Implementers Guide to the WISE Baseline Acceptable Use Policy

Publication Date 2019-02-26
Authors: David Groep;Ian Neilson;WISE SCI Working Group members

Document Code: AARC-I044
DOI:

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract
Applying the Baseline AUP to concrete use cases may appear straightforward, but there are many edge cases and specific circumstances where it is not entirely obvious how to both achieve the aim of user-friendliness as well as be complete and practical. In this write-up, we try to give hints how to use the WISE Baseline AUP in practice in both community-first as well as 'user-first' membership management services

Table of Contents

1. Aims of the Baseline AUP

Acceptable use policy (AUP) and terms and conditions are necessary instruments in the regulation of infrastructure access. They bind the user to the 'purpose' for which the services and resources they use have been provided. Yet, like with privacy notices, the reader is rather inclined to click through and proceed with the actual task at hand. Thus, to reduce the burden on the user and increase the likelihood that they will read the AUP, the number of times a user is presented with such notices must be kept to a minimum, preferably just a single time. Yet the notice should cover as much of the user's potential use of the infrastructure as possible: the more services and resources deem an AUP as sufficient for their policy purposes, the better it will be. This will allow users to use resources from multiple service and resource providers without the need to confirm acceptance of additional AUPs.

The aim of the WISE Baseline AUP is to

- provide a common baseline set of criteria for acceptable use and terms and conditions for the professional use of IT infrastructures for research globally – and thereby ease the trust of users across infrastructures: services within an infrastructure have a common framework describing the behaviour of users coming from multiple communities;
- facilitate a presentation format that allows necessary privacy notices (in Europe for GDPR compliance) to be presented at the same time and remain easily available thereafter;
- support services with varying levels of support and quality guarantees;
- provide for augmentation of the baseline AUP with community and infrastructure-specific terms and conditions
- be applicable to both 'community-first' and 'user-first' AAI membership management services.
  In the conventional 'community-first' model, the AUP is shown to the user when registering with their research community. The model here referred to as 'user-first' presumes that the user first enrols in a generic, potentially multi-tenancy, membership management service (MMS), and within that service petitions membership to one or more of the research communities hosted within the MMS.

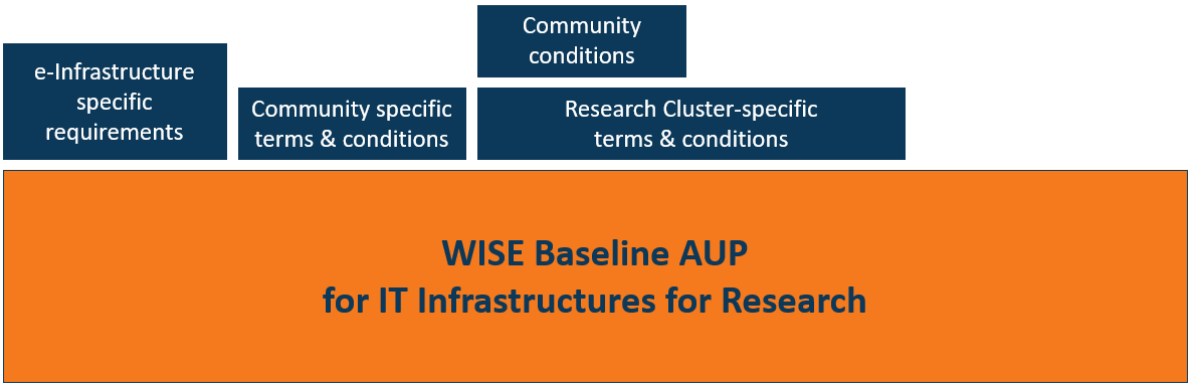
The AUP should preferably be presented only once, and then preferably during the first interaction of the applicant (potential user) with the Infrastructure. As such, the *membership management service* (MMS) is the most appropriate component to present and manage AUP acceptance.

2. A scalable model with shared language

Typical AUPs vary considerably between organisations, service providers, and infrastructures, even though the AUP Alignment Study identified a few main 'strands' of textual history common to multiple infrastructures. Having textual variations complicates comparison of AUPs and makes infrastructures and service providers feel the need to (at least) also present 'their own' AUP on first access to the service. For a Baseline AUP it is therefore critical that the basic AUP requirements are both common as well as immutable. Specific service providers and infrastructures may augment the AUP with domain- or service-specific clauses, but should present the Baseline AUP 'as is' without modifications. Only in this way can a policy mapping exercise, repeated user interaction, and a multitude of interstitial pages be avoided.

The WISE AUP model uses a layered approach to AUP composition:

- the Baseline AUP is a set of ten 'commandments' that are identical and equally applicable to all services and infrastructures
- the body or bodies that are authoritative to grant access (the community, infrastructure, etc.), as well as the purpose binding of the user's activities are templated explicitly in the preamble
- the AUP provides a place for optional additional agreements or terms and conditions, that augment (but not replace or contradict) the Baseline AUP commandments. For communities 'hosted within' one or more infrastructures, such additional agreements can be combined (stacked) and presented once, and together.



A logical view of how the baseline AUP can be augmented with more-specific terms and conditions is shown in the viewgraph above. Examples of such augmented terms include the requirement to recognise (cite, acknowledge) contributing infrastructures and service providers, or a condition that no attempts may be made to reverse pseudonymisation techniques that have been applied to protect sensitive data to which the user may gain access.

3. The WISE Baseline AUP

The WISE Baseline AUP[1], with its preamble and final clause placeholders, is given below. The blue text elements should be substituted in-line, whereas 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 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>

[1] This Baseline AUP is published by the WISE Information Security for e-Infrastructures SCI working Group, see https://wise-community.org/sci/ for the authoritative text. Text available under a CC-BY-NC-SA license from the Members of the WISE Community SCI Working Group.

4. AUP and supplementary user notices

In addition to the AUP base clauses and information discussed above, the template provides for other information that should be presented to the user during registration -

1. links to applicable GDPR, or other “Privacy Notices” for the AAI, infrastructures, proxies, and services connected to it;
2. links to items that supplement acceptable use, such as service level agreements and other rights and privileges the user may enjoy when using the service;
3. contact information for both administrative and security contacts to enable the user to question the AUP or report security breaches as requested in item #6. Of course, such contacts can be shared by many communities, or can be provided as a service to communities by Infrastructures that operate an AAI on behalf of such a community.

5. Application to community-first membership management services

The way in which a community (or other body) that has its own ‘AAI entry point’ can use the Baseline AUP model is straightforward. The community, when establishing itself, will identify the (existing or new) name of their collaboration and define a one-sentence *purpose* for which services will be used (typically, the aim or mission statement of the collaboration, community, or organisation). Any ancillary clauses that augment the Baseline AUP are also identified, alongside the responsible administrative and security contacts, the URL for the privacy notice, and any agreements that the community has in place with Service providers or infrastructures.

For presenting the AUP, it does not matter whether the community operates the MMS by itself, or whether it has outsourced its operation to a third party (a dedicated service provider, an infrastructure, or infrastructure consortium). The community remains the single ‘logical’ entry point into the AAI ecosystem. Any services ‘below’ the community AAI will be accessed via the community proxy, or by using community user identifiers, or by means of and on behalf of the community. Since users access services based on their community membership, they will all have seen and accepted the AUP when presented by the Community MMS.

It is up to the community management to ease the user’s workflow by collating the necessary documents: the list of Privacy Notices (for the MMS itself, but also for the connected services. If a community connects a new service or e-Infrastructure to its AAI, it shall record and post the Privacy Notice of such Service or infrastructure on the Community Privacy Notice page.

Similarly, if the community has agreed specific service levels with one or more service providers, it should maintain a list of such additional agreements so that their users will be

able to be informed of - and thus better enjoy - the service the community has negotiated for them.

5.1. Implementation suggestions

Some of the 'information' pages that the community AAI (or its MMS) has to maintain can be automatically generated. For example, each independent service provider already has to declare and publish its own privacy notice. Service meta-data often contains a reference to such a privacy notice, and, based on the meta-data of the list of connected services, the Privacy Notice overview page can be automatically populated. Users may (when deemed necessary) even be automatically informed of changes to this page for services the user has previously used.

5.2. Example

The following example shows a conventional community (the 3He SRC Collaboration) and the appropriate Acceptable Use Policy presented on enrolment

> 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 ("Services") as granted by **the EMIN group** for 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**

6. Application to user-first membership management services

Multi-tenant MMSs – services that support more than one community, agency, or infrastructure – may be designed such that the applicant first becomes a user of the MMS itself, and within that context can join one or more communities (virtual or collaborative organisations). This is especially prevalent if the MMS is designed to support a large number of small, lightweight collaborations. For the purpose of this document, we will refer to such MMSs as 'user-first' (since the MMS enrolment flow is centred on the user, not the community).

This leads to potential confusion in drafting the AUP that is presented by the MMS to the user on initial enrolment. At enrolment time, the only thing known to the MMS is the intent of the user to join the MMS. It cannot at that point infer subsequent enrolment in a community or VO, and thus cannot present the name of the community (or agency or infrastructure), nor the purpose statement for the community (or communities!) the user may ultimately join.

Since the purpose binding cannot be presented during the enrolment step, it is indeed unavoidable to show the user the purpose for which Services available to the community (VO) may be used. This, however, does not present a significant user interface barrier, since the user in any case has to be presented with an enrolment flow (petition, confirmation) page once they express the intent to join such a community.

Similarly, the ad-hoc creation of communities on a multi-tenant MMS does not pose issues per se. In fact, the creation of a new community provides the most appropriate interaction point at which to collect, from the new community manager (by definition the user who creates the community), the necessary information for a community to subsequently present to its users in the AUP.

The premise remains that the Baseline AUP commandments are immutable. What needs careful phrasing are the definition of the Granting Authority, the purpose, and the augmented terms and conditions.

The term *Services* should be construed in its broadest meaning, and which *Services* are part of the suite to which the user has access will vary over time. During enrolment, there may be just a single service (the MMS), under authority of its own operator. When joining a community or VO on the platform, the MMS will *in addition* be a Service also of the community, and the community (during its creation) will have (implicitly) linked the MMS as one of its services. This dual 'role' of the MMS thereby resolves the apparent conflict of priority between the hosting infrastructure (during initial enrolment) and the community (once a user has joined such).

6.1. Enrolment in the MMS

During the MMS enrolment phase, the body granting an applicant user access to the MMS (at that point the only infrastructure or organisation involved) is still the operator of the multi-tenant MMS, e.g. the generic e-Infrastructure or service provider running the service itself. The purpose for which an applicant registered with and starts using the MMS is also clear. It's *for the purpose of participating in activities of research and educational collaborations ("Collaborations"), which are represented in the Service as "Virtual Organizations"*.

The following example shows a multi-tenancy MMS (operated by OneRing GmbH) and the appropriate Acceptable Use Policy presented on enrolment of a new user on the platform:

> 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 ("Services") as granted by **OneRing** for the purpose of **participating in activities of research and educational collaborations ("Collaborations"), which are represented in the Service as "Virtual Organizations"**.
>
> *... Augmented Terms and Conditions and Baseline AUP Commandments follow ...*

At this time, the *Privacy Notice* will refer to only that of the MMS operator, and the same follows for the administrative and security contacts, as well as any service level description if there is one.

However, in its simple form above it will not be clear for the user that the *Baseline commandments* will also in the future apply to any Services (sources, infrastructures) to which the user may gain access by virtue of being a member of a Virtual Organisation. This is a place where the multi-tenant MMS service may be of significant help to the communities hosted within it: making such transitive applicability explicit through augmented terms and conditions shown already at this time during enrolment.

The following example shows an example of *augmented terms* that OneRing GmbH shows users of the platform to elucidate that its tenants (virtual organisations) are the one that control access to connected services:

> ...
> *The MMS Service may be used to facilitate access to services and resources ("Connected Services") , which are provided by other organizations and/or OneRing to members of Virtual Organizations ("Connected Services") and which are provided by other organizations and/or OneRing.*
>
> *Access granted by OneRing to the MMS Service does not imply that access to Connected Services is granted.*
>
> *Access to Connected Services available to a Virtual Organization is granted to members of that Virtual Organization by the owner(s) of the Virtual Organization. Users of the Service can be members of more than one Virtual Organizations hosted on the Service..*
>
> *The Baseline clauses of this AUP apply equally to both the MMS service as well as to all Connected Services, from now on collectively referred to as "Services", as augmented by any specific terms to which adherence will be required during enrolment in any Virtual Organisation.*

Having shown this 'decorated' AUP for the MMS on enrolment, any Services that either the operator of the MMS or the VOs will connect to the platform can rely on the fact that the Baseline AUP commandments have all been shown to the user. If these requirements are sufficient for service use, there is no need to present these again to the user on joining a community and require their confirmation of acceptance. However, the *purpose binding* of the AUP for the community has not yet been taken care of. We must ascertain that users will be permitted to use the Services to which the community (VO) gives them access are used in a way compatible with the purpose for the VO has granted access.

This purpose binding should be done *when the user petitions access to a VO*. It can be in the form of a (either pre-checked or explicit) tick box on the (electronic) VO enrolment form, which has to be shown to the user anyway (even if it is just a simple confirmation dialogue box). All relevant information (name of the VO, VO manager, and *purpose* of the VO) is available in the MMS platform and it can be used to construct the confirmation dialogue box.

Some of the information that has to be presented to users that petition access to a VO must be provided by the (hosted) VO. This is information that is customarily already collected:

- VO name (should become the community unless stated otherwise)
- VO description (should become the purpose of the VO unless stated otherwise)

A form for petitioning access to a VO could take the following form:

Name:	Pietje Puk
Email:	nobody@example.org
Affiliation:	Affiliate
[X]	I shall use the resources and services of ***VO_NAME*** for the purpose of ***VO_DESCRIPTION***
	[DECLINE] [CONFIRM]

Thus collecting the VO Name and the VO Description needs to be done during the VO creation process, and community creation templates should be built to allow collection of this information (although this is likely already done).

Specific care has to be taken for *auto approval* workflows. Since in such cases no interstitial confirmation screen is presented, it is impossible to inform the applicant of the purpose-binding of the VO. Therefore, auto-approval flows should be limited to those VOs that only connect Services owned and operated by or on behalf of the MMS operator itself.

For *invitation-based* enrolment, the requisite purpose binding can be shown on the enrolment confirmation page.

6.2. Supporting management of services by hosted VOs by way of the MMS

Several MMS platforms allow a community (VO) to *attach* services to a VO. The set of *connected services* may vary between VOs and will usually include services that are offered by third parties, i.e., other providers than that of the MMS service. Services may be connected to one or several VOs on the same platform, and will be accessible to users only by virtue of their VO membership.

Such connected services will each come with their own (“GDPR”) Privacy Notice, and *may* come with additional terms and conditions that augment the Baseline AUP. The MMS platform can provide significant help to the VOs they host by automating and specializing the Privacy Notices and AUPs on a per-user basis.

The MMS platform should

- collect a link to the privacy notice for each service they connect to the platform. Privacy notices may be shared, but each service should have one
- allow services to provide and manage service specific terms and conditions
- allow services to provide and manage (a link to) default service level descriptions
- collect from each service an administrative and security contact

Since the MMS has knowledge about the VOs of which a user is a member, and of the services available to each VO, it can automatically construct (per-user) pages that implement the links listed at the bottom of the Baseline AUP. This greatly facilitates its presentation, provides ease of use for the users of the MMS, and implements the requirement to be able to consult the (combined) Privacy Notices for the user at any time.

Example of a 'dynamic' AUP at
https://mms.onering.nu/my/aup?uid=5efefe18-c07a-461c-b718-17ccf349aef1

This Acceptable Use Policy and Conditions of Use ("AUP") defines …
… Baseline AUP commandments follow …

The administrative contact for this AUP is:
guru@onering.nu (MMS); voadm-alias@he3epp.org (VO: the EMIN group)
The security contact for this AUP is:
wraith@onering.nu (MMS); security@nikhef.nl (VO: the EMIN group)
The privacy statements are located at:
https://mms.onering.nu/my/privacy?uid=5efefe18-c07a-461c-b718-17ccf349aef1
Applicable service level agreements are located at:
https://mms.onering.nu/my/slds?uid=5efefe18-c07a-461c-b718-17ccf349aef1

And the page to which the Privacy statement URL given above could lead might look like this:

Privacy Statement for ***User Name***

You are a user of the membership management service of OneRing GmbH and have also joined 1 virtual organisation on this platform, whose service providers are independent controllers.

OneRing GmbH will process your personal data in accordance with its own privacy policy provided at https://onering.nu/privacy

For the VO "**the EMIN group**", its service providers process personal data according to their policies listed:

- Service Provider **Vrije Universiteit Amsterdam** at **https://www.vu.nl/nl/privacy-statement.aspx**
- Service Provider **Nikhef** at **https://www.nikhef.nl/privacy**
- Service Provider **ISS** at **http://home.infn.it/it/?id=268&Itemid=427**
- Service Provider **University of Glasgow** at **https://www.gla.ac.uk/legal/privacy/**
- …

As VO membership on the platform changes, and as VOs connect and disconnect Services on the platform, the Privacy Notices, contact addresses (and any service level descriptions) will then adjust automatically.

6.3. Supplementary terms and conditions for hosted VOs

A mechanism similar to the Privacy Notice generation can also be applied for VOs that have their own supplementary terms and conditions, as well as any augmented AUP terms that are the result of a VO connecting *services* that themselves have such additional statements.

Where possible, it should be the VO that presents *all supplementary terms and conditions* on behalf of *all its connected services*. This ensures that they are worded in a way that the user understands, and that makes sense in the context of the VO. Agreeing such terms and conditions should be done by the VO manager when connecting services.

It should be recognised that there might be cases in which the VO (or its technical administrators) do not have sufficient background regarding the service that will allow them to properly present these terms. For non-interactive workflows, every effort should be made to collect this information from Services that need to present additional terms and conditions: the user will have no other means to be informed about them. For interactive (web-based) services, one may resort to presenting them on first access to such a service.

Alternative approaches, such as those based on automatic collection of service-specific terms and presenting them (in a potentially automated way) akin to the *Privacy Notice* collection described above, is likely to pose issues: in particular the long collection of conditions that may result will even further deter the user from reading the AUP and Conditions of Use. Although technically possible, it defeats the aim of the WISE Baseline AUP of making the AUP presentable to users.

Generic e-Infrastructures, for at least their ‘common’ services, should endeavour to rely on the Baseline terms only, in line with the WISE community *Security for Collaborating Infrastructures Trust Framework* (SCI), and not augment these terms.

VOs with supplementary terms should register these terms in the MMS (alongside the VO description), and the MMS must present these terms during the enrolment flow – extending the purpose binding discussed previously. User confirmation in these cases should most likely be an explicit, positive action (active checking of the box).

A VO whose research work includes the processing of sensitive data could add these terms like this:

Name: **Pietje Puk** Email: **nobody@example.org** Affiliation: **Affiliate**

[X] I shall use the resources and services of ***VO_NAME*** for the purpose of ***VO_DESCRIPTION***

[ ] I agree to the following additional terms and conditions for the use of services to which VO_NAME may grant access:

** You shall provide appropriate acknowledgement of support for your use of the resources/services provided by adding*
"This work has been supported by VO_NAME, which is co-funded by The Agency"

** You will avoid any attempts to reverse privacy enhancing technologies (i.e., pseudonymization, anonymization) applied to the data and/or to (re-) identify individual natural persons (such as patients or donors who have consented to and contributed her/his data or biological material to be used in research) contributing the data and/or donating the biological material.*

[DECLINE] [CONFIRM]

Here, the user agrees to the purpose of the VO (which is implicitly true since the petition flow was initiated by the applicant), but the compliance with the additional terms and conditions has to be explicitly approved (the box starts in an un-checked state) to get positive agreement from the applicant.

References

WISE https://www.wise-community.org/
Baseline AUP https://www.wise-community.org/sci/