Suffolk University

Stage 1: Intra-campus Web Single Sign-on - *Central Identity Provider*

Task	Limited Scope	Broader Scope .....
Policy Steps		
1. Define who establishes various policies related to single sign-on (SSO) and authentication		
2. Have basic identity management policies in place, including data and service stewardship responsibilities and use of the system		
3. Have policy in place specifying whether NONE/SOME/ALL campus authenticated web sites are REQUIRED to use the central web single sign-on system		
Business Practice Steps		
4. Create Help desk support for users encountering problems accessing central web sites protected by SSO		
5. Reliably issue credentials to on-campus faculty/staff/students		
6. Create Help desk support for users encountering problems accessing department web sites protected by SSO		
Technical - Basic Identity and Access ManagementSteps		
7. Provision/de-provision accounts for and authenticate on-campus faculty, staff, and students		
8. Provision/de-provision accounts for and authenticate other constituencies (e.g. applicants, alums, affiliates)		
Technical - Shibboleth software Steps		
9. Install/operate/manage Shibboleth identity provider software		

Stage 1: Intra-campus Web Single Sign-on - *Central and Department Service Providers*

Task	Limited Scope	Broader Scope .....
Policy steps		
10. Define how often service providers should refresh their metadata		
11. Promulgate policy describing process and constraints when a service provider is compromised		
12. Define minimum operational and environmental requirements for the remote server/application		
13. Define policies on log retention at service providers		
Business practice steps		
14. Create process to register a new service providers (e.g. site inspection requirements)		
15. Create problem resolution process for when users cannot access department-supported service provider		
16. Create process for service providers to report abuse of their site (e.g. such as by anonymous users)		
Technical - Basic Identity and Access Management Steps		
17. Provide technical support to department service provider sites, including documentation describing the web SSO service (description, process to participate, etc)		
Technical - Shibboleth Software Steps		
18. Manage the metadata describing service providers and provide mechanism for distribution		
19. Choose approach to PKI trust within the campus federation (rooted, self-signed)		
20. Provide installation instructions, configuration files and other local files (e.g. error pages, logos) customized to the campus for the department sysadmins		

Stage 2: Attribute Delivery - *Central Identity Provider*

Task	Limited Scope	Broader Scope .....
Policy steps		
21. Identify attribute source systems and define and describe the set of attributes that are available		
22. Identify who governs the decision to release attribute X to service provider Y		
23. Develop policy defining, in a general way, which services are eligible to receive which attributes		
24. Achieve buy in to attribute release process from Identity stakeholders		
Business Practice Steps		
25. Define problem escalation procedure, such as when the wrong attributes are sent to a service provider		
26. Define process to follow when a service provider requests an attribute that is not currently available as defined by the policy above		
Technical - Basic Identity and Access Management Steps		
27. Maintain a minimal set of attributes describing each user		
28. Populate eduPerson attributes for each user		
29. Manage entitlement values on user objects		
30. Provide support for groups in the local directory and configure Shibboleth to use them		
Technical - Shibboleth Software Steps		
31. Configure the identity provider attribute resolver for the appropriate sources		
32. Identify who is responsible for editing/implementing the attribute release policies		

Stage 2: Attribute Delivery - *Central and Department Service Providers*

Task	Limited Scope	Broader Scope .....
Policy steps		
33. Develop policy governing use of attributes by service providers such as attribute retention, sharing, etc.		
Business Practice Steps		
34. Define process a service provider would use to request attributes and the process used to respond to the request		
Technical - Shibboleth Software Steps		
35. Document how a service provider's web server could authorize users given the provided attributes		
36. Document how an application could use the supplied attributes in alternative ways, such as for customization or form completion		

Stage 3: Inter-campus Federation - *Central Identity Provider*

Task	Limited Scope	Broader Scope .....
Policy steps		
37. Ensure compliance with federation policies		
38. Publish identity management and identification and authentication practice, if required		
Business practice steps		
39. Define process for a) a department requesting an attribute release policy referring to a remote site, and b) central IT reviewing, creating, and managing the attribute release policy		
40. Define help desk process for when user encounters a problem accessing service providers		
Technical - Basic Identity and Access Management Steps		

41. Ensure compliance with federation attribute practice		
Technical - Shibboleth Software and Federation Requirements Steps		
42. Follow technical steps to join the desired federation		
43. Configure identity provider software to use federation metadata and credentials and refresh when required		

Stage 3: Inter-campus Federation - *Central and Department Service Providers*

Task	**Limited Scope**	**Broader Scope** .....
Policy steps		
44. Ensure SP is compliant with federation policies		
Business Practice		
45. Ensure service provider has defined problem resolution process for remote users		
46. Create process for department service provider to ask to be added to federation metadata		
Technical - Shibboleth Software and Federation Requirements		
47. Add service provider information to the federation metadata		
48. Configure service provider software to use federation metadata and credentials and refresh when required		