1. **Purpose**
   This Information Technology Policy (ITP) is to establish and maintain a centralized account management system for online services for the Commonwealth.

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  **Application Programming Interface (API)** – Also known as a Web API as used in the context of Keystone Login, is an interface containing multiple web-exposed endpoints to a defined request-response data transfer system and/or messaging system.

   3.2  **Identity Verification** -- Used to ensure that users provide information that is associated with the identity of a real person. In the context of this ITP, it involves the verification of identity information (fields) against independent and authoritative sources, such as a credit bureau or Commonwealth data.

   3.3  **Keystone Login** – is an account management system for Commonwealth of Pennsylvania online services.

   3.4  **Level of Assurance (LOA)** -- The measurement of the degree or level of confidence that the person is who they are claiming to be. The Commonwealth recognizes two levels of assurance:

   3.4.1.1  **LOA1** – little or no confidence in the user’s identity beyond what the user claims

   3.4.1.2  **LOA2** – information provided by the user has been verified by a third party via the processes provided per  *ITP-SEC037 Identity Proofing of Online Users*.

   3.5  **Multi-Factor Authentication (MFA)** -- A security system that verifies a user’s identity by requiring the user to provide multiple types of credentials, which can include simple **Authentication** credentials, one-time passcodes, automated phone calls and/or biometrics.
3.6 **Single Sign-On** – Single Sign-On is a property of identity and access management that enables users to securely authenticate with multiple applications and websites by logging in only once—with just one set of credentials (username and password).

4. **Policy**

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 (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.

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, the Commonwealth employee account domain and the business partner account domain.

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

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

**Single Sign-On** – Keystone Login promotes a Single Sign-On 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

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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Purpose of Revision</th>
<th>Redline Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original</td>
<td>08/11/2020</td>
<td>Consolidate SEC013 and SEC014 to align with new technology standards</td>
<td>N/A</td>
</tr>
</tbody>
</table>