हिमाचल प्रदेश सरकार

Policy Document

on

Digital Identity and Access Management in the State of Himachal Pradesh (Him Access)

Department of Digital Technologies and Governance

Government of Himachal Pradesh

1. Purpose

Many e-Governance initiatives are being undertaken by various State Government Departments, Boards, Corporations and other Organisations. However, most of them are working in silos and thus not able to talk to each other or share data amongst applications which forces citizens to apply and collect certificate (like bonafide, character, BPL certificate) from one application and upload the same in other application. In the absence of any standards, integration of e-Governance applications has become difficult. Most of the e-Governance applications build their own mechanism for User Identity and Access Management, resulting in creation of multiple identities/profiles of a User. These applications are seldom interoperable even though many have similar features and functionalities. The formulation of standard guidelines for Identity and Access Management will promote the uniform, consistent and coherent approach amongst applications which in turn will help in building interoperable applications to deliver integrated services to the citizens as well as officials. These issues could be addressed by adopting multi-pronged approach. One among them is by way of implementation of Single Sign On system in all the applications of various State Government Departments, Boards, Corporations and other Organisations.

This policy outlines the guidelines and procedures for implementing and managing **Single Sign On** system in the software applications developed (and would be developed in future) by different State Government Departments, Boards, Corporations, and other Organizations. The primary objective of framing Single Sign-On (**also known as Him Access**) policy is to establish a comprehensive framework that ensures the secure, efficient, and consistent use of Him Access systems across all the State Government Departments, Boards, Corporations and other Organisations.

This Policy aligns with current industry standards for software development and will evolve as technologies advance.

2. Scope of Identity and Access Management Policy

This policy shall apply to all Government Departments, Boards, Corporations, Other Organizations, Employees of Himachal Pradesh Government and all the Citizens who access

State Government services through online portals developed and managed by State Government Departments, Boards, Corporations and Other Organizations. It covers the management, usage, and Governance of Him Access platform across all digital platforms owned and managed by the Government of Himachal Pradesh.

3. Key Definitions

Acronym/ Key Word	Definition
Identity	Identity is a set of attributes that uniquely identifies entity. An entity can be anything that the Government of Himachal Pradesh wishes to uniquely identify for its purposes. Identity is the presentation of the entity. Entity can be a person, group of persons, device, organization, service etc. The same entity may have multiple identities as people perform many social, economic, and political functions, for example a person can be a citizen, a trader, an employee, etc. Each role may require different set of attributes to establish the identity. Sometimes individuals are known by different names in different context. However, identity uniquely represents entity. A digital identity is a set of claims made by one digital subject about itself or another digital subject.
Identity and Access Management (IAM)	Identity and Access Management (IAM) comprises of set of business processes, technologies, supporting infrastructure and policies to create, maintain and use digital identities within a legal framework.
Authentication	Authentication is a process of checking the credentials of an identity against the values in an identity store.
Authorization	The process of determining the user's entitlements for accessing the resource against the permissions configured on that resource.
SSO – Single Sign On	Single sign-on is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems

Acronym/ Key Word	Definition
G2G	Government to Government
G2E	Government to Employees
G2B	Government to Business
G2C	Government to Citizens
G2X	Government to (X) Any Entity (often used to represent interactions with various stakeholders not explicitly covered by the other categories, such as NGOs, international organizations, etc.)
Government Employee	Any individual employed by the Government of Himachal Pradesh
Citizen	Any resident of Himachal Pradesh who utilizes online Government Services
RBAC	Role based Access Control
HOD	Head of the Department
DDO	Drawing and Disbursing Officer
Nodal Officer	An Officer/ Official appointed by HOD to manage the operation and management of Him Access platform on behalf of HOD

4. Stakeholders

Stakeholders	
Government Employees	All Government Employees will use the Him Access platform to login to various Government applications. The platform will serve as a centralized gateway for Government Employees to manage their access to different Departmental Applications efficiently.
Citizens	All residents of the State will use Him Access to access a wide range of Government services and applications. This ensures a unified and streamlined process for accessing public services, enhancing user convenience and efficiency.

Stakeholders	
Business Entities	All Business Entities operating within the State or initiating process to setup base in near future will use Him Access to access a wide range of Government to Business services as well as applications. This ensures a unified and streamlined process for accessing G2B services, enhancing user convenience and efficiency.

5. About Him Access

5.1 Introduction

Him Access is a Single Sign-On (SSO) application developed by the Department of Digital Technologies and Governance to facilitate citizens' and Government officers' access to a wide array of Government services and resources using a single set of login credentials, making the management of multiple accounts redundant. Through Him Access, Government Employees can access all Departmental Applications, such as SPARROW, e-Office, e-District, MMSS and more, without needing to maintain separate User Id/Passwords.

The adoption of the Him Access platform brings substantial benefits to both citizens of the State and the Government Employees. For citizens, it simplifies interactions with the Government, saving time and resources as they no longer need to create and remember multiple usernames and passwords. The platform enhances data security by requiring citizens to share their information only once during registration on Him Access platform, reducing the risk of identity theft or misuse. Additionally, the data collected during registration is verified through an OTP-based mechanism, ensuring accuracy and security.

For Government offices and agencies, Him Access streamlines the authentication process, significantly reducing administrative expenses associated with managing multiple user accounts across different applications. The Him Access platform also ensures data accuracy and consistency across various Departmental applications, serving as a single source of truth for citizen data and minimizing errors, duplications and ghost profiles. Centralized security measures can be implemented more effectively, enhancing data protection and compliance with privacy regulations.

Him Access fosters transparency by enabling citizens to monitor the real-time status of their applications, payments, and grievances across different Departments. Moreover, it streamlines all Government processes by facilitating collaboration between Departments and seamless information sharing. This leads to better resource management, informed decision-making, and optimized delivery of public services, ultimately driving cost efficiency and improving Governance.

5.2 Benefits

The use of Him Access is expected to provide the following benefits:

5.2.1 A single and comprehensive view of an identity (Single Source of Truth)

5.2.2 Elimination or significant reduction in storing duplicate identities.

5.2.3 Interoperability of applications by enforcement of Data standardization through IAM

5.2.4 Reduction in the risk of unauthorized access to and modification or destruction of Government information assets.

5.2.5 Control, enforce and monitor access to resources through auditing.

5.2.6 Improved user participation (one time sign on facility for availing all Government Services)

5.2.7 Improved service delivery to citizen

5.2.8 Improved regulatory capabilities.

5.3 Registration Process

5.3.1 Government Employees

5.3.1.1 The registration of Government Employees on the Him Access platform will be overseen by the HOD/ DDO/ Nodal Officer appointed by the respective departments in coordination with the Department of Digital Technologies and

Governance.

5.3.1.2 Respective departments are required to register all departmental employees with the employment type categorized as Regular using the PMIS Code, as recorded in the Service Book (Manav Sampada).

5.3.1.3 For departmental employees with employment types other than Regular, registration must be completed using Aadhaar eKYC to ensure user authenticity.

5.3.1.4 In the event of migration of users of existing applications to Him Access platform, the employees shall proceed using their existing username and password. Following the successful authentication, the departmental employee will be directed to update his/her profile. This updated profile will then become part of the Him Access platform. The concerned Department is required to verify the Him Access profile of the employee and accordingly grant access to the departmental applications.

5.3.1.5 All Government Employees are required to get their official Email IDs created through the Department of Digital Technologies and Governance and the same will be free of cost. On creation of official Email Id's, Employees would be able to Login to Him Access platform.

5.3.1.6 All Departments, Boards and Corporation Employees will be assigned a unique email address with the domain **"himaccess.hp.gov.in"**, which will be utilized for authentication and login purposes.

5.3.1.7 Access rights to the employees will be granted by the HOD/ DDO/ Nodal Officer of the respective Department based on the roles and responsibilities assigned to the Employee.

5.3.2 Citizens

5.3.2.1 Citizens can register themselves on Him Access platform through a dedicated portal (https://himaccess.hp.gov.in).

5.3.2.2 Identity verification will be mandatory during the registration process, leveraging Aadhaar eKYC/ Ration Card number/ HimParivar ID/ Him Member ID, Mobile Verification and Email Verification.

5.3.2.3 Each citizen will be provided with an autogenerated username, which will be suffixed with the domain "**himaccess.in**". Citizens will have the option to change or modify their autogenerated username.

6. Roles and Responsibilities

6.1 Departments

6.1.1 All Government Departments/Boards/ Corporations/ Organizations are responsible for integrating their existing as well as future applications and services with the Him Access platform (Citizen as well as Government users) to ensure seamless access for employees and authorized users. For Legacy applications, all Government Departments/Boards/ Corporations/ Organizations shall migrate their existing G2C, G2B, G2G and G2X applications within a period of six months.

6.1.2 The Him Access integration related documents are readily available on **https://himparivar.hp.gov.in/ssointegration**

6.1.3 All Government Departments/Boards/ Corporations/ Organizations to ensure that all employees are registered on Him Access system and have their access rights configured according to their roles and responsibilities.

6.1.4 All Government Departments/Boards/ Corporations/ Organizations to oversee the creation, modification, and deactivation of user accounts in the Him Access system as per the requirements. Ensure timely removal of access for employees who are transferred, promoted, retired, or left their roles etc.

6.1.5 All Government Departments/Boards/ Corporations/ Organizations to handle requests related to account management, including password resets, access issues, and other Him Access-related queries from employees.

6.1.6 All Government Departments/Boards/ Corporations/ Organizations to provide training and resources to employees on the use of the Him Access system, including security, best practices and procedures for accessing departmental services.

6.2 Government Employees

6.2.1 Government employees must ensure their Him Access accounts are created and maintained correctly. This involves accurate registration with up-to-date personal and professional information.

6.2.2 Employees should verify that their access rights are aligned with their job roles and responsibilities. Any change in job roles should be communicated to the HOD/ DDO/ Nodal Officer of the reporting department promptly to update access permissions accordingly.

6.2.3 Employees are required to create strong, unique passwords for their Him Access accounts and change them regularly. Passwords must be kept confidential and not shared with anyone.

6.2.4 Any suspected compromise or unauthorized use of their Him Access credentials must be reported immediately to the concerned Department.

6.2.5 Employees should use their Him Access credentials solely for accessing services and applications pertinent to their official duties. They must not attempt to access unauthorized areas or use their credentials for personal purposes.

6.2.6 Employees are fully accountable for their actions taken while using their Him Access accounts and must adhere to ethical and legal standards in the use of Government systems.

6.2.7 Employees are responsible for safeguarding their login credentials and must avoid sharing them with others. If credentials are compromised, they should immediately report the issue to their HOD/ DDO/ Nodal Officer and follow the prescribed steps to secure their account.

6.2.8 Employees are legally responsible for their actions taken while using their Him Access accounts. Any misuse or violation of terms could result in penalties or legal or disciplinary actions as per applicable laws.

6.3 Citizens

6.3.1 Citizens must register and create Him Access account through the designated Government portal (https://himaccess.hp.gov.in) for availing various government services.

6.3.2 During registration, they must provide accurate information and complete identity verification, typically using Aadhaar or other government-issued IDs.

6.3.3 Citizens are responsible for keeping their user profile information up to date.

6.3.4 Any changes in contact details or other relevant information must be updated through the Him Access portal to ensure continuous access to services.

6.3.5 Citizens must create strong, unique passwords for their Him Access accounts. Passwords should be changed regularly and should not be shared with anyone.

6.3.6 Citizens are responsible for safeguarding their login credentials and must avoid sharing them with others. If credentials are compromised, they should immediately report the issue and follow the prescribed steps to secure their account.

6.3.7 When using government services, citizens should follow the guidelines and processes provided to ensure smooth and effective service delivery.

6.3.8 Citizens are legally responsible for their actions taken while using their Him Access accounts. Any misuse or violation of terms could result in penalties or legal actions as per applicable laws.

7. Access Controls, Privacy and Security

7.1 Privacy

Him Access is committed to protecting the privacy of users. All personal data collected during the registration and use of the platform will be handled in accordance with applicable privacy laws and regulations. User data will be processed transparently and only for the purposes for which it was collected. The platform will not share personal data with third parties without explicit user consent, except when required by law. Regular audits and assessments will be conducted to ensure compliance with privacy policies and to safeguard user data from unauthorized access or disclosure.

7.2 Security

Security is a critical aspect of Him Access, with all credentials and associated data being encrypted using industry-standard methods to protect against unauthorized access and breaches. The platform will implement continuous monitoring of login activities to detect and respond to any suspicious activities promptly. In the event of a security breach or suspicious activity, affected user accounts will be temporarily locked, and users will be immediately notified to take corrective actions. Regular security audits will be performed by the Department of Digital Technologies and Governance to identify and address any vulnerabilities, ensuring that the platform remains secure against evolving threats.

7.3 Access Control

Him Access will enforce Role-Based Access Control (RBAC) for government employees, ensuring that access to information and services is restricted to what is necessary for their specific roles and responsibilities. The Identity and Access Management (IAM) system will dynamically manage access rights, adjusting them as user roles change within the organization. Access policies, whether role-based, rule-based, or identity-based, will be established in line with organizational requirements to ensure precise and effective management of entitlements. These measures will help to maintain a secure and controlled environment, minimizing the risk of unauthorized access and enhancing the overall security posture of government services accessed through Him Access.

8. Power to amend any provision of the policy

The Department of Digital Technologies and Governance retains the right to amend any provision of this Policy to accommodate advancements in digital technologies or to enhance system security and best practices.

Approved vide NN-12 by
Chief Secretary to the
Government of Himachal Pradesh

File No: E:119159-DIT-F02/1/2023-IT-DIT-148 **Dated:** 16.08.2024

Copy for information & necessary action is forwarded to: -

1. All the Administrative Secretaries to the Government of Himachal Pradesh.
2. All the Heads of the Departments in Himachal Pradesh.
3. The Registrar, HP High Court Shimla-171001.
4. The Divisional Commissioner, Shimla, Kangra and Mandi.
5. All the Deputy Commissioners in Himachal Pradesh.
6. All the Superintendent of Police in Himachal Pradesh.
7. All the Managing Director/ Member Secretary/ Commissioner / Secretary/ Chief Executive Officer/ Registrars of Boards/ Corporations/ Councils/ Authority/ Universities/ Municipal Corporations/ Co-Operative Banks in Himachal Pradesh.
8. Guard File

Director,
Department of Digital Technologies and Governance,
Government of Himachal Pradesh