Privacy & Security Policy

Last Updated: September 14, 2021

Slash Eureka Inc. DBA Ascend ("**Ascend**," "**we**," "**our**," and/or "**us**") values the privacy of individuals who use our website at useascend.com ("**Site**"). This privacy and security policy (the "**Privacy Policy**") explains how we collect, use, and share information from users of our Site. By using our Site, you agree to the collection, use, disclosure, and procedures this Privacy Policy describes. Beyond the Privacy Policy, your use of our Site is also subject to our Website Terms of Use.

Information We Collect

We may collect a variety of information from or about you or your devices from various sources, as described below.

A. Information You Provide to Us.

Contact Information. If you sign up for notifications or updates, we may ask for your name, company name, work phone number, and email address.

Payment Information. When you add a payment method to your account, a third party service provider that handles payments for us will receive your payment information.

Communications. If you contact us directly, we may receive additional information about you. For example, when you contact our customer support team, we will receive your name, email address, the contents of a message or attachments that you may send to us, information regarding your account such as a policy number, insurance coverage, and other information you choose to provide.

Careers. If you decide that you wish to apply for a job with us, you may submit your contact information and your resume online. We will collect the information you choose to provide on your resume, such as your education and employment experience.

B. Information We Collect When You Use Our Site.

Device Information . We receive information about the device and software you use to access our Site, including IP address, web browser type, operating system version, and device identifiers.

Usage Information. To help us understand how you use our Site and to help us improve it, we automatically receive information about your interactions with our Site, like the pages or other content you view and the dates and times of your visits.

Information from Cookies and Similar Technologies. We and third party partners collect information using cookies, pixel tags, or similar technologies. Our third-party partners, such as analytics partners, may use these technologies to collect information about your online activities over time and across different services. Cookies are small text files containing a string of alphanumeric characters. We may use both session cookies and persistent cookies. A session cookie disappears after you close your browser. A persistent cookie remains after you close your browser and may be used by your browser on subsequent visits to our Site.

Please review your web browser's "Help" file to learn the proper way to modify your cookie settings. Please note that if you delete or choose not to accept cookies from the Site, you may not be able to utilize the features of the Site to their fullest potential.

Call and Text Information. We work with a third party partner to facilitate phone calls and text messages between business users who use our Site. We receive information about these communications, such as the date and time of the call or SMS message, the parties' phone numbers, and the content of any SMS messages.

C. Information We Receive from Third Parties.

Information from third parties. We may receive additional information about you from third parties such as insurance, data, or marketing partners and combine it with other information we have about you.

How We Use the Information We Collect

We use the information we collect:

- To provide, maintain, improve, and enhance our Site;
- To understand and analyze how you use our Site and develop new products, services, features, and functionality;
- To communicate with you, provide you with updates and other information relating to our Site, provide information that you request, respond to comments and questions, and otherwise provide customer support;
- For marketing and advertising purposes, such as developing and providing promotional and advertising materials that may be relevant, valuable or otherwise of interest to you;
- To personalize your experience on our Site such as presenting tailored content;
- To send you text messages;
- To facilitate transactions and payments;
- To find and prevent fraud, and respond to trust and safety issues that may arise;

- For compliance purposes, including enforcing our Terms of Use or other legal rights, or as may be required by applicable laws and regulations or requested by any judicial process or governmental agency; and
- For other purposes for which we provide specific notice at the time the information is collected.

How We Share the Information We Collect

Vendors and Service Providers. We may share any information we receive with vendors and service providers retained in connection with the provision of our Site.

Affiliates. We may share any information we receive with our corporate affiliates for any of the purposes described in this Privacy Policy.

Marketing. We may rent, sell, or share information about you with non-affiliated companies for their direct marketing purposes. To opt out, please email support@useascend.com.

Analytics Partners. We use analytics services to collect and process certain analytics data. These services may also collect information about your use of other websites, apps, and online resources. To help us understand how you use our Site and to help us improve it, we automatically receive information about your interactions with our Site, like the pages or other content you view and the dates and times of your visits. You can learn about Google's practices by going to https://www.google.com/policies/privacy/partners/, and opt-out of them by downloading the Google Analytics opt-out browser add-on, available at https://tools.google.com/dlpage/gaoptout.

As Required By Law and Similar Disclosures. We may access, preserve, and disclose your information if we believe doing so is required or appropriate to: (a) comply with law enforcement requests and legal process, such as a court order or subpoena; (b) respond to your requests; or (c) protect your, our, or others' rights, property, or safety.

Merger, Sale, or Other Asset Transfers. We may transfer your information to service providers, advisors, potential transactional partners, or other third parties in connection with the consideration, negotiation, or completion of a corporate transaction in which we are acquired by or merged with another company or we sell, liquidate, or transfer all or a portion of our assets. The use of your information following any of these events will be governed by the provisions of this Privacy Policy in effect at the time the applicable information was collected.

Consent. We may also disclose information with your permission.

Your Choices

Marketing Communications. You can unsubscribe from our promotional emails via the link provided in the emails. Even if you opt out of receiving promotional messages from us, you will continue to receive administrative messages from us.

Do Not Track. There is no accepted standard on how to respond to Do Not Track signals, and we do not respond to such signals.

Third Parties

Our Site may contain links to other websites, products, or services that we do not own or operate. We are not responsible for the privacy practices of these third parties. Please be aware that this Privacy Policy does not apply to your activities on these third party services or any information you disclose to these third parties. We encourage you to read their privacy policies before providing any information to them.

Security

We make reasonable efforts to protect your information by using physical and electronic safeguards designed to improve the security of the information we maintain. However, as no electronic transmission or storage of information can be entirely secure, we can make no guarantees as to the security or privacy of your information.

Organizational Security

- **Information Security Program:** We have an Information Security Program in place that is communicated throughout the organization. Our Information Security Program follows the criteria set forth by the SOC 2 Framework. SOC 2 is a widely known information security auditing procedure created by the American Institute of Certified Public Accountants.
- **Third-Party Audits:** Our organization undergoes independent third-party assessments to test our security and compliance controls.
- **Third-Party Penetration Testing:** We perform an independent third-party penetration at least annually to ensure that the security posture of our services is uncompromised.
- **Roles and Responsibilities:** Roles and responsibilities related to our Information Security Program and the protection of our customer's data are well defined and documented. Our team members are required to review and accept all of the security policies.
- **Security Awareness Training:** Our team members are required to go through employee security awareness training covering industry standard practices and information security topics such as phishing and password management.
- **Confidentiality:** All team members are required to sign and adhere to an industry standard confidentiality agreement prior to their first day of work.

- **Background Checks:** We perform background checks on all new team members in accordance with local laws.

Cloud Security

- **Cloud Infrastructure Security:** All of our services are hosted with Heroku. They employ a robust security program with multiple certifications. For more information on our provider's security processes, please visit Heroku Security**.**
- **Data Hosting Security:** All of our data is hosted on Heroku databases. These databases are all located in the [United States]. Please reference the above vendor specific documentation linked above for more information.
- **Encryption at Rest:** All databases are encrypted at rest.
- **Encryption in Transit:** Our applications encrypt in transit with TLS/SSL only.
- **Vulnerability Scanning:** We perform vulnerability scanning and actively monitor for threats.
- **Logging and Monitoring:** We actively monitor and log various cloud services.
- **Business Continuity and Disaster Recovery:** We use our data hosting provider's backup services to reduce any risk of data loss in the event of a hardware failure. We utilize monitoring services to alert the team in the event of any failures affecting users.
- **Incident Response:** We have a process for handling information security events which includes escalation procedures, rapid mitigation and communication.

Access Security

- **Permissions and Authentication:**
    - Access to cloud infrastructure and other sensitive tools are limited to authorized employees who require it for their role.
    - Where available we have Single Sign-on (SSO), 2-factor authentication (2FA) and strong password policies to ensure access to cloud services are protected.
- **Least Privilege Access Control:** We follow the principle of least privilege with respect to identity and access management.
- **Quarterly Access Reviews:** We perform quarterly access reviews of all team members with access to sensitive systems.
- **Password Requirements:** All team members are required to adhere to a minimum set of password requirements and complexity for access.
- **Password Managers:** All company issued laptops utilize a password manager for team members to manage passwords and maintain password complexity.

Vendor and Risk Management

- **Annual Risk Assessments:** We undergo at least annual risk assessments to identify any potential threats, including considerations for fraud.
- **Vendor Risk Management:** Vendor risk is determined and the appropriate vendor reviews are performed prior to authorizing a new vendor.

Children's Privacy

We do not knowingly collect, maintain, or use personal information from children under 13 years of age, and no part of our Site is directed to children. If you learn that a child has provided us with personal information in violation of this Privacy Policy, then you may alert us at hello@useascend.com.

International Visitors

Our Site is hosted in the United States and intended for visitors located within the United States. If you choose to use the Site from the European Union or other regions of the world with laws governing data collection and use that may differ from U.S. law, then please note that you are transferring your personal information outside of those regions to the United States for storage and processing. Also, we may transfer your data from the U.S. to other countries or regions in connection with storage and processing of data, fulfilling your requests, and operating the Site. By providing any information, including personal information, on or to the Site, you consent to such transfer, storage, and processing.

Changes to this Privacy Policy

We will post any adjustments to the Privacy Policy on this page, and the revised version will be effective when it is posted. If we materially change the ways in which we use or share personal information previously collected from you through the Site, we will notify you through the Site, by email, or other communication.

Contact Information

If you have any questions, comments, or concerns about our processing activities or if you wish to report a potential security issue, please email us at hello@useascend.com or security@useascend.com. You can also write to us at:

Slash Eureka Inc.
955 Alma St. Suite C Palo Alto, CA 94301