Authentication and Authorisation for Research and Collaboration

AARC2 NA3 Acceptable Use Policy alignment

Ian Neilson
AARC2 NA3.3 Co-ordinator

Science & Technology Facilities Council

44th EUGridPMA, Toulouse
September 24-26, 2018

AARC2 NA3
Task 3 - e-Researcher-Centric Policies

"… develop the policy framework for communities, providing recommendations for baseline "policy profiles" for users, communities and identity providers, and, through such harmonisation, will reduce the "policy silos" that hinder interoperation. The policy profiles will be defined in close interaction with European and global stakeholders, specifically the e-infrastructures and research infrastructures, so that in the AAI ecosystem every participant is able to rely on well-defined predictable behaviour by the other participants in the infrastructure."

- MS19:MNA3.5:Month 9 ✓
  - Inventory of high-assurance identity requirements from the AARC2 use cases

- D3.3:DNA3.4:Month 24
  - Recommendations for e-Researcher-Centric Policies and Assurance

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.

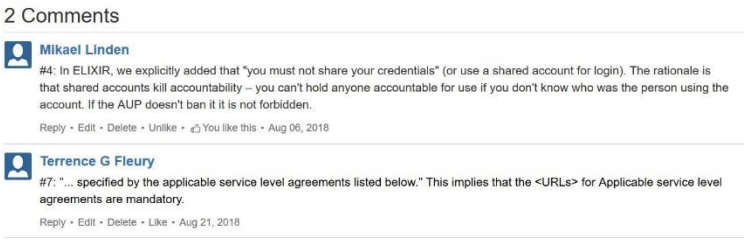
- To facilitate -
  a) a more rapid community infrastructure 'bootstrap'
  b) ease the trust of users across infrastructures
  c) provide a consistent and more understandable enrolment for users.
- Adoption of a policy preferred to template

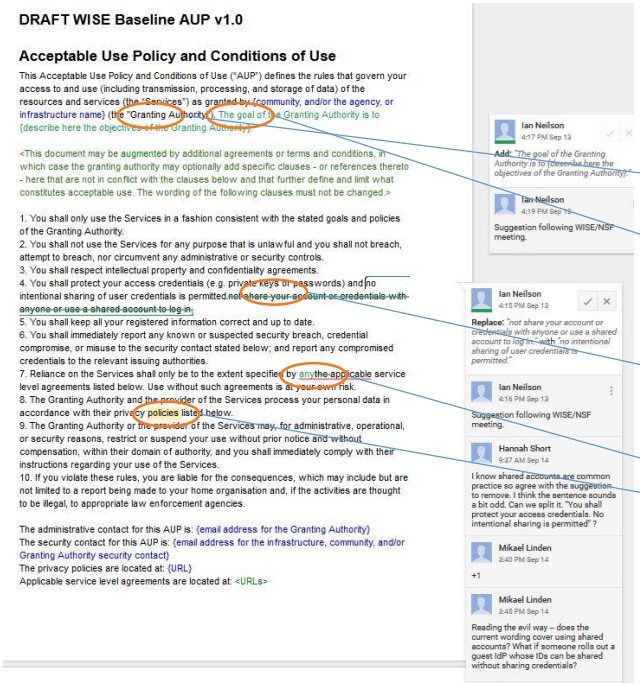
WISE Baseline AUP trajectory

- WISE security group meeting in Abingdon, UK 27/2/2018
  - Decide to base on “historic” JSPG (EGEE/WLCG/OSG/PRACE et al) AUP after analysis of existing community AUPs
  - https://wiki.geant.org/x/PIArBQ
- AARC2 third project meeting in Athens, Greece 10-13/4/2018
  - and 43rd EUGridPMA meeting in Karlsruhe, Germany 23-26/5/2018 with additional material
- EOSC-hub/AARC2/EGI/EUDAT/WLCG Joint Security Policy Workshop at CERN, Switzerland 18-20/7/2018
  - Significant re-wording based on feedback after AARC all-hands meeting
  - Basic clauses stay the same (less one) but restructured
  - Sustainable via WISE group -> Baseline AUP v1.0
- WISE @ 2018 NSF Cybersecurity Summit in Alexandria, VA, USA 21/8/2018
  - Thanks to Dave Kelsey
  - Comments and suggestions to follow
- 44th EUGridPMA @ Toulouse ? ……

Current draft discussion points

AARC wiki -




DRAFT WISE Baseline AUP v1.0

Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules that govern your access to and use (including transmission, processing, and storage of data) of the resources and services (the "Services") as granted by {community, and/or the agency, or infrastructure name} (the "Granting Authority"). The goal of the Granting Authority is to {describe here the objectives of the Granting Authority}.

<This document may be augmented by additional agreements or terms and conditions, in which case the granting authority may optionally add specific clauses - or references thereto - here that are not in conflict with the clauses below and that further define and limit what constitutes acceptable use. The wording of the following clauses must not be changed.>

1. You shall only use the Services in a fashion consistent with the stated goals and policies of the Granting Authority.
2. You shall not use the Services for any purpose that is unlawful and you shall not breach, attempt to breach, nor 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) and no intentional sharing of user credentials is permitted not share your account or credentials with anyone or use a shared account to log in.
5. You shall keep all your registered information correct and up to date.
6. You shall immediately report any known or suspected security breach, 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 anythe applicable service level agreements listed below. Use without such agreements is at your own risk.
8. The Granting Authority and the provider of the Services process your personal data in accordance with their privacy policies listed below.
9. The Granting Authority or the provider of the Services may, for administrative, operational, or security reasons, restrict or suspend your use without prior notice and without compensation, within their domain of authority, and you shall immediately comply with their instructions regarding your use of the Services.
10. If you violate these rules, you are liable for the consequences, which may include but are not limited to a report being made to your home organisation and, if the activities are thought to be illegal, to appropriate law enforcement agencies.

The administrative contact for this AUP is: {email address for the Granting Authority}
The security contact for this AUP is: {email address for the infrastructure, community, and/or Granting Authority security contact}
The privacy policies are located at: {URL}
Applicable service level agreements are located at: <URLs>

Ian Neilson 4:17 PM Sep 13
Add: "The goal of the Granting Authority is to [describe here the objectives of the Granting Authority)."
Ian Neilson 4:19 PM Sep 13
Suggestion following WISE/NSF meeting.
Ian Neilson 4:15 PM Sep 13
Replace: "not share your account or credentials with anyone or use a shared account to log in." with "no intentional sharing of user credentials is permitted."
Ian Neilson 4:16 PM Sep 13
Suggestion following WISE/NSF meeting.
Hannah Short 9:37 AM Sep 14
I know shared accounts are common practice so agree with the suggestion to remove. I think the sentence sounds a bit odd. Can we split it, "You shall protect your access credentials. No intentional sharing is permitted" ?
Mikael Linden 3:40 PM Sep 14
+1
Mikael Linden 3:45 PM Sep 14
Reading the evil way – does the current wording cover using shared accounts? What if someone rolls out a guest IdP whose IDs can be shared without sharing credentials?

- Google doc

Nobody likes “Granting Authority”

Describe the goal of the Granting Authority

Discussion on limiting shared credentials and accounts

Minor corrections

DRAFT WISE Baseline AUP v1.0 – (1)

Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use (“AUP”) defines the rules that govern your access to and use (including transmission, processing, and storage of data) of the resources and services (the “Services”) as granted by {community, and/or the agency, or infrastructure name} (the "Granting Authority"). The goal of the Granting Authority is to {describe here the objectives of the Granting Authority}.

<This document may be augmented by additional agreements or terms and conditions, in which case the granting authority may optionally add specific clauses - or references thereto - here that are not in conflict with the clauses below and that further define and limit what constitutes acceptable use. The wording of the following clauses must not be changed.>

1. You shall only use the Services in a fashion consistent with the stated goals and policies of the Granting Authority.
2. You shall not use the Services for any purpose that is unlawful and you shall not breach, attempt to breach, nor 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)~~ and nN~~o intentional sharing of user credentials is permitted.not share your account or credentials with anyone or use a shared account to log in.
5. You shall keep all your registered information correct and up to date.

DRAFT WISE Baseline AUP v1.0 – (2)

6. You shall immediately report any known or suspected security breach, 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~~the~~ applicable service level agreements listed below. Use without such agreements is at your own risk.

8. The Granting Authority and the provider of the Services process your personal data in accordance with their ~~privacy policies~~Privacy Notices listed below.

9. The Granting Authority or the provider of the Services may, for administrative, operational, or security reasons, restrict or suspend your use without prior notice and without compensation, within their domain of authority, and you shall immediately comply with their instructions regarding your use of the Services.

10. If you violate these rules, you are liable for the consequences, which may include but are not limited to a report being made to your home organisation and, if the activities are thought to be illegal, to appropriate law enforcement agencies.

The administrative contact for this AUP is: {email address for the Granting Authority}

The security contact for this AUP is: {email address for the infrastructure, community, and/or Granting Authority security contact}

The privacy policies are located at: {URL}

Applicable service level agreements are located at: <URLs>

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).