Single Sign-On Requirements and Recommendations

**Section 1.1: Requirements and Recommendations**

- **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 communication 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 logon on. EmployeeID and ePPN will not change while an attribute such as email or CaneID can change. For additional attributes, please refer to the list of attributes available from the University.

- **User access authorization lies within the application**
  Single Sign-on will authenticate all users with a valid CaneID and password. However, the application should be able to allow or deny user access. The Shibboleth IdP can release specific customized attributes such as affiliation or Active Directory (AD) group information to service the application identify the user’s AD groups and therefore determine his or her level of access.

- **“No access allowed” Page**
  If the user does not have access to the application, the user should be redirected to an “Access denied” page which should explain the user is not authorized to use the application and to contact user support.

- **Logout Page**
  The university recommends during logout, to let the user know to close the browser. The message should read: “To completely and safely logout and prevent others from accessing your account, please close/exit your web browser”. The SSO session should be terminated at the Service Provider’s side as well as the Identity Provider’s side. See logout document.

- **Single Sign-On Session Testing**
  We have a few test scenarios that will allow the application owner or users to make sure their Single Sign-on implementation works as expected. This includes testing the session “sharing” across different applications and recommended logout process flow and user access. Please refer to the following test cases documentation as a guide to test.

- **Single Sign-On (SSO) Onboard Process**
  Please read the onboarding process for next steps required here.