Authentication and Authorisation for Research and Collaboration

Baseline AUP Study

e-Researcher-centric policies (NA3.3)

Ian Neilson
STFC – UK Research and Innovation

AARC2 All-hands meeting / Athens
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
  - Work in progress
  - https://wiki.geant.org/pages/viewpage.action?pageId=86736956

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

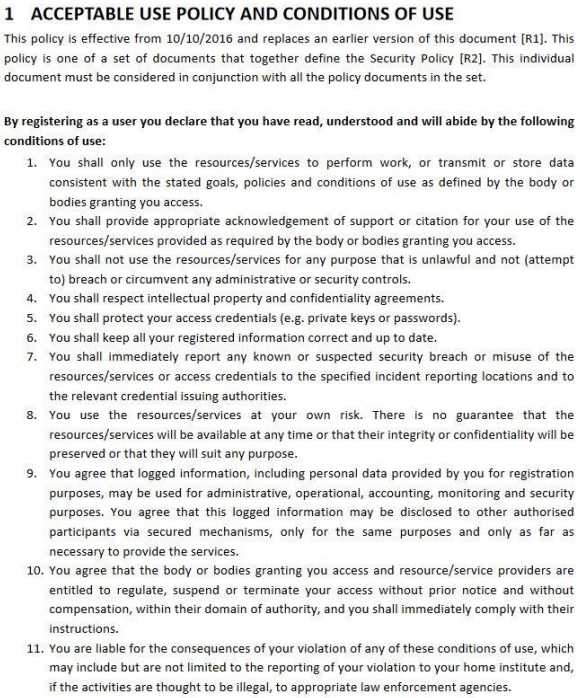
Inputs

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



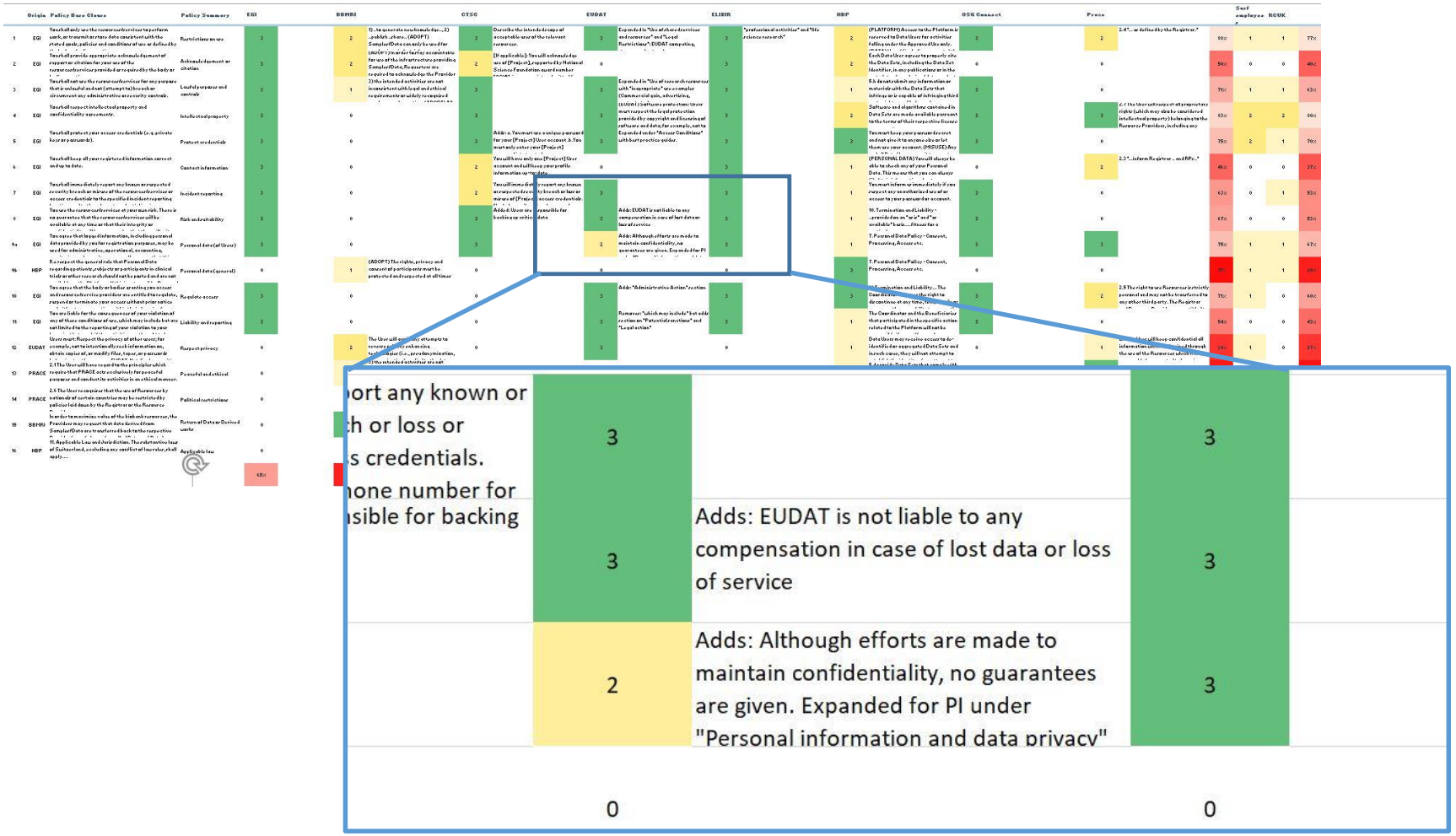
1 ACCEPTABLE USE POLICY AND CONDITIONS OF USE

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.

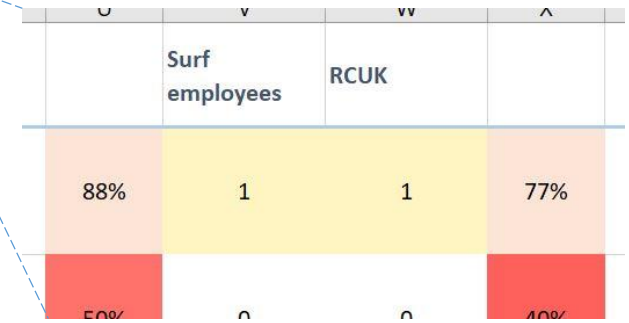
Method - tabulate, compare, “score”



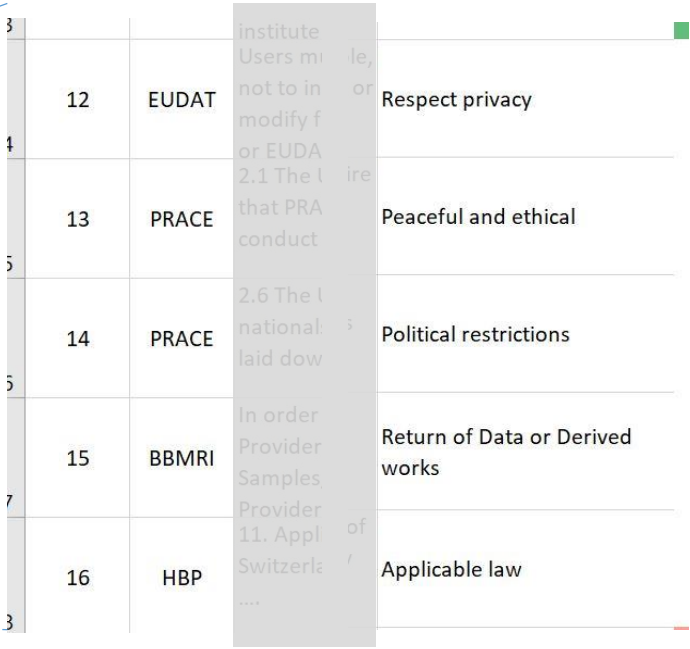
ort any known or h or loss or s credentials. hone number for sible for backing	3	3
	3 Adds: EUDAT is not liable to any compensation in case of lost data or loss of service	3
	2 Adds: Although efforts are made to maintain confidentiality, no guarantees are given. Expanded for PI under "Personal information 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				
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%	28%	47%	57%	65%	53%	53%	37%	Agreement	20%	16%	Agreement



	Surf employees	RCUK	
88%	1	1	77%
50%	0	0	40%



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

Conclusions

- Current EGI AUP clauses do provide a reasonable baseline
  - https://wiki.geant.org/pages/viewpage.action?pageId=97945151
- Some areas for consideration (based on scoring)
  - Personal data
    - How the user's (researcher) data is processed
      - Privacy Notices and Conditions of Use
    - How the user (researcher) treats 3rd party data
      - Respect Privacy of others
  - Ethical Use
    - EGI silent but implicit
  - Acknowledgement & Citation
    - European Charter for Access to Research Infrastructures
  - Contact Information
    - Maintenance

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/

AUP Study – "JSPG Evolved" as baseline?

- 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.

Thank you

Any Questions?

Ian.neilson@stfc.ac.uk

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).