Information Technology Policy
Keystone Login and Identity Proofing

Number
ITP-SEC039

Effective Date
August 11, 2020

Category
Security

Supersedes
ITP-SEC013, ITP-SEC014

Contact
RA-ITCentral@pa.gov

Scheduled Review
April 2024

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 and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. 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 (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 disabled.

Connectivity specifications for Criminal Justice Information Systems utilizing Keystone Login are outlined in *OPD-SEC039B, Authentication Requirements for Connectivity to Criminal Justice Information Systems*.

Identity Proofing

Identity Proofing is the process of verifying the real-life identity 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 Levels of Assurance (LOA) 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 IDs, Passwords, Sessions, and Multi-Factor Authentication*). This level is generally sufficient for most online interactions.

4. Service Description

There are two options to interface agency applications with Keystone Login: Keystone Login Portal and a suite of Keystone Login APIs (Public and Private). The Public APIs are available for integration efforts with SaaS/COTs systems. 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 provides MFA for users account via a one-time passcode to verified email or text enabled mobile number. Keystone Login allows account owners who have chosen to elevate their accounts to LOA2, to also enable Risk Based 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.

5. Responsibilities

5.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

5.2 Office of Administration, Office of Information Technology shall:

Comply with the requirements as outlined in this ITP.

- **Service Owner –** Enterprise Information Security Office
- **Service Provider –** Enterprise Solutions Office

5.3 Third-party vendors, licensors, contractors, or suppliers shall:

Ensure all citizen facing applications use Keystone Login for Authentication services and describe its use of the Commonwealth's established identity proofing services.

6. 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 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *OPD-SEC039A, Detailed Keystone Login Service Descriptions & Identity Proofing*
- *OPD-SEC039B, Authentication Requirements for Connectivity to Criminal Justice Information Systems*
- *ITP-ACC001, Information Technology Digital Accessibility Policy*
- *ITP-SEC007, Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*
- *Executive Order 2019-04, Establishing a "Citizen First" Directory and Promoting Customer Service Transformation*

- *Federal Identity, Credential, and Access Management (FICAM), Protecting Digital Identities and Assets*
- *Federal Office of Management and Budget M-04-04, E-Authentication Guidance for Federal Agencies*
- *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*
- *National Strategy for Trusted Identities in Cyberspace (NSTIC) Resource Information*
- *NIST SP 800-63-3 - Digital Identity Guidelines document suite*

7. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

Criminal Justice Information Services (CJIS) Security Policy

8. 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.

9. Exemption from this Policy

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

For CJIS exemptions, approval from the Pennsylvania State Police CLEAN Administrative Section is required, ra-clean@pa.gov.

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	N/A
Revision	09/07/2021	• Added Third-party vendors to Scope and Responsibilities Section • Responsibilities Section updated to include Agency and OA/OIT • Created new Supplemental Document OPD-SEC039B and added reference in Policy	N/A

Revision	04/27/2023	• ITP Refresh • Scope updated • Definitions replaced with links to glossary • Updated references and links • Responsibilities section was updated for Third-parties consistent with OPD-SEC000B. • Added exemption details for CJIS from supporting documents (OPD-SEC039A & OPD-SEC039B)	Revision Redline Link <04/27/2023>