “score”



	Origin	Policy Base Clause	Policy Summary	EGI
1	EGI	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	Restrictions on use	3
2	EGI	You shall provide appropriate acknowledgement of support or citation for your use of the resources/services provided as required by the body or	Acknowledgement or citation	3
3	EGI	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.	Lawful purposes and controls	3
4	EGI	You shall respect intellectual property and confidentiality agreements.	Intellectual property	3
5	EGI	You shall protect your access credentials (e.g. private keys or passwords).	Protect credentials	3
6	EGI	You shall keep all your registered information correct and up to date.	Contact information	3
7	EGI	You shall immediately report any known or suspected security breach or misuse of the resources/services or access credentials to the specified incident reporting	Incident reporting	3
8	EGI	You use the resources/services at your own risk. There is no guarantee that the resources/services will be available at any time or that their integrity or	Risk and suitability	3
9a	EGI	You agree that logged information, including personal data provided by you for registration purposes, may be used for administrative, operational, accounting,	Personal data (of Users)	3
9b	HBP	5.e respect the general rule that Personal Data regarding patients, subjects or participants in clinical trials or other research should not be posted and are not	Personal data (general)	0
10	EGI	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	Regulate access	3
11	EGI	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	Liability and reporting	3
12	EUDAT	Users must: Respect the privacy of other users; for example, not to intentionally seek information on, obtain copies of, or modify files, tapes, or passwords	Respect privacy	0
13	PRACE	2.1 The User will have regard to the principles which require that PRACE acts exclusively for peaceful purposes and conduct its activities in an ethical manner.	Peaceful and ethical	0
14	PRACE	2.6 The User recognises that the use of Resources by nationals of certain countries may be restricted by policies laid down by the Registrar or the Resource	Political restrictions	0
15	BBMRI	In order to maximize value of the biobank resources, the Providers may request that data derived from Samples/Data are transferred back to the respective	Return of Data or Derived works	0
16	HBP	11. Applicable Law and Jurisdiction. The substantive laws of Switzerland, excluding any conflict of law rules, shall apply....	Applicable law	0
				65%

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

Summary graphic



	Origin	Policy Summary	EGI	BBMRI	CTSC	EUDAT	ELIXIR	HBP	OSG Connect	Prace		Surf employees	RCUK	
1	EGI	Restrictions on use	3	2	3	3	3	2	3	2	88%	1	1	77%
2	EGI	Acknowledgement or citation	3	2	2	0	3	2	0	0	50%	0	0	40%
3	EGI	Lawful purposes and controls	3	1	3	3	3	1	3	0	71%	1	1	63%
4	EGI	Intellectual property	3	0	3	3	3	2	3	3	83%	2	2	80%
5	EGI	Protect credentials	3	0	3	3	3	3	3	0	75%	2	1	70%
6	EGI	Contact information	3	0	2	0	3	1	0	2	46%	0	0	37%
7	EGI	Incident reporting	3	0	2	3	3	1	3	0	63%	0	1	53%
8	EGI	Risk and suitability	3	0	3	3	3	1	3	0	67%	0	0	53%
9a	EGI	Personal data (of Users)	3	0	3	2	3	1	3	3	75%	1	1	67%
9b	HBP	Personal data (general)	0	1	0	0	0	3	0	0	17%	1	1	20%
10	EGI	Regulate access	3	0	0	3	3	3	3	2	71%	1	0	60%
11	EGI	Liability and reporting	3	0	0	3	3	1	3	0	54%	0	0	43%
12	EUDAT	Respect privacy	0	2	0	3	0	1	0	1	29%	1	0	27%
13	PRACE	Peaceful and ethical	0	1	0	0	0	1	0	3	21%	0	0	17%
14	PRACE	Political restrictions	0	0	0	0	0	0	0	3	13%	0	0	10%
15	BBMRI	Return of Data or Derived works	0	3	0	0	0	1	0	0	17%	0	0	13%
16	HBP	Applicable law	0	0	0	0	0	3	0	0	13%	0	0	10%
			65%	24%	47%	57%	65%	53%	53%	37%	Agreement	20%	16%	Agreement

U	V	W	X
	Surf employees	RCUK	
88%	1	1	77%
50%	0	0	40%

		institute	
12	EUDAT	Users mı le, not to in or modify f or EUDA	Respect privacy
13	PRACE	2.1 The ı ire that PRA conduct	Peaceful and ethical
14	PRACE	2.6 The ı national: laid dow	Political restrictions
15	BBMRI	In order Provider Samples, Provider	Return of Data or Derived works
16	HBP	11. Appl of Switzerla	Applicable law

Revision in May 2018

- Current EGI AUP clauses do provide a reasonable baseline
- Changes made at EUGridPMA, May 2018
    - https://wiki.geant.org/pages/viewpage.action?pageId=108007315
  - Adjustment to introduction clause to allow ‘augmentation’
  - Removal of acknowledgement and citation *(can be augmenting clause)*
  - Change to risk transfer –
    - ~~You use the resources/services at your own risk. There is no guarantee that the resources/services will be available at any time or that their integrity or confidentiality will be preserved or that they will suit any purpose.~~
    - You shall ensure that any reliance you place on the confidentiality, integrity and availability of resources/services is covered by appropriate agreements. Use without such agreements is at your own risk.
  - Change to personal data handling –
    - ~~You agree that logged information, including personal data provided by you for registration purposes, may be used 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.~~
    - You agree that use of your personal data shall be governed by the published privacy policies of the body or bodies granting you access, of the infrastructure and of the resource/service providers.

JSPG Evolved AUP version 2 (May 2018)

By registering as a user you agree to abide by the following conditions of use which may be augmented by additional agreements which shall also apply:

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 not use the resources/services for any purpose that is unlawful and not (attempt to) breach or circumvent any administrative or security controls.*
3. *You shall respect intellectual property and confidentiality agreements.*
4. *You shall protect your access credentials (e.g. private keys or passwords).*
5. *You shall keep all your registered information correct and up to date.*
6. *You shall immediately report any known or suspected security breach or misuse of the resources/services or access credentials to the specified incident reporting locations and to the relevant credential issuing authorities.*
7. *You shall ensure that any reliance you place on the confidentiality, integrity and availability of resources/services is covered by appropriate agreements. Use without such agreements is at your own risk.*
8. *You agree that use of your personal data shall be governed by the published privacy policies of the body or bodies granting you access, of the infrastructure and of the resource/service providers.*
9. *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.*
10. *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.*

Comments review 1

Mischa Salle -

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 not use the resources/services for any purpose that is unlawful and not (attempt to) breach or circumvent any administrative or security controls.

- *strictly speaking, 2 is already covered by 1, isn't it? (I know it's nitpicking)*

7. You shall ensure that any reliance you place on the confidentiality, integrity and availability of resources/services is covered by appropriate agreements. Use without such agreements is at your own risk.

- *end-users will probably not understand what is meant with 7, and if they already understand, they will probably not know how to get that working...*

9. 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.

- *Is point 9 really what we want to say, also in post-Grid era? For some yes, but in general this is rather harsh and probably not acceptable for a number of communities using production infrastructure*

Comments review 2

Niels van Dijk – "We are trying to implement the AUP for eduTEAMS"

- *What is the purpose of this document? Is it provided by a platform independently of the community, or is the expected to be an integral part of the agreement the community will present to the user?*
- *What is the scope of the document? Is it only about the AAI platform itself or also about all connected services? I note the latter are neither declared in or out of scope.*
- *The wording is sometimes ambiguous (i will discuss specific examples later on). As an introduction into the list of I would expect something like e.g. (here for eduTEAMS):*

  "This Acceptable Use Policy ("AUP") sets forth the principles that govern the use of the eduTEAMS resources and services (the "Services") provided by the operator GEANT Association ("Service Operator") and to its community members ("Users"). The Services enable the Users to use the identities from their home organisations (HO) for authentication and identification purposes, while augmenting the information available from the HO, with community specific information, such as membership and roles within the community."

  - *From then on the words "Services", "Service Provider" and "Users" have defined context and should be used a such. Especially useful as later-on the AUP will discuss services, but then in the context of services that are connected to the Service.*
  - *Then I would propose to make sure the use of semantics is consistent. So not "You shall only use the resources/services" but "You shall only use the Services".*

Comments review 3

Cont … from Niels van Dijk

- *What is the assumed GDPR role of the Service Operator?*
  - *Is it envisioned the AUP handles both Data processor and Data controller cases?*
  - *Is the CO also assumed to be a data controller? While that is primarily something that should be reflected in a privacy policy, some of the wording in the AUP may be confusing as the relation between the Service Operator and the CO. Like e.g "with the stated goals, policies and conditions of use as defined by the body or bodies granting you access" This clearly suggest the CO is the controller. However what if the CO is not a legal entity? In such case it cannot be a data controller.*
- *What is the expected scope of the operator? Is it to provide a technical platform that allows a community to operate its AAI? If so, the AUP should ONLY engage with things that are relevant in that context. So security, fair use etc are in, but IPR, copyright are out as that is up to the community.*
- *I note all of the things in the AUP protect the Service Operator, none protect the user. What may a user reasonably expect for the Service Operator? It makes it an unfair AUP. I would have expected stuff like "we protect you privacy as layed out by our privacy policy (and point to reference), we do not take you IPR. We will not sell you data personal or otherwise. etc. Where/how are these described?*

Comments review 4

Cont … from Niels van Dijk cont

- *I think a AUP should contain a direct pointer to the privacy policy and if it is there, also a terms of service, so we do not create a "it is up to you to find all relevant information" puzzle for the users*
- *Is there a difference in AUP between the REAL end user and a user that is action on behalf off the community as the admin?*

Comments review 5

Cont… from Niels van Dijk

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.

- *"to perform work" is not relevant here.*
  - *First of all because later in the same sentence it said that the actual reason for using the service is "the stated goals, policies and conditions of use as defined by the body or bodies granting you access"*
  - *Second, because there might e.g. be Citizen scientists participating in the collaboration who are not joining "to perform work“*
  - *Also See my generic comment that what constitutes the service should be clearly defined. And suggestion to use proper semantics*

3. You shall respect intellectual property and confidentiality agreements.

  - *While that is a fair statement, it is not one to make for the Service Operator to make, but for the community*

Comments review 6

Cont… from Niels van Dijk

7. You shall ensure that any reliance you place on the confidentiality, integrity and availability of resources/services is covered by appropriate agreements. Use without such agreements is at your own risk.

This statement is unfair, impossible to enforce and possibly against the law:

- *Whatever role the platform has under GDPR, a breach of either confidentiality, integrity or availability of personal data is by definition a data leak and hence the Service Operator has responsibility. This responsibility cannot be waved off like this. If you allow personal data to be collected you have responsibilities.*
- *How would a normal end user learn about what is "covered by appropriate agreements"?. Assuming an end user gets invited by the community, do we really expect the user to then go and check the contract between the Service Operator and the community? How would that work in practice?*
- *If I were an operator of an identity provider I would not ever release personal data to an entity that basically declares any issue with data confidentiality, integrity and availability not its problem*
  To me the whole purpose of community AAI platforms is to enable communities to do their work. To allow that to happen you need to create an AAI that is trusted and worry free. This statement is orthogonal to all of that.

Comments review 6

Cont… from Niels van Dijk

9. You agree that use of your personal data shall be governed by the published privacy policies of the body or bodies granting you access, of the infrastructure and of the resource/service providers.

- *Here the scope suddenly gets stretched. In (1) we had two entities: "the body or bodies granting you access" and "Service Operator". Now we suddenly we also have "the infrastructure" Which infrastructure? Operated by whom? Where? How is it different from the other entities?*
  Where/how can the user find these privacy polities?

10. 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.

- *What does "and you shall immediately comply with their instructions." entail? Can you provide with an example of what a user would have to do?*

Thank you

Any Questions?

ian.neilson@stfc.ac.uk

AARC

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).

Acceptable Use Policy alignment study

Acceptable Use Policies can vary considerably between organisations, service providers, and infrastructures. An AUP alignment study [AUPSTUDY] is currently ongoing, and its preliminary results indicate there is one 'family' of AUPs that are roughly similar, but beyond that a wider range of quite disparate AUP models. Of these disparate AUPs, many are either project specific and name specific services, or include managerial content (such as sanctions) that are specific to the Infrastructure or organisation. Organisational AUPs in addition may include references to personal use that are not appropriate in this case.

The one 'family' of AUPs are all derived from a single source, the Joint Security Policy Group Acceptable Use Policy (2006), whose signature has been preserved over time. This common heritage is evident …………

David Groep et al. - Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)
https://aarc-project.eu/guidelines/aarc-g040/

JSPG Evolved version 1 (April 2018)

- 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.
- 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.
- 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.
- You shall respect intellectual property and confidentiality agreements.
- You shall protect your access credentials (e.g. private keys or passwords).
- You shall keep all your registered information correct and up to date.
- You shall immediately report any known or suspected security breach or misuse of the resources/services or access credentials to the specified incident reporting locations and to the relevant credential issuing authorities.
- You use the resources/services at your own risk. There is no guarantee that the resources/services will be available at any time or that their integrity or confidentiality will be preserved or that they will suit any purpose.
- You agree that logged information, including personal data provided by you for registration purposes, may be used 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.
- 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.
- 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.