Basic Application & Access Information:

What is the name of the application?

What is the purpose of the application?

How will users access the system? (i.e., URL, linked from a webpage)

Will the user need to access the application through a VPN?

Will this application be hosted by Purdue or in the cloud?

What campuses will have access to utilize this application?

Who will have access to this application (i.e. department(s), students, employees, retirees)?

Purdue-branded name (if applicable)

Is there any other information you'd like to share with our team?

Project and Contact Information

Departmental Contact Name

Departmental Contact Email

Branded name (if applicable)

Name of Purdue application administrator

Who will be the Purdue departmental contact to assist in testing once single sign-on is set up?

What is the implementation timeline for your request?

What is the earliest date that single sign-on can be set up?

Has this application been purchased?

Will there be a non-production environment to integrate with SSO?

Vendor Name

Vendor Website URL

Vendor Contact Name

Vendor Contact Email

Has a Purdue security review been initiated?

- ◯ Yes
- ◯ No

If a Purdue security review has not been initiated, it is required for all Purdue application implementations. Please go to the following page to submit a security review request: https://www.purdue.edu/securepurdue/services/solution-services-review.php

---

***Typically, the vendor will assist with answering the following SSO-specific questions. Also needed from them is a copy of the application's metadata (XML file or URL). They will also need our production metadata, which is available at https://sso.purdue.edu/idp/shibboleth. Please note that this version assumes the application supports ECDSA signing.

SSO Protocol

What is the SSO protocol supported by the vendor?

- ◯ SAML with Shibboleth
- ◯ CAS
- ◯ OIDC
- ◯ SAML with Entra ID
- ◯ Other/I Don't Know

Is the vendor a member of InCommon? No

Please provide a URL of the vendor's metadata and/or vendor's documentation explaining their single sign-on set-up process here.

Does the vendor support the ECDSA signing method? Unsure

Who is responsible for setting up single sign-on on the application side?

Has the vendor supplied a list of roles that are standard within the system?

How will accounts be created in this application?

How will permissions, rights and roles be set up?

What attributes are required for this application? Select all that apply.

- [ ] uid
- [ ] mail
- [ ] displayName
- [ ] cn
- [ ] sn
- [ ] givenName
- [ ] employeeNumber
- [ ] employeeType
- [ ] eduPersonPrincipal Name (ePPN)
- [ ] eduPersonScopedAffiliation
- [ ] eduPersonTargetedID
- [ ] eduCourseOffering
- [ ] Other/Unknown