

Privacy Policy & Cookie Notice

EFFECTIVE: October 19, 2026 · VERSION 2026-10-19.1

1. SCOPE; RESPONSIBLE ORGANIZATION

1.1. Scenic City Studios, LLC (“SCS,” “we,” “us,” or “our”) explains in this Privacy Policy how information is handled through the Website and enabled development, hosting, maintenance, email, software, Company Builder, AI, automation, and support Services. Practices depend on the Service actually used. A description of an available feature does not mean it is active on every page.

1.2. This notice distinguishes the new2026 Website’s practices from processing under separate customer agreements and older SCS properties. It does not replace a customer’s privacy notice or a required data-processing agreement. Acknowledgment means receipt of this notice; it is not a release of claims, a waiver of privacy rights, or unrestricted consent. Contractual allocations of responsibility are addressed in the Terms and applicable Orders, subject to law.

2. INFORMATION YOU PROVIDE

2.1. We receive information you submit, including name, email, telephone, business identity, website, address, billing contact, service requests, messages, company profile, industry, service area, and uploaded logos, images, or documents. We may also receive account preferences, support communications, project approvals, and instructions necessary for agreed Services.

2.2. Customer-directed Services may process website content, prompts, approved knowledge materials, configuration, customer or prospect details, form submissions, chat conversations, and generated output. Submit only information you are authorized to provide. The general Website forms are not intended for passwords, live card details, health records, government identifiers, or other highly sensitive data.

3. TECHNICAL INFORMATION; SOURCES

3.1. Hosting and application systems may record IP addresses, request times, browser or device information, requested URLs, security events, and diagnostic errors. The new2026 agreement system records the actual IP address observed by the server together with its likely network-provider label and ASN, if available. Inquiry forms separately use keyed network hashes for abuse prevention. Each affirmative terms, privacy, or combined agreement also stores an acceptance snapshot with the request IP address, a one-way cookie-token fingerprint, browser and language information, browser-reported time zone when available, timestamp, and exact policy version and document hashes. We estimate country, region, city, and approximate geographic coordinates using a locally hosted DB-IP City Lite database. We retain the estimate, lookup status, source, and database date with that event. These coordinates represent an IP-location estimate, not GPS, a verified residence, or proof of identity. VPNs, proxies, shared connections, and mobile networks can affect accuracy. Visitor IPs are not sent to an external geolocation service for this lookup. Older acceptances may not contain location data. These agreement records follow our agreement-record retention practices, not the AI tools’ 30-day result deletion schedule.

3.2. Information comes from your direct submissions, necessary browser requests, your authorized users, customer-provided materials, and integrations you enable. Depending on the agreed Service, providers may supply transaction status, support events, or diagnostic information. This new2026 Website does not currently load advertising pixels, social tracking embeds, or analytics cookies.

3.3. For email and hosting Services, operational records may include sender and recipient addresses, timestamps, message-routing and delivery information, authentication results, mailbox access events, forwarding settings, spam or malware classifications, and abuse reports. Message bodies, attachments, and mailbox contents are processed to the extent required by the selected Service, authorized support, legitimate security activity permitted by law, or legal obligations. We do not represent that personnel read every message or that every message is screened successfully.

4. PURPOSES AND PROCESSING BASIS

4.1. We use information to respond to requests; prepare and perform agreements; administer accounts and billing; deliver and support enabled Services; maintain security; prevent abuse; preserve approvals and acceptance records; resolve disputes; and comply with legal obligations. We use relevant inputs for an AI or automation job only when that feature is enabled or instructed.

4.2. Where a law requires an identified lawful basis, processing may be necessary for requested precontractual steps or a contract, compliance with law, legitimate operational and security interests subject to applicable balancing requirements, or specific consent where required. Website acceptance does not replace a separate consent required for optional tracking, marketing, or sensitive-data processing.

5. CUSTOMER DATA; CONTROLLER AND PROCESSOR ROLES

5.1. SCS generally determines the purposes of information collected for its own inquiries, business relationships, security, and acceptance records. For information collected by a customer through its own website or business, that customer ordinarily determines the purposes and instructs SCS to act as a service provider or processor.

5.2. The customer must establish appropriate notices, permissions, and lawful instructions. Requests concerning data controlled by a customer may need to be directed to that customer; SCS will assist as required by its agreement and applicable law. Roles are determined by actual activities and law, not solely by the labels in this policy.

5.3. Customer responsibility for end-user notices does not remove SCS's own duties under applicable law. Access to hosted communications is limited to legally permitted purposes and authorized roles; a customer cannot authorize unlawful access to another person's communications. A request for account investigation or fraud assistance may require verification of identity and authority.

6. WEBSITE FORMS; FILES; PAYMENT INFORMATION

6.1. General inquiries are saved privately and sent to the relevant SCS contact. Billing, company, sample payment, and upload submissions in new2026 are routed to accounts@sceniccitystudios.com. Uploaded files are kept outside the public website directory. Notification emails contain private download links that expire after seven days; link expiration does not itself delete the stored file.

6.2. THE NEW2026 PAYMENT FORM IS TEST-ONLY. IT ACCEPTS ONLY THE DISPLAYED SAMPLE CARD NUMBER AND SAMPLE SECURITY CODE, EMAILS THOSE SAMPLE DETAILS, AND DOES NOT CHARGE A CARD. DO NOT ENTER REAL CARD OR BANK INFORMATION. Where an actual paid Service uses Stripe or another authorized processor, the processor handles the payment information under its own notices; SCS may receive billing identity, processor references, invoice details, and payment status.

7. AI AND AUTOMATION PROVIDERS

7.1. For an enabled AI job, relevant prompts, reference material, communications, or content may be transmitted to the provider used for that function. Consider whether each input is necessary and appropriate before submission. Provider locations, retention, and permitted uses depend on the applicable provider and configuration; do not assume all providers offer identical privacy terms.

7.2. Customer-specific retention, training restrictions, approved providers, regulated-data handling, or transfer requirements must be addressed in the relevant agreement or configuration before use. SCS does not promise that a general notice alone provides those controls. Generated output may be inaccurate and requires appropriate human review. Master API keys and internal credentials remain restricted.

8. DISCLOSURES; SERVICE PROVIDERS

8.1. We disclose information reasonably needed by hosting, storage, email, security, domain, payment, AI, technical support, and professional service providers involved in the requested Services. Appropriate restrictions are applied according to the provider's role, the agreement, and applicable law. A provider acting independently may have its own notice and legal duties.

8.2. Information may also be disclosed at your direction, to respond to lawful process, protect rights or safety, investigate abuse, or carry out a merger or business transfer subject to applicable protections. We do not describe every transfer as consent-based; mandatory disclosure obligations may apply independently. Public website information that you direct us to publish becomes accessible to others.

8.3. Where reasonably necessary and legally permitted, relevant logs or communications may be shared with the affected authorized customer, infrastructure or security providers, legal advisers, insurers, financial institutions, or competent authorities to investigate an incident, respond to legal process, mitigate fraud, or establish or defend legal claims. Disclosure is limited by applicable communications-privacy law, confidentiality duties, legal process requirements, and the information reasonably needed for the purpose. This is not blanket consent to disclose every mailbox or message.

9. SALE; SHARING; TARGETED ADVERTISING

9.1. The new2026 Website has no advertising or cross-site analytics tracking enabled, and its acceptance mechanism does not enroll visitors in targeted advertising. Acceptance records are maintained for agreement administration and security, not as a marketing list.

9.2. This notice does not establish identical practices throughout every SCS property. Other SCS pages, customer sites, and separately enabled campaigns may have their own technologies and notices. Before optional advertising technology is introduced here, its purposes and choices must be separately disclosed and any required consent obtained.

9.3. Where applicable law treats a disclosure as a sale, sharing, or targeted advertising, you may exercise the corresponding opt-out right. Contact support@sceniccitystudios.com. The new2026 Website does not activate those activities even when a browser sends no opt-out signal.

10. ESSENTIAL COOKIE NOTICE

10.1. The first-party scs2026 session cookie supports request security for consent and forms. Consent requests run only on the homepage; forms on other pages may independently use their necessary session cookie. The scs2026_accept cookie contains a random browser-recognition token and is placed when the choice interface loads, before a decision is made. Its server record initially indicates pending, not accepted. It can subsequently remember declined, partially accepted, or fully accepted choices. Both cookies are scoped to /, Secure, HttpOnly, and SameSite=Lax. The AI tools also set scs_ai_visitor, an essential random browser identifier with Secure, HttpOnly, SameSite=Lax attributes and root scope, renewed for up to 365 days when the tool is used. It helps enforce per-feature usage limits.

10.1A. The domain-services pages additionally use the first-party scsdomains session cookie to secure forms, prevent repeat submissions, and associate a service request with its browser session. It is scoped to / with Secure, HttpOnly, and SameSite=Lax attributes. Booking and other forms may use the existing necessary scs2026 session independently of the homepage choice prompt.

10.2. The recognition cookie expires no later than 365 days after creation; the session cookie lasts for the browser session subject to server cleanup. A changed IP, cleared or expired cookie, or revised policy requires a fresh choice. Shared IP addresses are not used alone to recognize another visitor's consent. Cookies contain no name or email.

10.3. Only essential session, choice-recognition, and AI usage-limit cookies are used here. No advertising or analytics cookies are enabled by YES. NO records refusal and takes you to the policy/options page; the homepage still requires agreement; other pages remain accessible without this consent check. Reading and printing the policies remain available without agreement. Browser settings can delete or block the necessary cookies, which may cause repeated prompts or prevent secure choice recording. Consent in the footer returns you to the homepage to inspect or change your choice.

11. ACCEPTANCE AND AUDIT RECORDS

11.1. The agreement mechanism records a random browser-token hash, the actual IP address seen by the server, a likely network owner/provider label and ASN when available, current policy identifiers and document hashes, creation and choice timestamps, and pending/declined/individual/full-agreement states. It does not ask for name or email. Those details may still be collected through separate inquiry/account forms, or retained in historical acceptance records created under earlier versions.

11.2. Provider lookup uses a locally downloaded bulk IPtoASN database. No visitor IP is sent to a third-party lookup service. Network ownership is an estimate, not verified identity, a traceroute, or a confirmed first hop. An unavailable match is reported as Not identified. VPNs, proxies, shared IPs, and changes in routing can affect accuracy.

11.3. Only an explicit YES on the homepage records new affirmative agreement. Merely setting a cookie, loading a page, or scrolling does not. Homepage consent checks and YES or NO choices are logged as distinct activity events, including timestamps, browser-provided user agent and language, IP address, estimated provider and ASN, browser reference, and policy version. Historical individual-policy decisions are preserved. These records are used for agreement administration and security, not as authorization for marketing or charging a payment method.

12. RETENTION; DELETION; EXPORT

12.1. Information is retained according to its purpose, the customer relationship, service configuration, legal duties, security needs, and disputes. Inquiries and uploads are retained while reasonably needed for the request or account. Billing and acceptance evidence may remain after a cookie expires or a Service ends when needed for accounting, compliance, or the establishment or defense of claims. Cookie expiration is not a promise that the underlying records have been deleted.

12.2. We do not state a single universal deletion period for all Services. A verified deletion request is evaluated against applicable retention requirements and exceptions. Active-system deletion may precede expiration from backups or restricted logs. Any retained information remains subject to appropriate restrictions. Customer exports are subject to technical feasibility and applicable agreements, but exercising a statutory privacy right is not conditioned on payment of an unrelated invoice.

12.3. Relevant information may be retained beyond an ordinary deletion schedule where reasonably necessary for an identified security investigation, reasonably anticipated or pending litigation, a legal preservation duty, insurance claim, regulatory matter, or defense of legal rights. Access is restricted and retention is reviewed as the need changes. Such an exception is not a promise that every record exists or will be retained indefinitely, and does not authorize destruction contrary to an applicable legal hold.

12.4. Ordinary email hosting is not a litigation archive unless expressly agreed. Customers must identify applicable recordkeeping requirements and request an appropriate retention or preservation arrangement. We evaluate lawful preservation requests according to their scope, authority, technical availability, applicable agreements, and law. Deletion or export requests do not automatically override preservation duties or the rights of other individuals.

13. SECURITY; INCIDENTS

13.1. The new2026 implementation uses measures appropriate to particular functions, such as HTTPS, access-restricted storage, prepared database queries, form tokens, upload-type checks, and signed time-limited result or download links. Some functions use request limits; not every function has identical controls. These measures reduce risk but do not make information invulnerable. Transport encryption does not establish the identity or honesty of a sender or recipient; file-type validation does not guarantee a malware-free file.

13.2. Access is limited according to operational need. You should protect your email account, devices, and any received download links. If a security incident creates a notification duty, SCS will investigate and provide notices required by applicable law or contract. We do not promise that all events, attacks, or unauthorized access can be prevented.

13.3. Suspected account compromise, phishing, or an unauthorized payment instruction may be reported to support@sceniccitystudios.com or by calling (423) 401-8394 using independently verified contact details. Provide relevant facts and message headers without unnecessary sensitive data. We may request verification before discussing an account or disclosing records. Notification, investigation, preservation, and cooperation duties are determined by applicable law, the incident facts, and any controlling agreement; acknowledging this policy does not waive them.

13.4. Keep credentials, devices, and private links secure. Independently verify unusual payment or credential requests through a trusted channel. A message's transit through SCS servers, apparent SCS or customer sender address, or successful authentication checks does not establish that it is legitimate. These recommendations and contractual customer duties do not shift statutory responsibility away from SCS for its own conduct.

14. INTERNATIONAL PROCESSING

14.1. SCS operates in the United States. Depending on the Service and its providers, information may be processed in other countries with different legal protections. Where transfer restrictions apply, an appropriate permitted mechanism or safeguard is required. Merely accepting this policy is not presented as a substitute for every legally required transfer safeguard.

14.2. Customers with geographic, residency, or regulated processing requirements must identify those requirements before enabling the relevant Service so the parties can assess appropriate contractual and technical measures.

15. INDIVIDUAL RIGHTS; VERIFICATION; APPEALS

15.1. Depending on your residence, the information involved, and whether the relevant law applies, you may have rights to know or access information, receive a portable copy, correct inaccuracies, request deletion, restrict or object to processing, withdraw specific consent, opt out of sale/sharing/targeted advertising or certain profiling, limit qualifying sensitive-data uses, and appeal a denied request.

15.2. Send requests to support@sceniccitystudios.com or call (423) 401-8394. Identify your request and the website or relationship involved without sending unnecessary sensitive identifiers. We may request information reasonably needed to verify identity and an authorized agent's authority. We respond within applicable legal periods, explain permissible refusals, and provide any required appeal process. To appeal, reply to the decision or email support with "Privacy appeal." You may also complain to the regulator with authority over your matter.

15.3. We will not unlawfully discriminate for exercising an applicable privacy right. Exceptions may permit retention for security, accounting, legal duties, or claims. Withdrawal affects consent-based future processing and does not invalidate lawful earlier processing. It does not automatically cancel a separate contract or erase evidence necessary to administer it.

16. CALIFORNIA AND OTHER REGIONAL DISCLOSURES

16.1. Where applicable, categories described here include identifiers and contact details; commercial and billing records; internet or network activity; submitted content and communications; and business or professional information. Sources, purposes, recipients, and retention criteria are described in Sections 2–12. Not every category is collected from every person, and the sample payment form is not a live payment collection channel.

16.2. The new2026 Website does not sell acceptance records or share them for cross-context behavioral advertising. Information about historical advertising activity or other SCS properties should be requested from the privacy contact; this policy does not fabricate a retrospective twelve-month activity report. Legally required supplemental disclosures will be supplied where applicable. Rights depend on the law’s coverage and exceptions, including any business-contact or employment provisions.

17. CHILDREN; COMMUNICATION PREFERENCES

17.1. The Website is intended for businesses and authorized adults, not children under 13. Do not knowingly submit children’s personal information through these general forms. If you believe a child has supplied information, contact support@sceniccitystudios.com so we can evaluate and take appropriate action.

17.2. Acceptance of these policies is not promotional consent. You can opt out of marketing through the message’s unsubscribe method or by contacting SCS. Necessary replies, billing, security, and service notices may continue while relevant to the relationship. Unsubscribing from marketing does not itself cancel a paid Service.

18. OTHER WEBSITES; CHANGES; CONTACT

18.1. External links, customer websites, independently operated providers, and older SCS pages may have different practices. Review the notice for the service you actually visit. This new2026 consent record does not automatically establish consent on a separate website.

18.2. We identify revisions by effective date and version and provide additional notice or seek new consent when required. The new2026 mechanism requests acceptance again when its policy version changes. We do not retroactively convert an earlier acknowledgment into authorization for materially different undisclosed uses.

18.3. Privacy requests: support@sceniccitystudios.com. General and legal inquiries: info@sceniccitystudios.com. Account matters: accounts@sceniccitystudios.com. Telephone: (423) 401-8394. Responsible organization: Scenic City Studios, LLC. Please identify the relevant account or website and provide a reliable reply address.

19. WEBSITE CONCEPTS AND VISIBILITY REPORTS

19.1. When you use the website redesign tool, we process your company name, current website address, and uploaded logo. We discover and scan publicly accessible pages and sitemaps, then provide the resulting website content, company details, and logo to OpenAI to plan and generate concept artwork. Submit only a website and logo you are authorized to provide for this purpose, and do not include confidential or sensitive personal information. Scans are subject to page, time, and content limits.

19.2. When you request a visibility report, we process the company name, public website address, and state you provide. Our server retrieves a limited set of public website pages, and OpenAI researches publicly available business information. Website content and public business information may be transmitted to OpenAI for this purpose.

19.3. After an AI-tool request is queued, you may optionally provide your name and email address to receive the completed design or report. You may instead wait and view the result in the requesting browser without providing contact details. When you request email delivery, we store your details with the request, send private result links to your supplied address, and provide the request and results to Derek at Scenic City Studios for potential follow-up about the findings and related services. This action does not subscribe you to a mailing list. This is separate from cookie or policy acceptance; the cookie prompt does not request your name or email.

19.4. We use an essential session cookie to associate a request and its private output with your browser. We retain a keyed hash of the requesting IP address for usage limits and abuse prevention. Tool inputs, uploaded logos, generated concepts, reports, and associated lead records are scheduled for deletion from the tool database and storage after 30 days.

Copies sent to our mailbox are retained under our communication-retention practices. OpenAI processing is subject to its applicable service terms and data-retention practices. Separate per-feature usage counters retain keyed hashes of the browser identifier and IP address, attempt counts, and an update timestamp while the complimentary-tool limit remains in effect; they are not deleted with the 30-day result records. Each feature allows three queued requests, with no automatic reset. Either the browser or IP reaching the limit prevents further requests, including on shared networks. Invalid submissions do not count; queued requests that later fail do count. These counters are not consent records and contain no names, emails, logos, or website content.

19.5. You can print or save a report and download a concept during its availability period. Browser-only access may be lost if your session expires or its cookies are removed. If you requested email delivery, a private bearer link can provide access until the 30-day request-retention period expires. Anyone with that link can view the result, so share it only with intended recipients. Contact us for privacy questions or requests concerning your submitted information.

20. CONSULTATION BOOKINGS AND CALENDARS

20.1. Consultation requests collect the contact details and message submitted, requested meeting time, request status, and operational approval and notification records. Relevant details are sent to the designated SCS recipient and used to coordinate the requested meeting. A request is not a confirmed appointment until approved.

20.2. Availability calculations use configured calendar feeds and existing booking records. Connected feeds may contain event details; the public calendar presents availability rather than the contents of private events. Administrators can use an add-to-calendar link that supplies meeting details to Google when opened; completing that action is subject to Google's practices. Booking records are retained as reasonably needed for scheduling, customer follow-up, administration, security, and legal obligations; the AI tools' 30-day schedule does not automatically apply to booking records.

21. DOMAIN SERVICES AND REGISTRAR PROCESSING

21.1. A domain availability query sends the requested domain name to NameSilo through SCS's server. Customer requests collect the domain, service type, name, email, optional phone number, message, request time, and status; they are stored in access-restricted records and emailed to the designated SCS contact. A domain-services session and keyed network identifier support form security, duplicate prevention, and abuse controls.

21.2. If you authorize a domain transaction, relevant registrant, contact-profile, domain, DNS, transaction, and authorization information is provided to NameSilo and, where necessary, the registry or other authorized providers. Registrars may act independently under their own terms, policies, and legal requirements, including registration-data disclosure rules. WHOIS privacy availability varies by extension and does not prevent legally required access or disclosure.

21.3. Public requests do not collect customer card numbers, perform checkout, or automatically purchase domains. Registrar credentials and transfer authorization codes are restricted to administrative functions. Domain requests and action records are retained as reasonably needed for fulfillment, support, ownership and authorization evidence, security, accounting, and legal obligations; they are not subject to the AI tools' automatic 30-day schedule.

22. FIRST-PARTY SITE ACTIVITY AND INTERNAL REPORTS

22.1. We measure public-page visits, approximate visitor counts, device categories, time-of-day patterns, and active time on visible, focused pages with recent interaction. Our server derives a keyed hash from the network IP address and browser user agent to estimate repeat visits; the activity table does not retain the raw IP address or full user-agent string. Page paths are recorded without query strings, form contents, or private link tokens. A random per-page event identifier exists only in page memory. No additional analytics cookie or browser-storage identifier is set. Estimates may combine people on shared networks or split a person across browsers or networks. We do not infer or collect visitor age through this measurement.

22.2. Activity measurement excludes recognized bots and honors browser Do Not Track and Global Privacy Control signals. Blocking scripts, closing a page, idle time, or connectivity interruptions can limit measurements. Domain availability attempts record the requested domain, time, and result or unavailable status. These activity records are separate from the agreement-evidence and security records described above.

22.3. Authorized studio administrators receive internal daily, weekly, or monthly summaries containing activity totals, popular pages and hours, device categories, domain lookups, and website-tool requests. Tool entries may include the company, website, submitted name and email, request state, delivery status, and administrator-only links to generated

reports or graphics. These summaries support service operation and requested follow-up, not an automatic marketing-list subscription.

22.4. Activity measurements, domain-lookup logs, internal report snapshots, and private administrative copies of generated outputs and associated tool contact details are retained for up to 90 days in ordinary operation. Public tool results and their public bearer links retain the separate 30-day availability period. Report emails are retained under our mailbox retention practices. Administrator archive links require sign-in and cease working after archive expiration. Contact support@sceniccitystudios.com about privacy choices or access/deletion requests.

END OF PRIVACY POLICY & COOKIE NOTICE · 2026-10-19.1