IAMO Shibboleth Attribute Release
Memorandum of Understanding

Between the designated Purdue University administrative or educational group, called the “Client”, and the Department of Human Resource Services and/or the Office of the Registrar, for the electronic distribution of Purdue University attribute data to the Client for purposes of federated authentication and authorization using Shibboleth.

I. PARTIES
This document constitutes an agreement between the designated Purdue University administrative or educational group, called the Client, and the Department of Human Resource Services and/or the Office of the Registrar. The Identity and Access Management Office (IAMO), a unit of the Networks and Security Division in the Office of the Vice President for Information Technology, is an advisor to Human Resource Services and/or the Office of the Registrar for this agreement.

II. PURPOSE
A. Background and Goals
The purpose of this Memorandum of Understanding (MOU) is to define the practices, guidelines, approvals, security and specific University attribute data to be released from Human Resource Services and/or the Office of the Registrar via IAMO to the Client.

B. Definitions and Principles
1) For the purposes of this document, Purdue University includes, but is not limited to, the West Lafayette Campus, other Purdue campuses including Statewide Technology, Continuing Education, and other Purdue stakeholders.
2) The Department of Human Resource Services is the steward of Purdue University personnel data, via the human resource data steward. Human Resource Services rules for use of the attribute data take precedence over IAMO and Client requirements.
3) The Office of the Registrar is the steward of Purdue University student data, via the student services data steward. Office of the Registrar rules for use of the attribute data take precedence over IAMO and Client requirements.
4) Approved Clients are Purdue University administrative and educational groups for whom the use of University attribute data are necessary for conducting official business, or to support distributed operations, for the purpose of authentication and authorization.
5) A Client requesting attributes must sign this Memorandum of Understanding with Human Resource Services and/or the Office of the Registrar, and the signed MOU must be reviewed by and made available to IAMO before attributes can be released.
6) Best security practices will be used to transfer attributes and to administer the systems to which attributes are transferred, including IAMO and Client systems.
7) The Client receiving University attributes will hold those attributes in strict confidence according to best security practices and current regulations, and will
use attribute information only for the purpose defined in this agreement and will not redistribute it to another party.

8) When policy changes are required, the Client, Human Resource Services, and/or the Office of the Registrar, with Iamo advice, will cooperate in their development.

III. RESPONSIBILITIES

The Purdue University Department of Human Resource Services and/or the Office of the Registrar will:
- Provide accurate and complete descriptions of the data delivered to Iamo and the Client.
- Consult with Iamo about the provisions of this MOU and forward a signed copy of this MOU to Iamo for execution.
- Provide University data for attribute release to Iamo on a regular basis and in a secure fashion.
- Advise the Iamo of changes in data format and content.
- Make prompt and timely changes to errors in data reported by the Client to the Iamo.

The Client will:
- Agree to a specific set of data items to be released as attributes by Iamo.
- Agree to an initial and subsequent regular security audits of the receiving Client system.
- Agree to provide the secure attribute data transfer mechanism defined by Iamo.
- Agree to hold the received attribute data in strict confidentiality and abide by current regulations.
- Agree to use the attribute data only for the purposes defined in this agreement.
- The Client must execute a new agreement to define new uses of the attribute data.
- Agree not to redistribute the received attribute data to any third party.
- Provide information to Human Resource Services and/or the Office of the Registrar and Iamo on use, protection, and release of University attribute data, as requested.
- Report errors in received attributes to the Iamo.

The Identity and Access Management Office will:
- Receive the signed Client MOU from Human Resource Services and/or the Office of the Registrar and arrange for the secure release of University attributes to the Client system;
- Audit Client systems before initiating attribute data release to insure their system security; and audit them subsequently on a regular basis to insure continued security;
- Describe and release approved attribute data to the Client system in a secure fashion, and monitor attribute release to the Client destination system to insure their correct and secure delivery;
- Notify Human Resource Services and/or the Office of the Registrar of errors in the data and request prompt and timely corrections;
When requested, provide reports to Human Resource Services and/or the Office of the Registrar on attributes that have been released.
IV. **TERMINATION**

This agreement terminates automatically upon termination of the University data distribution (agreement) between Human Resource Services and/or the Office of the Registrar, and IAMO.

This agreement may also be terminated ninety (90) days after either party presents a written notice of termination, signed by the school or department representative who authorized this agreement.

V. **PENALTIES**

Violation of this agreement will be adjudicated by the Executive Director of Networks and Security, the Director of Human Resource Services and/or the Registrar from the Office of the Registrar.

Violation may result in temporary or permanent suspension of the release of University attributes from the IAMO to the client.
VI. CLIENT AUTHENTICATION/AUTHORIZATION REQUIREMENTS

1) For the purposes of effecting this agreement, these specific Client definitions are in force:

Client Contact Information
- Client Area Name: __________________________________________
- Client Department or School: _________________________________
- Client Department or School Head: ___________________________
- Client Technical Contact Name: ______________________________
- Client Technical Contact Campus Email Address: _______________
- Client Technical Contact Campus Telephone Number: ____________

Federated Application and Use Definition (list for each application/use):
- Name of Application: _______________________________________
- Application/Use Description: _________________________________
  ___________________________________________________________
  ___________________________________________________________
  ___________________________________________________________
- Vendor Name _______________________________________________
- InCommon Member: □ Yes □ No
- Service Provider Metadata URL: _______________________________
- Service Provider Entity-ID: _________________________________
Requested Attributes to be Released:

<table>
<thead>
<tr>
<th>Request Y/N</th>
<th>Attribute</th>
<th>SAML 1 Name</th>
<th>SAML 2 Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>uid</td>
<td>urn:mace:dir:attribute-def:uid</td>
<td>urn:oid:0.9.2342.19200300.100.1.1</td>
</tr>
<tr>
<td></td>
<td>mail</td>
<td>urn:mace:dir:attribute-def:mail</td>
<td>urn:oid:0.9.2342.19200300.100.1.3</td>
</tr>
<tr>
<td></td>
<td>displayName</td>
<td>urn:mace:dir:attribute-def:displayName</td>
<td>urn:oid:2.16.840.1.113730.3.1.241</td>
</tr>
<tr>
<td></td>
<td>cn</td>
<td>urn:mace:dir:attribute-def:cn</td>
<td>urn:oid:2.5.4.3</td>
</tr>
<tr>
<td></td>
<td>sn</td>
<td>urn:mace:dir:attribute-def:sn</td>
<td>urn:oid:2.5.4.4</td>
</tr>
<tr>
<td></td>
<td>givenName</td>
<td>urn:mace:dir:attribute-def:givenName</td>
<td>urn:oid:2.5.4.42</td>
</tr>
<tr>
<td></td>
<td>employeeNumber</td>
<td>urn:mace:dir:attribute-def:employeeNumber</td>
<td>urn:oid:2.16.840.1.113730.3.1.3</td>
</tr>
<tr>
<td></td>
<td>employeeType</td>
<td>urn:mace:dir:attribute-def:employeeType</td>
<td>urn:oid:2.16.840.1.113730.3.1.4</td>
</tr>
<tr>
<td></td>
<td>eduPersonPrincipalName (ePPN)</td>
<td>urn:mace:dir:attribute-def:eduPersonPrincipalName</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.1.1.6</td>
</tr>
<tr>
<td></td>
<td>eduPersonScopedAffiliation</td>
<td>urn:mace:dir:attribute-def:eduPersonScopedAffiliation</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.1.1.9</td>
</tr>
<tr>
<td>Y</td>
<td>eduPersonTargetedID</td>
<td>urn:mace:dir:attribute-def:eduPersonTargetedID</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.1.1.10</td>
</tr>
<tr>
<td></td>
<td>eduCourseOffering</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.6.1.1</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.6.1.1</td>
</tr>
</tbody>
</table>

The eduPersonTargetedID attribute is included by default. Attribute descriptions are available at: https://www.purdue.edu/apps/account/docs/Shibboleth/Shibboleth_information.jsp
Print Name:___________________________________
Client Director or Department Head
Signed:_______________________________ Date: ______________

Please forward in campus mail to the Director of the Identity and Access Management Office for further processing: IAMO Director / ITNS / ROSS.

Print Name:___________________________________
Human Resource Services Data Steward
Signed: ________________________________ Date: ______________

Print Name:___________________________________
Student Services Data Steward
Signed: ________________________________ Date: ______________

Print Name:___________________________________
Director of Identity and Access Management Office
Signed: ________________________________ Date: ______________