Jennifer Krupp, MPH, MBA, PHP, Administrator
Division of Consumer Health Services

Stacie Weeks, JD, MPH, Director
Nevada Health Authority

Silver State Health Insurance Exchange (SSHIX) Acceptable Use Agreement

August, 2026

Version 26.01

Table of Contents

Purpose

This acceptable use agreement governs the use of computers, networks, and other information technology (IT) resources administered by the Silver State Health Insurance Exchange (SSHIX), including the Nevada Health Link SBE Platform (SBE Platform). This statement applies to all SSHIX employees and contractors, insurance carrier personnel utilizing the SBE Platform for Plan Management or Enrollment Reconciliation functions, and any other persons authorized to access or use SSHIX systems, resources, or information owned or managed by SSHIX, including devices connected by any means to Nevada's SilverNet Wide Area Network.

IT resources within SSHIX shall be used only in a manner consistent with authorized business purposes. "IT resources" include State- or SSHIX-owned or managed hardware, software, computers, mobile devices, networks, applications, cloud services, information systems, and data, as well as personally owned or third-party devices used to access SSHIX systems or information.

Requirements

Users of SSHIX systems, information, networks, applications, devices, and other IT resources are responsible for protecting the confidentiality, integrity, and availability of those resources and for using them only for authorized business purposes.

2.1 Authorized Access and Account Security

Users shall:

- Access only those systems, applications, functions, and information for which they have been specifically authorized.
- Use SSHIX access only for legitimate business purposes consistent with the user's assigned duties or authorized functions.
- Protect passwords, access codes, authentication tokens, certificates, multifactor authentication methods, and other authentication credentials from unauthorized use or disclosure.
- Maintain unique user accountability and shall not share accounts or credentials with another individual.
- Comply with authentication and access-control requirements established by SSHIX, NVHA, or the State of Nevada, including multifactor authentication where required.
- Promptly report suspected credential compromise, unauthorized account activity, or other indications that an account may have been misused.
- Comply with access restrictions and shall not attempt to circumvent, disable, or bypass security controls.

Access privileges shall be limited to the minimum level necessary to perform the user's authorized functions.

2.2 Protection of SSHIX Systems and Information

Users shall safeguard SSHIX systems and information against unauthorized access, use, disclosure, alteration, destruction, loss, or disruption.

Users shall:

- Access, use, modify, transmit, disclose, retain, or dispose of information only when authorized.
- Access and use only the minimum information reasonably necessary to perform the user's authorized function.
- Introduce or enter information into SSHIX systems only when it serves a legitimate and authorized business purpose.
- Protect nonpublic and Sensitive Data when stored, processed, displayed, printed, or transmitted.
- Follow applicable federal, State of Nevada, NVHA, and SSHIX privacy, security, records-management, and information-handling requirements.
- Protect SSHIX information from unauthorized disclosure when communicating over internal or external networks.

2.3 Devices Used to Access SSHIX Resources

State-owned, SSHIX-managed, personally owned, or third-party devices may be used to access SSHIX systems or information only when such access is authorized.

Devices used for authorized access shall:

- Be protected against unauthorized physical and logical access.
- Use appropriate device authentication and access controls.
- Maintain current security updates and supported software where applicable.
- Use malware protection or other endpoint safeguards where required.
- Use encryption where required based on the type or sensitivity of information being accessed or stored.
- Comply with applicable SSHIX, NVHA, and State of Nevada device-security requirements.

Users shall not download, locally store, copy, or otherwise retain SSHIX Sensitive Data on personally owned or unauthorized devices unless specifically authorized.

Users shall immediately report the loss, theft, compromise, or suspected compromise of any device containing SSHIX information or used to access SSHIX systems.

2.4 Software and Technology

Only authorized and properly licensed software, applications, browser extensions, utilities, and other technology may be installed or used on SSHIX-managed devices or systems.

Users shall:

- Comply with applicable software licensing requirements.
- Use software and technology only for authorized purposes.
- Obtain required approval before installing software or connecting devices to SSHIX-managed systems or networks.
- Not use software, services, or technology designed or configured to circumvent established security controls.

2.5 Storage and Transmission of Sensitive Data

SSHIX Sensitive Data shall be stored, processed, and transmitted only through systems, applications, and methods authorized for the sensitivity and classification of the information.
Users shall:

- Use approved secure transmission methods when transmitting PII, PHI, financial information, or other Sensitive Data.
- Apply encryption where required by applicable law, regulation, policy, agreement, or data classification.
- Verify recipients and transmission methods before sending Sensitive Data.
- Limit Sensitive Data included in communications to the minimum information necessary for the authorized business purpose.
- Not transmit or store Sensitive Data through personal email, personal cloud storage, unauthorized file-sharing services, unauthorized messaging platforms, artificial intelligence services, or other unapproved systems.

2.6 Federal Tax Information

Users authorized to access Federal Tax Information (FTI) shall safeguard such information at rest and in transit in accordance with applicable requirements of IRS Publication 1075 and SSHIX-approved FTI security policies, standards, and procedures. FTI shall be accessed, used, disclosed, stored, and transmitted only for authorized purposes and only by individuals authorized to receive such information. Transmission of IRS Forms 1095-A or any other information constituting FTI through email, fax, or any other method prohibited by applicable IRS requirements or SSHIX policy is prohibited.

2.7 Workstation, Session, and Physical Security

Users shall take reasonable precautions to prevent unauthorized persons from accessing or viewing SSHIX systems or Sensitive Data.
Users shall:

- Lock or otherwise secure workstations and devices when left unattended.
- Prevent unauthorized persons from viewing Sensitive Data displayed on screens or printed materials.
- Secure printed or physical records containing Sensitive Data when not in use.
- Dispose of Sensitive Data only through authorized secure-disposal methods.
- Take appropriate precautions when accessing SSHIX systems from remote, public, or shared locations.

2.8 Records and Data Retention

SSHIX information shall be retained and disposed of in accordance with applicable records-retention requirements and authorized business processes.
Users shall not:

- Retain SSHIX information longer than authorized or required.
- Create unnecessary duplicate copies of Sensitive Data.

- Destroy, alter, conceal, or dispose of records in violation of applicable retention requirements, legal holds, investigations, audits, or other preservation obligations.

2.9 Security and Privacy Incident Reporting

Users shall promptly report suspected or actual security or privacy events involving SSHIX systems or information, including but not limited to:

- Unauthorized access or disclosure.
- Suspected credential compromise.
- Phishing or other suspected social-engineering activity affecting SSHIX access.
- Malware or other malicious activity.
- Loss or theft of devices or information.
- Unintended delivery or transmission of Sensitive Data.
- Suspected misuse of SSHIX systems or information.
- Attempts to circumvent security controls.
- Any other event that may compromise the confidentiality, integrity, or availability of SSHIX systems or information.

Reports shall be made through the reporting process established by SSHIX. Users shall not include passwords, authentication credentials, FTI, or unnecessary PII or PHI in an initial email notification.
Users shall cooperate with SSHIX, NVHA Information Security, Privacy, and other authorized personnel in the investigation, containment, remediation, recovery, and documentation of security or privacy events.

2.10 Termination or Change of Access

When a user's employment, contract, business relationship, or authorized function ends or changes, the user shall no longer access SSHIX systems, accounts, information, or privileges for which authorization no longer exists.
Users shall return or appropriately dispose of SSHIX-owned or SSHIX-provided equipment, information, software, records, and other resources as directed.
Users shall not retain copies of SSHIX information following termination of authorized access unless specifically permitted by applicable law, agreement, or written authorization.

Prohibited Actions

Users shall not use SSHIX systems, information, networks, applications, devices, or other IT resources in a manner that is unlawful, unauthorized, inconsistent with legitimate business purposes, or that could adversely affect the confidentiality, integrity, or availability of SSHIX systems or information.
Prohibited activities include, but are not limited to, the following:

3.1 Unauthorized Access and Credential Use

Users shall not:

- Access or attempt to access systems, applications, information, functions, or privileges for which they have not been specifically authorized.
- Use another individual's account, credentials, authentication token, certificate, or other means of authentication.

- Share passwords, authentication tokens, multifactor authentication approvals, access codes, or other authentication credentials with another individual.
- Permit another person to use an account or system session assigned to the user.
- Attempt to obtain elevated privileges or otherwise exceed assigned access permissions without authorization.
- Circumvent, disable, modify, interfere with, or attempt to bypass security controls, access restrictions, monitoring, logging, endpoint protection, encryption, or other safeguards implemented by SSHIX, NVHA, or the State of Nevada.

3.2 Unauthorized Devices, Software, and Services

Users shall not:

- Connect unauthorized hardware, devices, network equipment, or removable storage media to SSHIX-managed systems or networks.
- Install or use unauthorized software, applications, utilities, browser extensions, scripts, or other technology on SSHIX-managed systems.
- Introduce or intentionally facilitate the introduction of malware, viruses, ransomware, key-loggers, Trojans, spyware, or other malicious code.
- Use peer-to-peer file-sharing services or other unauthorized file-transfer technologies.
- Establish or use unauthorized remote-access connections, remote-control software, virtual private networks, tunneling technologies, or other mechanisms intended to bypass established access controls.
- Use technology or services in a manner that interferes with the normal operation, availability, performance, or security of SSHIX systems.

3.3 Protection and Handling of Sensitive Data

Users shall not:

- Access, use, copy, alter, disclose, transmit, retain, or destroy Sensitive Data except as necessary to perform an authorized business function.
- Access or use more information than is reasonably necessary to perform the user's authorized function.
- Copy, download, or store SSHIX Sensitive Data on personally owned devices, removable media, personal storage locations, or other unauthorized systems.
- Send or forward SSHIX Sensitive Data to personal email accounts.
- Upload, enter, transmit, disclose, or otherwise provide SSHIX Sensitive Data to unauthorized websites, cloud services, file-sharing platforms, artificial intelligence systems, collaboration tools, or other external services.
- Transmit PII, PHI, or other Sensitive Data using methods that have not been authorized for the type and sensitivity of information involved.

- Transmit Federal Tax Information, including IRS Forms 1095-A, through email, fax, or any other method prohibited by applicable IRS requirements or SSHIX policy.
- Photograph, record, capture, reproduce, or otherwise retain Sensitive Data using unauthorized devices or applications.

3.4 Electronic Communications

Electronic communication tools used for SSHIX business shall be used professionally and only through authorized methods.

Users shall not use email, messaging platforms, collaboration tools, text messaging, video conferencing, or other electronic communication tools to send, forward, post, upload, or otherwise transmit:

- PII, PHI, or other Sensitive Data without appropriate authorization and required safeguards.
- Federal Tax Information through a prohibited communication method.
- Content that is unlawful, discriminatory, harassing, defamatory, obscene, threatening, sexually explicit, or otherwise inconsistent with applicable State, NVHA, SSHIX, or employer policies.
- Chain letters, unauthorized solicitations, or materials related to personal commercial ventures.
- Copyrighted, licensed, or proprietary materials when the user is not authorized to reproduce, distribute, or transmit such materials.

Users shall not use unauthorized external messaging, collaboration, file-sharing, or communication services to conduct SSHIX business or to transmit or store SSHIX information.

3.5 Internet and External Service Use

Users shall not use SSHIX systems or network resources to access, download, upload, transmit, or distribute content or services that:

- Are unlawful or inconsistent with applicable State, NVHA, SSHIX, or employer policy.
- Contain sexually explicit, pornographic, harassing, discriminatory, threatening, or otherwise inappropriate material.
- Support unauthorized gambling, commercial activities, or personal financial gain.
- Contain malware, malicious code, or software that SSHIX is not authorized or licensed to use.
- Create an unreasonable security risk or interfere with SSHIX business operations.
- Result in unauthorized disclosure, storage, or processing of SSHIX Sensitive Data.

3.6 Personal Use

SSHIX systems and resources are intended primarily for authorized business purposes.

Where permitted by the user's employer and applicable SSHIX policy, limited incidental personal use may be permitted provided that such use:

- Does not interfere with the user's work responsibilities or SSHIX business operations.
- Does not consume unreasonable system, network, or personnel resources.
- Does not result in additional or inappropriate cost to SSHIX or the State.
- Does not involve outside business activities, commercial ventures, fundraising, political activity, or other unauthorized activities.
- Does not violate any applicable federal or State law, regulation, agreement, security requirement, or organizational policy.

- Does not result in the storage, transmission, or processing of SSHIX Sensitive Data through unauthorized systems or services.

3.7 Security and Privacy Violations

Users shall not knowingly conceal, alter, destroy, or withhold information relevant to a security, privacy, compliance, or administrative investigation.
Users shall not interfere with or attempt to prevent authorized security monitoring, auditing, logging, vulnerability assessment, incident response, forensic examination, or other security activities conducted by or on behalf of SSHIX, NVHA, or the State of Nevada.
Users shall promptly report suspected or actual unauthorized access, credential compromise, malware, loss or theft of devices or information, improper disclosure of Sensitive Data, or other suspected security or privacy violations in accordance with SSHIX reporting procedures.

Complaints

Suspected violations of this agreement shall be reported through the appropriate SSHIX reporting channel. Privacy concerns or suspected improper handling of PII, PHI, or FTI shall be reported to the SSHIX Privacy Officer by emailing NVHLprivacy@nvha.nv.gov. Suspected cybersecurity incidents, credential compromise, malware, unauthorized system access, or other security events shall be promptly reported to the SSHIX Information Security Officer or other designated security reporting channel.

Sensitive information, passwords, authentication credentials, FTI, or unnecessary PII/PHI shall not be included in an initial email notification.

Consequences

Violation of this Acceptable Use Agreement may result in restriction, suspension, or revocation of access to SSHIX systems or information and other corrective action appropriate to the individual's relationship with SSHIX.

For SSHIX or State employees, violations may result in disciplinary action in accordance with applicable personnel policies, up to and including termination of employment.

For contractors, insurance carrier personnel, business partners, agents, or other external users, violations may result in notification to the individual's employer or sponsoring organization, suspension or termination of access, removal from authorized functions, contractual remedies, or other action available to SSHIX or the State of Nevada.

Violations may also be referred to law enforcement, regulatory authorities, or other appropriate entities when required or authorized by law.

Definitions

Authentication Credentials:
Any information, device, token, certificate, biometric factor, password, passphrase, authentication application, MFA approval, or other mechanism used to verify identity or authorize access.

Authorized Use:
Use of SSHIX systems, networks, and data that is explicitly approved for official business purposes in accordance with job duties, policy, and management direction.

Personally Identifiable Information (PII):
Any information that can be used to identify an individual, either on its own or when combined with other data. Examples include full name, date of birth, Social Security Number, mailing address, phone number, and government-issued ID numbers.

Protected Health Information (PHI):
Health-related information that is linked to an individual and is protected under HIPAA. This includes medical records, treatment details, insurance information, and any health data tied to a person's identity.

Security Incident:
An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information it processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, procedures, or acceptable use requirements.

Sensitive Data
Includes PII, PHI, Federal Tax Information (FTI), financial information, authentication information, confidential business information, and any other information classified as confidential, restricted, or otherwise requiring protection under applicable federal, State of Nevada, NVHA, or SSHIX requirements.

SSHIX Systems and Information:
Information systems, applications, networks, technology resources, and data owned, operated, managed, or made available by or on behalf of SSHIX, including the Nevada Health Link platform and supporting services.

Electronic Communication Tools
Any technology used to send, receive, or store messages or data as part of SSHIX business operations. This includes, but is not limited to, email, phone calls, voicemail, text messages, instant messaging apps (e.g., Microsoft Teams, Slack), video conferencing platforms, and internal chat systems; regardless of whether accessed via agency-issued or personal devices.

Document Revision History

Version	Issue Date	Changes	Drafted	Approved
1.0	June 3, 2019	Initial Release	R. Cook	R. High
20.01	May 18, 2020	No changes; 2020 annual review	R. Cook	R. High
21.01	May 12, 2021	No changes; 2021 annual review	R. Cook	R. High
22.01	May 05, 2022	No changes; 2022 annual review	R. Cook	R. High
23.01	May 15, 2023	No changes; 2023 annual review	R. Cook	R. High
24.01	May 01, 2024	No changes; 2024 annual review	M. Borgman	R. Cook
25.01	June 13, 2025	No changes; 2025 annual review	M. Borgman	J. Davis
25.02	July 01, 2025	Added handling of PII, PHI, Definitions and updated Consequences.	M. Borgman	J. Davis
26.01	August 26, 2026	NVHA letterhead; consolidate overlapping provisions and better align the Acceptable Use Policy with current NVHA/SSHIX security expectations.	J. Davies, NVHA Information Security Officer	S. Moses, Chief Operations Officer

Silver State Health Insurance Exchange

Acknowledgment of Acceptable Use Agreement

I acknowledge that I have received, read, understand, and agree to comply with the SSHIX Acceptable Use Agreement and applicable privacy and information security requirements governing my access to SSHIX systems and information.

I understand that access to SSHIX systems and information is provided solely for authorized purposes and that my activities may be monitored, logged, reviewed, or audited as permitted by applicable law and policy.

I understand that violations of these requirements may result in restriction or revocation of access, disciplinary or contractual action, and other consequences as authorized by law, regulation, policy, or agreement.

NAME (please print)	
SIGNATURE	
EMPLOYER (LEGAL NAME)	
DATE	