Onboarding Process

Section 1.1: Onboarding Process Flow

1. Application owner requests Single Sign-on (SSO) integration by sending to SSO Support at umsso@miami.edu as an RFS (Request for Service). SSO services should be requested specifically on the Description of Service Requested.
2. Project Managers should provide the assessment form filled out to Middleware group for us to estimate effort required.
3. The Middleware Identity Management Team starts assessing requirements and effort for SSO integration.
4. Request is approved by Middleware Identity Management Team.
5. 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.

UM SSO Information for Vendors/Application:

Test Redirect URL: https://cas.cgcent.miami.edu/idp/profile/SAML2/Redirect/SSO
Test Metadata URL: https://cas.cgcent.miami.edu/idp/shibboleth
Test EntityID: https://cas.cgcent.miami.edu/idp/shibboleth
Test Logout: https://cas.cgcent.miami.edu/idp/logoutIDP.jsp

6. Testing is initiated and recommended based on the following test cases.
7. Once testing is successful, all parties agree on promotion to production with e-mail from application owner approving IdP promotion.
8. Middleware Identity Management Team receives request to promote and approves promotion to production IdP.
9. 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.
10. 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.
11. Production metadata information will be provided to the vendor/application as soon as IdP promotion is completed.
12. 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.