PRIVACY POLICY FOR ABLELINK SMART LIVING MANAGER

Effective Date: May 29, 2026

This Privacy Policy explains how AbleLink Smart Living Technologies, LLC ("we", "us", or "our") collects, uses, discloses, and protects your information in connection with AbleLink Smart Living Manager ("SLM"). SLM is an AbleLink-internal service that performs three functions:

1. It serves as a single sign-on ("SSO") system for AbleLink web applications, allowing a user to authenticate once and then access multiple AbleLink web applications.
2. It manages license assignments for AbleLink mobile and desktop applications, allowing those applications to validate that the device or person using them is properly licensed.
3. It provides a small set of supporting services to AbleLink mobile applications, such as schedule storage and exchange for the AbleLink Endeavor scheduling app.

Because SLM serves AbleLink web, mobile, and desktop applications, it holds information about two distinct populations of users, described separately below. Each AbleLink application that uses SLM also has its own privacy policy describing what that application does with your information once SLM has authenticated you or confirmed your license.

1. Information We Collect

SLM holds information about two populations of users, which it treats separately.

a. Web Users (Sign-In Accounts for AbleLink Web Applications)

A "web user" is an account holder who signs in through SLM's web interface to access an AbleLink web application (such as AbleLink Smart Living Email). When a web user account is created — either by you or by an AbleLink administrator on your behalf — the following information is collected:

- Your name
- A username
- A password (stored only as a one-way hash; we do not retain the password itself)
- An email address (used for password resets, two-factor authentication codes if enabled, and account-related notifications)
- An organization affiliation and a role designation (such as user, organization administrator, or super administrator)

- A flag indicating whether two-factor authentication is enabled for your account
- An API key (a long random string used to allow certain automated launches of AbleLink web applications on your behalf)

While you are using SLM and the AbleLink web applications it provides access to, SLM also records:

- The date and time of your most recent successful login
- A count of consecutive failed login attempts (used to lock the account after too many failures)
- Application log entries describing the actions you took within SLM, including the date and time, your user ID, your IP address, and the action

Once authenticated through SLM, you may launch an AbleLink web application from the SLM portal. When you do so, SLM transmits your name, username, user ID, role, organization ID, and organization name to that application so it can recognize you. The application then issues a one-time access token that is used to complete your sign-in to that application. The data the application stores about you thereafter is governed by that application's own privacy policy.

b. Users of Licensed AbleLink Mobile and Desktop Applications

SLM is also used to validate licenses for AbleLink mobile applications (such as AbleLink Endeavor) and desktop applications (such as AbleLink Smart Living Desktop). Users of these applications do not sign in to SLM's web interface; instead, the application itself contacts SLM to confirm that it is properly licensed and that the device using it is within the licensed quantity for the organization.

Two licensing patterns are used, depending on the application:

- **License key with device user account.** Some AbleLink mobile applications associate a license with a "device user" account so that an individual person can be identified across devices. In this pattern, an AbleLink administrator (or, in some cases, the user) creates a device user account in SLM with a name, a username, a password (stored only as a one-way hash), an organization affiliation, and an API key and identifier used by the mobile application. The user enters these credentials into the mobile application, which then uses them to authenticate to SLM.
- **License key only.** Other AbleLink applications, such as AbleLink Smart Living Desktop, validate a license key directly against the device the application is installed on, without an associated device user account. In this pattern, no per-user account is created in SLM; only the license and the device are tracked.

When a licensed AbleLink mobile or desktop application contacts SLM to validate a license, SLM records information about each device on which the application is being used:

- A device identifier provided by the device or operating system
- A device name (often the name the device's owner has assigned to it, such as "John's iPad" or the Windows computer name)
- The version of the AbleLink application being used

- The IP address of each device check-in, the most recent timestamp of access, and a count of how many times the device has accessed SLM
- A history of recent device check-ins (limited to a small number of most-recent entries per device)

For support and contact purposes, an AbleLink administrator may also store an email address and a contact name associated with a particular device. These fields are used as administrator-maintained notes; they are not collected from the device's user automatically.

c. Application Data Stored on Behalf of AbleLink Mobile Applications

Some AbleLink mobile applications use SLM as a backend for storing or exchanging application data tied to a device user. As of this writing, this consists primarily of schedule data for the AbleLink Endeavor scheduling app:

- A description of the schedule (in a structured data format)
- A package of associated media files, which may include audio recordings made by or for the device user, photographs or images selected by or for the device user, and other media used to make the schedule cognitively accessible
- The date and time the schedule was last updated

Endeavor schedule data is stored so that a device user can move a schedule between Endeavor installations associated with the same device user account. SLM does not access, listen to, view, or otherwise process the contents of these recordings or images for any purpose other than storing them and making them available to the device user's authorized Endeavor installations.

d. Automatically Collected Information

When you interact with SLM's web interface, we may automatically collect technical information including IP address, browser type and version, operating system, pages visited within SLM, and the date and time of your visits. When AbleLink mobile or desktop applications contact SLM, we collect the technical information described in subsections (b) and (c) above.

2. How We Use Your Information

We use the information SLM collects for the following purposes:

- To authenticate web users and allow you to sign in to AbleLink web applications
- To pass basic identifying information (such as your name, username, role, and organization) to the AbleLink web application you are signing in to, so that the application can recognize you
- To allow you to reset your password
- To send a one-time verification code by email if you have enabled two-factor authentication

- To validate that an AbleLink mobile or desktop application is properly licensed and that the device using it is within the licensed quantity for the organization
- To store and return Endeavor schedule data on behalf of device users, as described in Section 1c
- To detect and prevent abuse, including by limiting failed login attempts and locking accounts when appropriate
- To administer accounts, organizations, licenses, and devices at an organizational level (for administrator and super-administrator users)
- To maintain application logs for security, troubleshooting, and audit purposes
- To comply with legal obligations and protect the security and integrity of SLM and the applications it serves

We do not use SLM data for advertising, and we do not sell SLM data. We do not use the contents of stored Endeavor schedules, audio recordings, or images to train artificial intelligence or machine learning models.

3. Sharing Your Information

We do not sell your personal information. We share information only in the following limited circumstances:

- **AbleLink applications you use.** When you authenticate through SLM to use an AbleLink web application, SLM passes your name, username, user ID, role, organization ID, and organization name to that application so that it can recognize you and load your account. When an AbleLink mobile or desktop application is licensed through SLM, SLM returns license, organization, and (where applicable) device-user identification information to that application so it can determine what the user is authorized to do. Each application's handling of your data is governed by its own privacy policy.
- **Hosting and infrastructure providers.** SLM and its database are hosted by third-party cloud infrastructure providers located in the United States. These providers supply the underlying compute, storage, and database infrastructure but do not access your data for their own purposes.
- **Email delivery.** When SLM sends a password reset email or a two-factor authentication code, the email is delivered through AbleLink's email infrastructure to the address you have on file.
- **Legal compliance and protection.** We may disclose your information if required to do so by law, or if we believe such action is necessary to comply with legal obligations, protect the rights or safety of our users, or prevent fraud.

4. Cookies

SLM's web interface uses cookies and similar technologies only as necessary for authentication and session management (for example, to keep a web user signed in for the duration of a session, and to remember a device for two-factor authentication purposes if the user has chosen that option). We do not use third-party advertising cookies, analytics trackers, or error-tracking services in SLM.

5. Two-Factor Authentication

Web users may choose to enable email-based two-factor authentication on their account. When two-factor authentication is enabled, after you enter your username and password during sign-in, SLM emails a six-digit verification code to the email address on your account. You must enter that code within ten minutes to complete sign-in. The code is invalidated after a small number of incorrect attempts. Two-factor authentication applies only to web user sign-ins; it does not apply to the licensing flows used by AbleLink mobile and desktop applications.

6. Data Security

We take reasonable measures to protect your information from unauthorized access, alteration, disclosure, or destruction.

- **In transit.** All connections between your browser and SLM's web interface are encrypted using HTTPS/TLS with industry-standard methods and algorithms. Connections from AbleLink mobile and desktop applications to SLM are likewise encrypted.
- **At rest.** Our database is configured with encryption at rest enabled, using industry-standard methods and algorithms. The server file system on which application data (including Endeavor schedule audio recordings and images stored on behalf of device users) is held is also hosted on volumes that are encrypted at rest. Account passwords — for both web users and device users — are not stored; only a one-way password hash is kept, so the password itself cannot be recovered even by us.
- **Access controls.** Access to production systems and data is restricted to authorized personnel.

However, no method of transmission over the Internet, and no method of electronic storage, is completely secure, and we cannot guarantee the absolute security of your data.

7. Data Retention

We retain your information for as long as necessary to provide the service to you, to your organization, or as required by law.

- **Web user account information** is retained for as long as your account is active. When your account is closed, we will securely delete your account information.
- **Device user account information, license records, and device records** are retained for as long as the associated organization holds an active license. Recent device check-in records are retained on a rolling basis (a small number of most-recent entries per device).
- **Endeavor schedule data** stored on behalf of a device user is retained until the device user account is removed, the schedule is replaced by a new upload, or the associated license is closed.
- **Application logs** may be retained for a reasonable period for security, troubleshooting, and audit purposes.

When your SLM account is closed, the AbleLink applications that use SLM will, in turn, delete the application-specific data they hold about you in accordance with their own privacy policies.

8. Your Rights

You have the right to:

- Access, correct, or delete the personal information SLM holds about you
- Change your password at any time
- Disable two-factor authentication on your web user account, or enable it if it is not yet enabled
- Close your SLM account, which will result in the deletion of your SLM account information and trigger the deletion of data held about you by AbleLink applications that use SLM

To exercise any of these rights, please contact us at info@ablelinktech.com.

9. Your California Privacy Rights

This section applies to residents of California and supplements the rest of this Privacy Policy. It is provided pursuant to the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA").

a. Categories of Personal Information We Collect

In the preceding twelve months, SLM has collected the following categories of personal information:

- **Identifiers**, such as name, username, email address, IP address, organization affiliation, device identifiers, and device names.
- **Personal information categories listed in Cal. Civ. Code § 1798.80(e)**, such as account log-in credentials (stored as a one-way hash).
- **Internet or other electronic network activity information**, such as browser type, operating system, login timestamps, failed login counts, application log entries, device check-in timestamps, application versions, and pages visited within SLM.
- **Audio, electronic, or visual information**, specifically audio recordings and images stored on behalf of device users as part of Endeavor schedule data (see Section 1c).
- **Sensitive personal information**, specifically: (i) account log-in credentials for both web users and device users, and (ii) the contents of Endeavor schedules stored on behalf of device users, to the extent that the audio recordings or images they contain may reveal information about the device user's personal life or routines.

We do not knowingly collect biometric information used for identification, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, genetic data, health information, or information about sex life, sexual orientation, or criminal history. We do not analyze the audio or image contents of stored Endeavor schedules; they are stored only to be returned to the device user's authorized Endeavor installations.

b. Sources, Purposes, and Disclosures

SLM collects this information from you directly, from an AbleLink administrator who creates accounts on your behalf, from AbleLink mobile and desktop applications used by or for you, and automatically through your interactions with the service. We use it for the purposes described in Section 2 and disclose it only to the categories of recipients described in Section 3.

c. Sale and Sharing

We do not sell personal information, and we do not share personal information for cross-context behavioral advertising, as those terms are defined under the CCPA. We have not done so in the preceding twelve months.

d. Use of Sensitive Personal Information

We use sensitive personal information only for purposes that the CCPA permits without separate opt-in or opt-out, namely to provide the services you and your organization have requested (including authentication, license validation, and application data storage), to ensure the security and integrity of SLM, and to comply with law. We do not use sensitive personal information to infer characteristics about you.

e. Your Rights and How to Exercise Them

If you are a California resident, you have the right to know, access, correct, and delete your personal information, and the right not to be discriminated against for exercising those rights. To exercise these rights, contact us at info@ablelinktech.com or +1 719.592.0347. We will need to verify your identity before responding to your request.

10. Children's Privacy

SLM is not directed to children under the age of 13, and we do not knowingly collect personal information from children under 13. If you believe we have collected information from a child under 13, please contact us at info@ablelinktech.com so that we can delete it.

11. Users Outside the United States

SLM is hosted in the United States and is intended primarily for users in the United States. If you access SLM from outside the United States, you understand that your information will be transferred to, stored in, and processed in the United States.

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. Any changes will be posted in this document with the "Effective Date" updated. We encourage you to review this Privacy Policy periodically.

13. Contact Us

If you have any questions or concerns about this Privacy Policy or our data practices, please contact us at:

- info@ablelinktech.com
- +1 719.592.0347