Corporate Privacy Impact Assessment for Keycloak

Appendix A – Keycloak

What is Keycloak?

This BC Government **Single Sign-On (SSO)** service, based on the Open Source Keycloak (aka Red Hat SSO) product, provides an industry standard (OIDC) and enterprise-policy compliant means of implementing authentication and authorization within applications that is also simple for development teams to provision, utilize and manage. This service is offered to BC Government development teams building cloud native web or mobile applications. Teams wishing to use this service should connect with the Enterprise DevOps Team to discuss their needs and ensure alignment prior to making a request.

Approved Identity Providers

Keycloak must only be used with these specific approved identity providers:

Approved BC Government Identity Providers	BC Gov IDIR and BCeID (Basic, Business, Personal).
Approved Third Party Identity Providers	GitHub, Linked In, and Google

Ministries seeking to use alternative identity providers should contact the Enterprise DevOps Team at Pathfinder@gov.bc.ca. **Any use of an alternative identity provider will need to be assessed in the application or project PIA.**

My Project is Using Keycloak, Now What?

The Privacy Impact Assessment (PIA) for the application or project using Keycloak will need to address some specific Keycloak details. This requirement originates from the Corporate Keycloak PIA. Here is a list of details that should be included in the application or project PIA which uses Keycloak.

Detail	Explanation
1. Identity Provider	Only approved identity providers can be used with Keycloak
2. Data Elements	Each Identity Provider has slightly different data objects as part of their authentication responses. Part of the different data objects contains user information which may contain personal information and will be to be assessed in the PIA.

3. Disclosure	User information that is personal information may be disclosed to the application using Keycloak. This disclosure needs to be assessed in the PIA.
4. Collection Notice	Ensure your application or project PIA includes the required collection notice as found in the Corporate Keycloak PIA – question 10.
5. Personal Information Bank (PIB)	Any personal information that is stored and searchable by a personal identifier needs to be recorded as a PIB. This includes any user information that is personal information.

For more information on Single Sing-On (SSO) service and Keycloak, please visit: https://developer.gov.bc.ca/Authentication-and-Authorization/BC-Government-SSO-Service-Definition

For more information on The Keycloak Corporate Privacy Impact Assessment, please visit <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments/corporate>, contact your Ministry Privacy Officer, or call or email the Privacy and Access Helpline at 250-356-1851 or privacy.helpline@gov.bc.ca