Information Technology Policy

Keystone Login and Identity Proofing

ITP Number	**Effective Date**
ITP-SEC039	August 11, 2020
Category	**Supersedes**
Security	ITP-SEC013, ITP-SEC014
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	December 2021

1.   Purpose

This Information Technology Policy (ITP) is to establish and maintain a centralized account management system for online services for the Commonwealth and to establish standards for online identity proofing of public users accessing Commonwealth IT web services or online applications.

2.   Scope

This ITP applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction (collectively "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3.   Definitions

3.1   Keystone Login - is an account management system for Commonwealth of Pennsylvania online services.

4   Policy

Keystone Login

All citizen facing applications are to use Keystone Login for Authentication services. Keystone Login is an account management system for Commonwealth of Pennsylvania online services. The Keystone Login portal provides the following capabilities: account creation and management, Identity Verification, Authentication services and Single Sign-On (SSO) (sign on once to access multiple applications), social media login (e.g., Google), and risk-based multi-factor authentication. The Keystone Login provides citizens with a single credential (username and password) that can be used to access online services from multiple state agencies.

Keystone Login Accounts that have not been accessed in 18 months will be purged.

Identity Proofing

Identity Proofing is the process of verifying the real-life identify being claimed by a person. For purposes of this ITP, Identity Proofing shall be limited to identity proofing levels and corresponding authentication requirements. Authorization focused on the actions or activities the public user is permitted after authentication has occurred is outside of the scope of this ITP. This ITP DOES NOT seek to establish or to impose business requirements on agency applications or services, particularly with regard to authorization of a public user. Such requirements are left to the agency and/or the appropriate business unit within the agency to determine.

The following <u>Levels of Assurance (LOA)</u> are established for the Commonwealth:

> **LOA1:** Self-asserted identity with little or no confidence in who the *person* behind the identity is. This is the lowest level of assurance and should only be used in circumstances where anonymous logons would be allowed and where the true identity of the person is irrelevant.
>
> Examples of such use would include:
> - **1.1** Portal logon to greet returning people
> - **1.2** Dissemination of publicly available information
> - **1.3** Preliminary application or registration for a program where the identity is established at a later step.

> **LOA2:** Identity for which there is some level of confidence in who the *person* behind the identity is. The identity may be verified in a number of ways such as presentation of proofing materials (e.g. driver's license) or something that they have knowledge of (e.g. knowledge based Q&A). A minimum of user ID and password is sufficient for authentication and shall be in compliance with current Commonwealth password policies (ITP-SEC007 *Minimum Standards for User IDs and Passwords*). This level is generally sufficient for most online interactions.

5   Service Description

There are two options to interface agency applications with Keystone Login: Keystone Login Portal and a suite of Keystone Login APIs. The following list of functionalities is supported by either option:

Account Creation and Management – Keystone Login provides this functionality by interacting with the Commonwealth's only approved citizen-facing user account domain called SRPROD. Keystone Login allows citizens to create an account in the SRPROD domain, maintain that account by changing account information, and manage that account by adding other features to the account.

Authentication – Keystone Login provides this functionality by interacting with the citizen-facing user account domain and the Commonwealth employee account domain.

Identity Verification – Keystone Login allows SRPROD account owners to verify themselves as LOA2 authenticated accounts.

Multi-Factor Authentication Services (MFA) – Keystone Login allows account owners who have chosen to elevate their accounts to LOA2, to also enable MFA on those accounts

Single Sign-On (SSO) – Keystone Login promotes a SSO experience.

Keystone Login also offers the ability to login using an existing Google social media account. This is available only by using the Keystone Login Portal, as it cannot be extended through an API.

6   Responsibilities

6.1   Service Owner – Enterprise Information Security Office

6.2   Service Provider – Enterprise Solutions Office

7   Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx

- Management Directive 205.34 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*

- ITP-SEC007 – *Minimum Standards for IDs, Passwords and Multi-Factor Authentication*

- Executive Order 2019-04 – *Establishing a "Citizen First" Directory and Promoting Customer Service Transformation*

8   Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

9   Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

10 Exemption from This Policy

In the event an agency chooses to seek an exemption from the guidance within this IT policy, a request for a policy waiver is to be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	08/11/2020	Consolidate SEC013 and SEC014 to align with new technology standards	N/A
Revision	12/07/2020	Added hyperlinks to OA Glossary and removed words from definition section Consolidated SEC037 and SEC039	Revision Redline Link <12/7/2020>