# Example of a standard attribute filter for Shibboleth IdP v4 and above

This is an example of a standard entity category based attribute filter for SWAMID 2.0 in a Shibboleth IdP which fulfils SWAMID's Entity Category attribute release in SWAMID

The latest published SWAMID example standard filter for Shibboleth Identity Provider 4 is published at https://mds.swamid.se/entity-configurations/Shibboleth-IdP/v4/attribute-filter.xml. Below is the latest version included from the publication repository.

```
<?xml version="1.0" encoding="UTF-8"?>

<AttributeFilterPolicyGroup id="ShibbolethFilterPolicy"
    xmlns="urn:mace:shibboleth:2.0:afp"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:mace:shibboleth:2.0:afp
http://shibboleth.net/schema/idp/shibboleth-afp.xsd">

    <!-- REFEDS Anonymous Authorization Entity Category -->
    <AttributeFilterPolicy id="releaseToRefedsAnonymous">
        <PolicyRequirementRule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-
category" attributeValue="https://refeds.org/category/anonymous" />
        <AttributeRule attributeID="eduPersonScopedAffiliation">
            <PermitValueRule xsi:type="ANY"/>
        </AttributeRule>
        <AttributeRule attributeID="schacHomeOrganization">
            <PermitValueRule xsi:type="ANY"/>
        </AttributeRule>
    </AttributeFilterPolicy>

    <!-- REFEDS Pseudonymous Authorization Entity Category -->
    <!-- Supports data minimalisation to prevent use together with anonymous -->
    <AttributeFilterPolicy id="releaseToRefedsPseudonymous">
        <PolicyRequirementRule xsi:type="AND">
            <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category"
attributeValue="https://refeds.org/category/pseudonymous" />
            <Rule xsi:type="NOT">
                <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category"
attributeValue="https://refeds.org/category/anonymous" />
            </Rule>
        </PolicyRequirementRule>
        <AttributeRule attributeID="samlPairwiseID">
            <PermitValueRule xsi:type="ANY"/>
        </AttributeRule>
        <AttributeRule attributeID="eduPersonScopedAffiliation">
            <PermitValueRule xsi:type="ANY"/>
        </AttributeRule>
        <AttributeRule attributeID="schacHomeOrganization">
            <PermitValueRule xsi:type="ANY"/>
        </AttributeRule>
        <AttributeRule attributeID="eduPersonAssurance">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
    </AttributeFilterPolicy>

    <!-- REFEDS Personalized Access Entity Category  -->
    <!-- Supports data minimalisation to prevent use together with anonymous and pseudonymous-->
    <AttributeFilterPolicy id="releaseToRefedsPersonalized">
        <PolicyRequirementRule xsi:type="AND">
            <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category"
attributeValue="https://refeds.org/category/personalized" />
            <Rule xsi:type="NOT">
                <Rule xsi:type="OR">
                    <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-
category" attributeValue="https://refeds.org/category/anonymous" />
                    <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-
category" attributeValue="https://refeds.org/category/pseudonymous" />
                </Rule>
            </Rule>
```

```
        </PolicyRequirementRule>
        <AttributeRule attributeID="samlSubjectID">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="displayName">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="givenName">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="sn">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="mail">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="eduPersonAssurance">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="schacHomeOrganization">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="eduPersonScopedAffiliation">
            <PermitValueRule xsi:type="OR">
                <Rule xsi:type="Value" value="faculty" caseSensitive="false" />
                <Rule xsi:type="Value" value="student" caseSensitive="false"/>
                <Rule xsi:type="Value" value="staff" caseSensitive="false"/>
                <Rule xsi:type="Value" value="alum" caseSensitive="false"/>
                <Rule xsi:type="Value" value="member" caseSensitive="false"/>
                <Rule xsi:type="Value" value="affiliate" caseSensitive="false"/>
                <Rule xsi:type="Value" value="employee" caseSensitive="false"/>
                <Rule xsi:type="Value" value="library-walk-in" caseSensitive="false"/>
            </PermitValueRule>
        </AttributeRule>
    </AttributeFilterPolicy>

    <!-- Rule to honour Subject ID requirement tag in metadata. Used in combination with Geant/Refeds Code of
Conduct v* -->
    <!-- Code of Conduct can be combined with other entity categories -->
    <!-- Supports data minimalisation to prevent subject-id and pairwise-id being released together -->
    <AttributeFilterPolicy id="subject-identifiers">
        <PolicyRequirementRule xsi:type="OR">
            <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category"
attributeValue="http://www.geant.net/uri/dataprotection-code-of-conduct/v1" />
            <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category"
attributeValue="https://refeds.org/category/code-of-conduct/v2" />
        </PolicyRequirementRule>
        <AttributeRule attributeID="samlPairwiseID">
            <PermitValueRule xsi:type="AND">
                <Rule xsi:type="NOT">
                    <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-
category" attributeValue="https://refeds.org/category/personalized" />
                </Rule>
                <Rule xsi:type="OR">
                    <Rule xsi:type="EntityAttributeExactMatch" attributeName="urn:oasis:names:tc:SAML:profiles:
subject-id:req" attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" attributeValue="pairwise-
id" />
                    <Rule xsi:type="EntityAttributeExactMatch" attributeName="urn:oasis:names:tc:SAML:profiles:
subject-id:req" attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" attributeValue="any" />
                </Rule>
            </PermitValueRule>
        </AttributeRule>
        <AttributeRule attributeID="samlSubjectID">
            <PermitValueRule xsi:type="AND">
                <Rule xsi:type="NOT">
                    <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-
category" attributeValue="https://refeds.org/category/pseudonymous" />
                </Rule>
                <Rule xsi:type="EntityAttributeExactMatch" attributeName="urn:oasis:names:tc:SAML:profiles:
subject-id:req" attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" attributeValue="subject-
id" />
```

```
            </PermitValueRule>
        </AttributeRule>
    </AttributeFilterPolicy>

    <!-- GEANT Data protection Code of Conduct or REFEDS Data Protection Code of Conduct Entity Category -->
    <AttributeFilterPolicy id="releaseToCodeOfConduct">
        <PolicyRequirementRule xsi:type="OR">
            <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category"
attributeValue="http://www.geant.net/uri/dataprotection-code-of-conduct/v1" />
            <Rule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category"
attributeValue="https://refeds.org/category/code-of-conduct/v2" />
        </PolicyRequirementRule>
        <AttributeRule attributeID="eduPersonTargetedID">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="eduPersonPrincipalName">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="eduPersonOrcid">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="norEduPersonNIN">
            <PermitValueRule xsi:type="AND">
                <Rule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
                <Rule xsi:type="RegistrationAuthority" registrars="http://www.swamid.se/" />
            </PermitValueRule>
        </AttributeRule>
        <AttributeRule attributeID="personalIdentityNumber">
            <PermitValueRule xsi:type="AND">
                <Rule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
                <Rule xsi:type="RegistrationAuthority" registrars="http://www.swamid.se/" />
            </PermitValueRule>
        </AttributeRule>
        <AttributeRule attributeID="schacDateOfBirth">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="mail">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="mailLocalAddress">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="cn">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="displayName">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="givenName">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="sn">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="eduPersonAssurance">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="eduPersonScopedAffiliation">
            <PermitValueRule xsi:type="AND">
                <Rule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
                <Rule xsi:type="OR">
                    <Rule xsi:type="Value" value="faculty" caseSensitive="false" />
                    <Rule xsi:type="Value" value="student" caseSensitive="false" />
                    <Rule xsi:type="Value" value="staff" caseSensitive="false" />
                    <Rule xsi:type="Value" value="alum" caseSensitive="false" />
                    <Rule xsi:type="Value" value="member" caseSensitive="false" />
                    <Rule xsi:type="Value" value="affiliate" caseSensitive="false" />
                    <Rule xsi:type="Value" value="employee" caseSensitive="false" />
                    <Rule xsi:type="Value" value="library-walk-in" caseSensitive="false" />
                </Rule>
            </PermitValueRule>
```

```
        </AttributeRule>
        <AttributeRule attributeID="eduPersonAffiliation">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="o">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="norEduOrgAcronym">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="c">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="co">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="schacHomeOrganization">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
        <AttributeRule attributeID="schacHomeOrganizationType">
            <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        </AttributeRule>
    </AttributeFilterPolicy>

    <!-- REFEDS Research and Scholarship Entity Category -->
    <AttributeFilterPolicy id="releaseToRefedsResearchAndScholarship">
        <PolicyRequirementRule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-
category" attributeValue="http://refeds.org/category/research-and-scholarship" />
        <AttributeRule attributeID="eduPersonTargetedID">
            <PermitValueRule xsi:type="NOT">
                <Rule xsi:type="Value" value="https://refeds.org/assurance/ID/eppn-unique-no-reassign"
attributeID="eduPersonAssurance" />
            </PermitValueRule>
        </AttributeRule>
        <AttributeRule attributeID="displayName">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="givenName">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="sn">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="mail">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="eduPersonAssurance">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="eduPersonPrincipalName">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="eduPersonScopedAffiliation">
            <PermitValueRule xsi:type="OR">
                <Rule xsi:type="Value" value="faculty" caseSensitive="false" />
                <Rule xsi:type="Value" value="student" caseSensitive="false" />
                <Rule xsi:type="Value" value="staff" caseSensitive="false" />
                <Rule xsi:type="Value" value="alum" caseSensitive="false" />
                <Rule xsi:type="Value" value="member" caseSensitive="false" />
                <Rule xsi:type="Value" value="affiliate" caseSensitive="false" />
                <Rule xsi:type="Value" value="employee" caseSensitive="false" />
                <Rule xsi:type="Value" value="library-walk-in" caseSensitive="false" />
            </PermitValueRule>
        </AttributeRule>
    </AttributeFilterPolicy>

    <!-- ESI European Student Identifier -->
    <AttributeFilterPolicy id="entity-category-european-student-identifier">
        <PolicyRequirementRule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-
category" attributeValue="https://myacademicid.org/entity-categories/esi" />
        <AttributeRule attributeID="schacPersonalUniqueCode">
```

```
            <PermitValueRule xsi:type="ValueRegex" regex="^urn:schac:personalUniqueCode:int:esi:.*" />
        </AttributeRule>
    </AttributeFilterPolicy>

    <!-- Sectigo -->
    <AttributeFilterPolicy id="releaseSectigoAttributeBundle">
        <PolicyRequirementRule xsi:type="Requester" value="https://cert-manager.com/shibboleth" />
        <AttributeRule attributeID="eduPersonPrincipalName">
            <PermitValueRule xsi:type="ANY"/>
        </AttributeRule>
        <AttributeRule attributeID="displayName">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="givenName">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="mail">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
        <AttributeRule attributeID="sn">
            <PermitValueRule xsi:type="ANY"/>
        </AttributeRule>
        <AttributeRule attributeID="schacHomeOrganization">
            <PermitValueRule xsi:type="ANY"/>
        </AttributeRule>
        <AttributeRule attributeID="tcsPersonalEntitlement">
            <PermitValueRule xsi:type="ANY"/>
        </AttributeRule>
   </AttributeFilterPolicy>

 <!-- PLACEHOLDER DO NOT REMOVE -->
</AttributeFilterPolicyGroup>
```