Onboarding Process

Section 1.1: Onboarding Process Flow

1. Requesters should review requirements below and in the SSO requirements and recommendations document:
   - **SSL and SAML 2.0 are a requirement**
     We need the Service Provider or application to enable SSL on their server as a pre-requisite to make sure all communications are over https instead of http. We require to use SAML 2.0 in order to take advantage of Multi-Factor Authentication (MFA) layer of security.
   - **The recommended Unique Identifier is EmployeeID**
     We recommend to use the EmployeeID (i.e. 500####) or ePPN (eduPrincipalPersonName) to identify the user and validate their account when they login. EmployeeID and ePPN will not change while an attribute such as email or CanID can change. Please review the list of attributes available from the University.

2. Once the requirements above have been met, application owner requests Single Sign-On (SSO) integration by submitting an RFS (Request for Service) through UService. When submitting the RFS, requesters should provide the assessment form filled out and attach it to the UService request. RFS will not go forward with a missing assessment form.

3. Request is approved by UMIT Governance.

4. Middleware Identity Management will coordinate with project manager/vendor to exchange metadata information and customized attribute requirements between the (service provider/application) SP and our Shibboleth (Identity Provider) IdP technical contact.

UMSSO Information for Vendors/Application:

- **Test Redirect URL**: [https://cas.cgcent.miami.edu/idp/profile/SAML2/Redirect/SSO](https://cas.cgcent.miami.edu/idp/profile/SAML2/Redirect/SSO)
- **Test Metadata URL**: [https://cas.cgcent.miami.edu/idp/shibboleth](https://cas.cgcent.miami.edu/idp/shibboleth)
- **Test EntityID**: [https://cas.cgcent.miami.edu/idp/shibboleth](https://cas.cgcent.miami.edu/idp/shibboleth)
- **Test Logout**: [https://cas.cgcent.miami.edu/idp/logoutIDP.jsp](https://cas.cgcent.miami.edu/idp/logoutIDP.jsp)

5. Testing is initiated and recommended based on the following test cases.
6. Once testing is successful, all parties agree on promotion to production with e-mail from application owner approving IdP promotion.
7. Middleware Identity Management Team receives request to promote and approves promotion to production IdP.
8. Once IdP promotion has been approved internally, a target date is set and we start
coordinating promotion, usually done on **Tuesdays** or **Thursdays** at **8 p.m.** The application owner/SSO integration requester is responsible for the application and obtaining approval for changes with the Change Advisory Board (CAB). The Clinical CAB is on Tuesdays and Non-Clinical CAB is on Wednesdays. The Middleware Identity group will submit request for the SSO integration to the Non-Clinical CAB.

9. Once CAB approvals have been obtained, promotion to IdP production will be coordinated between the SSO team and the application owner and/or vendor. Emails will be sent to all parties involved once promotion has been successfully completed.

10. Production metadata information will be provided to the vendor/application as soon as IdP promotion is completed.

11. Application redirects to Production IdP and user testing is performed in Production by application owners. User testing results will be provided to the Middleware Identity Services Team to determine promotion has been successfully completed. Any issues with the promotion will be addressed immediately.