

# **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
  - <u>Milestone Document AARC2-MNA3.5</u> (submitted Jan 2018) referencing <u>wiki</u> <u>page with requirements</u> 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

- 7. Incident reporting
- 2. Acknowledgement or citation 8. Risk and suitability
- 3. Lawful purposes and controls 9. Personal data
- 4. Intellectual property

10. Regulate access

5. Protect credentials

11. Liability and reporting

6. Contact information

#### 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:

- 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 graphing you access
- Dodies 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.
- 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.
- 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.
- 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"



Palicy Bare Claure	Palicy Summery	EGI	BBMRI	erse	EUDAT	FLIEIR	HBP	OSG Cannest	Press		Surf employee ROUS	
Yourhall only we the resources front contaperform work, or transmit arcture data consistent with the stored goals, palleter and conditions of we as defined by Yourhall provide appropriate acknowledgement of	Restrictions on we	*	1) . to generate new knowledge 2 . publish . shore. (ADDPT) Samplus Data can ank) be weed for (ADDPT) to airdistanting accounts	g acceptable was of the re	levent 3 endrormercer* and "Lo Restrictions": EUDAT o	rel 2 reinneurorech*	2 received to D fulling under	Accounts the Platform in the University of the University of the Appraised University of the Appraised University of the Appraised to properly of the	2 2.41	or defined by the Registrer."	1 ,	77%
repport or citation for your use of the resources from item provided or required by the body or		3	far uso of the infrastructure provis Sampler/Data, Requestors are required to acknowledge the Provi	inq 2 wo of [Project]_repport	chraufedeo ad by Notional g rénumber Loyanded in 'Use of res	*	2 the Date Sets Identifier, in-	respects properly cite , including the Data Set g ny publications or in the mit my information or		50%		40%
Yaushall not use the resources fear vises for any purpose that is unlauful and not (attempt to) broach or air converent any administrative arrequently controls.	Lauful purparer and cantrals		2) the intended activities are not incompletent with logal and othical requirements or widely recognized		Engended in The off re- guith "in oproprieto" we (Commercial quin, afo- (NUMA) San'twee pre-	oxempler stiring,	n materials wit infrinça es is	s the Data Setrithat apable of infringing third	•	The	1 1	63%
Yauzhall respect intollectual praporty and ausfidentiality agreements.	intellactual property	30	10	3	murtrarpost the legals pravided by empyright raftwere and data: far	ratuction nd Sconnings yamelo, natta	2 Data Satz are to the termina	algorithme contained in mode available purvent 3 f their respective license	3 right	z (uhich may alza bo cauzidorod loctual praporty) holanging ta tho rarco Pravidorz, including any	92 3	80%
Yauzh all prato et yeur accoer ero dontisk (o.q. privato koprar pezzuardr).	Protect credentials	*	0	Adde a Teamout are our g for your (Project) User o mout only onless your (Pro	occount b.You 3 with burt practice quid niret]	r Conditions* v. 3	3 and not give i them we you	year persented or or to the onyone observat.  The onyone observat.  The onyone of the or to the or		75×	2 1	70%
Yaurhall keep all your registered information correct and up to date.	Castect information	3		You will have only one (P) 2 account and will knop you information up-to-date.	urprofile g	*	g able to check Data Thirms	PATA) Yavu ill alu oyz bo any af yave Postanal anz thet you con alu oyz	2 23*	_inform Regists or _ and RPs_**	0 0	576
Yourhall immo firstely report only known or ruspected so curity beseth or misuse of the resources/services or occors are deathful to the specified incident reporting	Incident reporting	à.	0	2 arxurpectodrocu tybro miraro of [Preject   ecce	art eny knawn ook er laur er er orodentielr.	3	1 zurpockanyu acceszta yes	rm w immediatoly if you coutherized we of ar r parruardar account.		63×	0 1	53×
You we the renouncertransicer at your own risk. There is no quarantee that the renouncertransicer will be available at any time or that their integrity or	Pürk en ézeitebility	\$	•	Adduct Usoss era uspena 3 becking up critic data	Add: EUDAT ir nat liabi g compensation in care o lars of service	flart dotoer y	1 .pravidadas available ba	ovand Liability - en "oria" and "or Gr Jitnoss far a		167×	0 0	\$210
You agree that In age distorm ation, in cluding parronal data practiced by you for registration purposes, may be used for administrative, operational, accounting,	Possenel data (of Uross)	<b>b</b>	•	3	Addr: Although offertr 2 maintein cuadidantialit quarantee are given. E	y, to g	7. Porrenel D 1. Processing, #	ste Palicy - Canzont, coursete.	3	19×	1 1	67%
So respect the general rule that Possenal Data regarding patients, rubjects or participents in clinical tricks as other research should not be parted and are ass	Posrenel data (general)	0	(ADOPT) The rights, privacy and concent of porticip entropy and protected and respected at all time.			60 CO	g Proceering, F		. 0	- 1000	1 1	2000
Yaw ogroe that the lody ar badier grenting yaw access on drasaw cofrarnice providers are antitled to regulate suspend ar torminato yawr access without prior natice	* Regulate access		•	3	3	iction*zoction	g Caardinas directions o		2.5T 2 pers onys	ho right to use Resources is strictly and and may not be transferred to other third party. The Registres	1 6	60×
You are liable for the conce guester of your violation of any of these conditions of use, which may include but as not limited to the reporting of your violation to your	* Lishibly endroperting	2	•		Remanuer "which may in goodins on "Potontialer "Legal action"	citods but edds notions and	1 thatparticip- related to the	tar and the Beneficiaries thed in the specific action 3 Platform will eat be		54%	0 0	4300
User most: Respect the privacy of other weer, for exemple, not mintentionally reak information on, obtain copies of, or modify files, toper, or passues of	Raspact privacy	•	The Uner util eye intry ottompte to reverse to any enhancing tool onior (i.e., previdenymizati	0 an,	9	6	Data Urerr m i identificator in rech carer,	pyroceino accept to do- nepropeto d'Data Sotr and thoy will not attompt to	1 infan thes	metion unit keep confidential all metion unit in debraugh 297 pe of the Forour cor which	1 6	27.0
2.1The Upon will have request to the principles which require that PRACE acts exclusively for proceeds purposes and another the nativities in an other manage.	Poecoful and othical	0)	oj tha nikariin d'actoliniii ati nabi				6 44.0	e Caraka amada da		100 8		_
2.6 The User recognizer that the use of Resources by nationals of certain countries may be restricted by policies leid down by the Registrar or the Resource	Palkicelrestrictions	0	ort any kr	nown or								
In order to mecimize value of the biobank remover, th Provides may request that data derived from Samples (Data are transferred back to the respective	Raturn of Date or Darina works		h or loss	or	3					3		
11. Applicable Law and Justi diction. The substantive law of Switzerland, excluding any conflict of law rates, shall apply	Applicable lau	0	s credenti	als.						3		
	(G)	45%	none num	*A-20000								
			isible for b			Adds: EUDAT	icnot	liable to any				
			ISIDIE IOI L	Jacking		STATE OF THE STATE		the state of the s	%			
					3	compensatio	n in cas	se of lost data	or loss	3		
						of service						
						Adds: Althou	gh effo	rts are made	to			
						maintain con						
					2					3		
						are given. Ex						
						"Personal inf	ormation	on and data r	rivacv"			
					0					0		
					0					0		

# **Summary graphic**



200	Origin	Policy Summary	EGI	BBMRI	CTSC	EUDAT	ELIXIR	НВР	OSG Connect	Prace		Surf employees	RCUK				C			
	EGI	Restrictions on use	3	2	3	3	3	2	3	2	88%	1	1	77%			Surf employees	RCUK	200	
	EGI	Acknowledgement or citation	3	2	2	0	3	2	0	0	204	0	-	404						
		Lawful purposes and controls	3	210	3	3	3	1:	3	0	71%	18	<b>31</b>	63%		88%	1		1	77%
	EGI	Intellectual property	3	0	3	3	3	2	3	3	83%	2	2	80%						
	EGI	Protect credentials	3	0	3	3	3	3	3	0	75%	2	j	70%		E09/	0		n	400/
	EGI	Contact information	3	0	2	0	3	1	0	2	46%	0	0	37%						
	EGI	Incident reporting	3	0	2	3	3	1	3	0	63%	0	/1	53%			inet			
	EGI	Risk and suitability	3	0	3	3	3	1	3	0	67%	0		53%						
	EGI	Personal data (of Users)	3	0	3	2	3	1	3	3 -	75%	1	1	67%		12	EUDAI		Respect privacy	
	НВР	Personal data (general)	0	1	0	0	0	3	0	0	H%	1.	ı	20%	1					
	EGI	Regulate access	3:	0	0		3%	3	3	2	71%	18	0	60%		13	PRACE		Peaceful a	and ethical
	EGI	Liability and reporting	3	0	0	3	3	1	3	0	54%	0	0	43%	5					
	EUDAT	Γ Respect privacy	0	2	0	3	0	1	0	1	29%	1	0	27%		14	PRACE nati		Political restrictions	
	PRACE	E Peaceful and ethical	0	1	0	0	0	1	0	3	21%	0	0	98	5					
	PRACE	E Political restrictions	0	0	0	0	0	0	0	3	(13%)	0	0	10%		15			Return of Data or Derive works	
	BBMRI	Return of Data or Derived works	0	3	o	0	0	1	0	0	17%	0	0	18%	7	15	Sam			
6 НВР	НВР	Applicable law	0	0	0	0	0	3	0	0	13%	0	0	10%						
			65%	24%	47%	1% 57%	65%	53%	53%	37%	V. George	20%	16%	No contra	h .	16	HBP Swit		Applicable	e law

#### **Conclusions**



- Current EGI AUP clauses do provide a reasonable baseline
  - <a href="https://wiki.geant.org/pages/viewpage.action?pageId=97945151">https://wiki.geant.org/pages/viewpage.action?pageId=97945151</a>
- 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 3<sup>rd</sup> 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?

lan.neilson@stfc.ac.uk



https://aarc-project.eu

