SYYCLOPS, INC.
PRIVACY POLICY

Last Updated: February 13, 2026

1. Introduction

Syyclops, Inc. ("Syyclops," "we," "our," or "us") is a Delaware corporation with its principal place of business in Washington, DC. We are committed to protecting the privacy and security of the personal data entrusted to us through our website (syyclops.com), applications, digital twin platform, and related services (collectively, the "Services").

This Privacy Policy explains how we collect, use, disclose, retain, and safeguard personal information. By accessing or using the Services, you acknowledge that you have read and agree to the practices described herein. If you do not agree, you must discontinue use of the Services immediately. This Privacy Policy is incorporated into and subject to our Terms of Service.

2. Personal Data We Collect

2.1 Information You Provide

- **Account Information:** Name, email address, password, organization name, job title, billing address, and payment details.
- **Service Data:** Data, files, text, images, building models, equipment data, sensor readings, telemetry, or other materials you upload to or generate within the Services. This includes building information models (BIM), CAD files, maintenance records, work orders, and IoT/BAS telemetry data. You are solely responsible for the accuracy, completeness, legality, and quality of all Service Data.
- **Communications:** Messages sent to Syyclops through support channels, surveys, or feedback forms.

2.2 Information Collected Automatically

- **Usage Data:** Features used, session duration, actions taken, pages viewed, search queries, and interaction patterns.
- **Log Data:** IP address, browser type, operating system, device identifiers, referring URLs, and date/time stamps.
- **Location Data:** Approximate geographic location derived from IP address only. We do not collect precise geolocation unless you explicitly enable it and may disable it at any time.
- **Cookies and Similar Technologies:** See Section 11 (Cookies and Tracking).

2.3 Information from Third Parties

- **Integrations:** Data received from third-party services you connect to the Services, including SSO providers, building automation systems (BAS), CMMS platforms, IoT gateways, and payment processors. Syyclops is not responsible for the privacy practices of third-party services.
- **Public Sources:** Information from publicly available databases or professional networks, as permitted by applicable law.

2.4 IoT and Sensor Data

The Services may receive real-time or periodic data from IoT devices, BACnet gateways, and building sensors installed at your facilities. This telemetry data (temperature readings, equipment status, energy consumption, occupancy data, etc.) is classified as Service Data and governed accordingly. Syyclops does not control, operate, or maintain on-premise IoT devices or gateways; responsibility for their security, maintenance, and proper configuration rests with the Subscriber. Syyclops's obligations are limited to data received after secure transmission to the Services.

3. Artificial Intelligence and Automated Processing

3.1 AI-Powered Features

The Services incorporate artificial intelligence and machine learning capabilities ("AI Features") to provide analytics, recommendations, anomaly detection, predictive maintenance insights, natural language interfaces, and other functionality. AI Features may include large language models (LLMs), machine learning classifiers, computer vision, and other algorithmic analysis.

3.2 AI Disclosure

Syyclops discloses that the following categories of AI Features are currently embedded in the Services:

- **Analytics and Insights:** AI-driven analysis of building performance, equipment health, and energy consumption patterns.
- **Natural Language Processing:** AI chatbots and query interfaces for interacting with facility data.
- **Anomaly and Fault Detection:** Automated identification of deviations from expected system behavior.
- **Predictive Maintenance:** Forecasting of equipment failures and maintenance needs based on historical and real-time data.

The specific AI Features available may vary by subscription tier and are described in the applicable Documentation.

3.3 Third-Party AI Providers

Certain AI Features are powered by third-party AI providers, which may include OpenAI, Anthropic, Google, or other providers as updated from time to time. When data is processed by third-party AI providers: (a) we share only the minimum data necessary to deliver the requested feature; (b) we anonymize and de-identify inputs where technically feasible; (c) we contractually prohibit third-party AI providers from using your data for purposes other than delivering the requested service; and (d) such providers process data under their own terms and privacy policies. A current list of third-party AI providers is available upon written request to privacy@syyclops.com.

3.4 AI Model Training

Syyclops may use de-identified and aggregated Service Data and Usage Data to train, improve, and develop AI models that power the Services. Such data will be processed so that it cannot reasonably identify any individual Subscriber, Authorized User, or data subject. Syyclops will not use identifiable Service Data to train or fine-tune AI models without the Subscriber's prior written consent. Subscribers who wish to opt out of all AI processing of their Service Data (including de-identified and aggregated use) may submit a written request to privacy@syyclops.com; Syyclops will honor such requests, provided that opting out may limit or disable certain AI-powered features.

3.5 AI Output Disclaimer

AI-GENERATED OUTPUTS, INCLUDING ANALYTICS, RECOMMENDATIONS, PREDICTIONS, AND INSIGHTS, ARE PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND ARE NOT GUARANTEED TO BE ACCURATE, COMPLETE, OR RELIABLE. AI FEATURES ARE TOOLS TO ASSIST HUMAN DECISION-MAKING AND DO NOT REPLACE PROFESSIONAL ENGINEERING JUDGMENT, BUILDING CODE COMPLIANCE ANALYSIS, OR QUALIFIED EXPERT ASSESSMENT. SYYCLOPS DISCLAIMS ALL LIABILITY FOR DECISIONS MADE OR ACTIONS TAKEN BASED ON AI-GENERATED OUTPUTS. SUBSCRIBERS ARE SOLELY RESPONSIBLE FOR INDEPENDENTLY VERIFYING AI OUTPUTS BEFORE RELYING ON THEM FOR OPERATIONAL, MAINTENANCE, SAFETY, OR COMPLIANCE DECISIONS.

4. How We Use Personal Data

- **Operating the Services:** Delivering platform functionality, processing transactions, providing support.
- **AI Processing:** Powering AI Features as described in Section 3.
- **Communications:** Transactional messages (invoices, security alerts, service notifications) and, where permitted, promotional communications. You may opt out of promotional communications at any time by emailing privacy@syyclops.com. All commercial emails comply with the CAN-SPAM Act

(15 U.S.C. §7701 et seq.), including accurate header information, clear identification as advertising, a functioning unsubscribe mechanism, and a valid physical postal address.

- **Improving the Services:** Anonymized and aggregated analytics to develop features and improve functionality.
- **Security and Fraud Prevention:** Detecting and preventing unauthorized access, security incidents, and abuse.
- **Legal Compliance:** Complying with applicable laws, regulations, legal processes, and governmental requests.
- **Personalization:** Tailoring features and recommendations to usage patterns.

5. How We Share Personal Data

We do not sell personal information. We do not "sell" or "share" (as those terms are defined under the California Consumer Privacy Act) personal information for monetary or other valuable consideration, and have not done so in the preceding twelve (12) months. We may disclose personal data to the following categories of recipients for the business purposes described in this Privacy Policy:

- **Service Providers and Contractors:** Third-party vendors who process data on our behalf to operate, secure, and improve the Services. These include cloud hosting providers, payment processors, analytics services, communications platforms, AI/ML providers, and security monitoring services. All service providers and contractors are bound by written agreements that: (i) specify the business purpose for processing; (ii) prohibit selling or sharing the data; (iii) prohibit use for purposes other than those specified; and (iv) require compliance with applicable data protection laws.
- **Business Transfers:** In connection with a merger, acquisition, reorganization, sale of assets, or bankruptcy.
- **Legal and Safety:** To comply with laws, legal processes, or governmental requests; to enforce our Terms of Service; to protect the rights, property, or safety of Syyclops, our users, or the public.
- **Affiliates:** Companies under common ownership or control, subject to this Privacy Policy.
- **At Your Direction:** When you instruct us through third-party integrations or other user-directed actions.

6. Data Retention

We retain personal data only as long as necessary for the purposes described in this Privacy Policy or as required by law. Specific retention periods:

Data Category	Retention Period	Legal Basis
Account information	Duration of account + 1 year	Contract performance; legal compliance
Service Data (customer content)	Duration of subscription + 30-day export, then deleted within 60 days	Contract performance; customer instructions
Usage Data	Up to 3 years (anonymized/aggregated)	Legitimate interest in improving Services
Log and security data	Minimum 12 months	Security; legal compliance; incident response
Payment and billing records	7 years from transaction	Tax and legal compliance (26 U.S.C.)
Support communications	3 years from resolution	Service improvement; dispute resolution
AI training data (de-identified)	Indefinite (cannot be traced to individuals)	Legitimate interest; product improvement

When personal data is no longer needed, we delete or anonymize it using commercially reasonable methods. Residual copies in backup systems are overwritten per our standard rotation schedule (not to exceed 180 days). Syyclops retains the right to retain data as necessary to comply with legal holds, regulatory investigations, or pending or anticipated litigation.

7. Data Security

Syyclops maintains commercially reasonable administrative, technical, and physical safeguards designed to protect personal data, including:

- **Access Controls:** Centralized IAM with MFA, RBAC, and least-privilege principles.
- **Encryption:** TLS 1.2+ in transit; AES-256 or equivalent at rest.
- **Infrastructure:** Cloud-native architecture, network segmentation, vulnerability scanning, and penetration testing.
- **Incident Response:** Documented plan tested and updated at least annually (see Section 9).
- **Personnel:** Background checks, security awareness training, and confidentiality obligations.
- **Vendor Management:** Risk assessments for providers with access to personal data.
- **Business Continuity / Disaster Recovery:** Syyclops maintains a documented disaster recovery and business continuity plan that includes regular data backups, tested restoration procedures, geographically distributed redundancy, and defined recovery time and recovery point objectives. The DR/BC plan is reviewed and updated at least annually.

WHILE SYYCLOPS IMPLEMENTS COMMERCIALLY REASONABLE SAFEGUARDS, NO SYSTEM IS COMPLETELY SECURE. SYYCLOPS DOES NOT WARRANT OR GUARANTEE THE ABSOLUTE SECURITY OF ANY DATA AND SHALL NOT BE LIABLE FOR UNAUTHORIZED ACCESS RESULTING FROM CAUSES BEYOND SYYCLOPS'S REASONABLE CONTROL, INCLUDING BUT NOT LIMITED TO SUBSCRIBER'S FAILURE TO MAINTAIN ADEQUATE SECURITY OF ITS OWN SYSTEMS, CREDENTIALS, OR ON-PREMISE DEVICES.

8. Sub-Processors

Syyclops engages the following categories of sub-processors:

- **Cloud Infrastructure:** Hosting and storage (e.g., AWS, Google Cloud, Microsoft Azure).
- **Payment Processing:** Billing and payment transactions.
- **Analytics:** Usage Data collection and analysis.
- **Communications:** Transactional and promotional email delivery.
- **AI/ML Providers:** Processing for AI-powered features (see Section 3.3).
- **Security and Monitoring:** Threat detection, logging, and incident response support.

A current list of named sub-processors is available upon written request to privacy@syyclops.com. Syyclops will provide at least thirty (30) days' notice before engaging a new sub-processor. Enterprise customers under an MSA may exercise objection rights per their agreement. Syyclops is responsible for the acts and omissions of its sub-processors to the same extent as if Syyclops were performing the services directly.

9. Security Incident Notification

If Syyclops confirms a security incident involving unauthorized access to, acquisition of, or disclosure of personal data, Syyclops will: (a) notify affected Subscribers within seventy-two (72) hours of confirmation via email to the account owner or designated security contact; (b) describe the nature, categories, and approximate volume of data affected (to the extent known); (c) identify Syyclops's point of contact; (d) describe likely consequences and measures taken or proposed; and (e) provide reasonable updates as information becomes available. Syyclops will notify applicable regulatory authorities as required by law. Notification is not an acknowledgment of fault or liability. Syyclops's obligation to notify does not extend to incidents caused by the Subscriber's own systems, credentials, on-premise equipment, or Authorized Users.

10. Digital Twin and IoT Data Practices

10.1. Data Accuracy. The quality, accuracy, and reliability of digital twin outputs depend entirely on the quality, accuracy, and completeness of the data provided by the Subscriber, including building information models, sensor feeds, maintenance records, and system configurations. Syyclops does not independently verify the accuracy of Subscriber-provided data and assumes no responsibility for errors, omissions, or inaccuracies in such data or any resulting digital twin outputs.

10.2. Physical Systems. The Services create digital representations of physical building systems but do not directly control, operate, or modify any physical equipment, HVAC systems, electrical systems, plumbing, fire

protection, or other building infrastructure. Any operational decisions or actions taken based on information provided through the Services are the sole responsibility of the Subscriber and its qualified personnel.

10.3. On-Premise Devices. Where the Services require installation of on-premise hardware (e.g., BACnet gateways, IoT collectors), the Subscriber is solely responsible for: (a) physical security of the device; (b) network segmentation and access controls on the Subscriber's local network; (c) maintaining firmware updates as recommended by the device manufacturer; and (d) ensuring the device does not create unauthorized access to the Subscriber's building automation or IT systems. Syyclops's responsibility begins at the point of secure data transmission from the device to the Services.

10.4. Sensor and Telemetry Data Ownership. All raw sensor, telemetry, and IoT data transmitted from the Subscriber's facilities to the Services constitutes Service Data and is owned by the Subscriber. Syyclops may use de-identified and aggregated telemetry data for the purposes described in Sections 3.4 and 4.

11. Cookies and Tracking Technologies

11.1 Types of Cookies

- **Strictly Necessary:** Required for authentication, security, and core functionality. Cannot be disabled.
- **Functional:** Remember preferences, settings, and dashboard configurations.
- **Analytics:** Help us understand usage patterns. May be provided by third-party analytics services.

We do not use advertising or behavioral tracking cookies. We do not engage in cross-context behavioral advertising.

11.2 Your Choices

You can control cookies through your browser settings. Disabling cookies may affect functionality. We honor Global Privacy Control (GPC) signals as a valid opt-out request for the sale or sharing of personal information in jurisdictions where required by law. We do not currently respond to Do Not Track (DNT) signals, as no uniform standard exists.

12. Your Privacy Rights

12.1 Rights Available to All Users

Depending on your jurisdiction, you may have some or all of the following rights:

- **Access:** Request a copy of the personal data we hold about you.
- **Correction:** Request correction of inaccurate or incomplete data.
- **Deletion:** Request deletion, subject to legal retention requirements and our legitimate interests.
- **Restriction:** Request restriction of processing in certain circumstances.
- **Portability:** Request a copy in a structured, commonly used, machine-readable format.
- **Objection:** Object to processing based on legitimate interests or for direct marketing.
- **Withdrawal of Consent:** Where processing is based on consent, withdraw at any time.
- **Non-Discrimination:** Exercise rights without receiving discriminatory treatment.

12.2 California Residents (CCPA/CPRA)

If you are a California resident, you have the following additional rights under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, "CCPA"):

- **Right to Know:** You may request that we disclose the categories and specific pieces of personal information we have collected about you, the categories of sources, the business purposes for collection, and the categories of third parties with whom we share your information.
- **Right to Delete:** You may request deletion of personal information we have collected, subject to statutory exceptions (e.g., completing transactions, detecting security incidents, complying with legal obligations, internal uses reasonably aligned with your expectations).
- **Right to Correct:** You may request correction of inaccurate personal information.

- **Right to Opt Out of Sale/Sharing:** We do not sell or share your personal information as defined under the CCPA. If this practice changes, we will provide a “Do Not Sell or Share My Personal Information” link on our website.
- **Right to Limit Use of Sensitive Personal Information:** We collect only the sensitive personal information necessary to provide the Services (such as account login credentials). We do not use sensitive personal information for purposes beyond those permitted under the CCPA.
- **Right Regarding Automated Decision-Making Technology (ADMT):** To the extent Syyclops uses ADMT to make significant decisions concerning you, you may have the right to opt out of such processing and to request information about the logic involved. Contact privacy@syyclops.com for more information.
- **Global Privacy Control (GPC):** We honor GPC signals received from your browser as a valid opt-out request for the sale or sharing of personal information.

Categories of Personal Information Collected (preceding 12 months): Identifiers (name, email, IP address); commercial information (subscription records, payment history); internet/electronic activity (log data, usage data, cookies); geolocation data (approximate, from IP); professional/employment information (job title, organization); inferences drawn from the foregoing. Categories of sensitive personal information: account login credentials (username/password combination).

Categories of Recipients: Cloud infrastructure providers; payment processors; analytics providers; AI/ML providers; communications services; security monitoring services. All are service providers or contractors bound by CCPA-compliant written agreements. We do not disclose personal information to third parties for their own commercial purposes.

Verification: We will verify your identity before processing requests by matching the information you provide against our records. Authorized agents must submit proof of authorization (power of attorney or signed written permission).

Appeal Process: If we deny a request in whole or in part, you may appeal by emailing privacy@syyclops.com with the subject line “Privacy Rights Appeal.” We will respond to appeals within forty-five (45) days. If the appeal is denied, you will be provided with instructions for contacting the California Attorney General’s office.

12.3 Residents of Other U.S. States

Residents of Virginia, Colorado, Connecticut, Texas, Oregon, Montana, Iowa, Indiana, Tennessee, and other states with comprehensive privacy laws may have similar rights to access, correct, delete, and opt out. We will process requests from residents of these states in accordance with applicable law. Colorado residents may appeal denials by following the appeal process in Section 12.2. To submit a request under any state privacy law, email privacy@syyclops.com specifying your state of residence.

12.4 Response Timing

We will respond to verified requests within forty-five (45) days (or thirty (30) days where required by applicable state law). We may extend the response period by an additional forty-five (45) days where reasonably necessary, with notice to you. We reserve the right to deny requests that are manifestly unfounded, excessive, or where exceptions under applicable law apply.

13. Data Return and Deletion

Upon termination or expiration of your subscription, Syyclops will make Service Data available for export for thirty (30) days. Following the export period, Syyclops will delete Service Data from production systems within sixty (60) days and provide written certification upon request. Backup copies will be overwritten within one hundred eighty (180) days. Syyclops retains the right to maintain data required by law, legal hold, or pending litigation, isolated from further processing.

14. International Data Transfers

Syyclops processes data primarily in the United States. If you are located outside the United States, your data may be transferred to and processed in the United States or other countries where our service providers operate. Where required, we implement appropriate safeguards (such as Standard Contractual Clauses).

Syyclops's Services are operated from the United States and are not specifically designed or intended for users subject to the EU General Data Protection Regulation (GDPR). If you are in the European Economic Area, please be aware that by using the Services, you consent to the transfer of your data to the United States.

15. Children's Privacy

The Services are not directed to children under 13 (or 16 where applicable law requires a higher threshold). We do not knowingly collect data from children. If you believe we have inadvertently collected such data, contact privacy@syyclops.com and we will promptly delete it.

16. Accessibility

Syyclops is committed to making its Services accessible to users with disabilities. We strive to conform to the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA and continuously work to improve the accessibility of our platform. If you encounter accessibility barriers, please contact accessibility@syyclops.com and we will make reasonable efforts to provide the information or service in an alternative format.

17. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices, technology, legal requirements, or business operations. When we make material changes, we will: (a) post the revised policy with a new "Last Updated" date; and (b) notify registered users by email at least thirty (30) days before changes take effect. Your continued use of the Services after the effective date constitutes acceptance. Syyclops reserves the right to update this Privacy Policy as necessary to comply with changes in applicable law, including new state privacy laws, federal regulations, and AI governance requirements, with such updates effective immediately upon posting if required by law.

18. Contact Us

For questions, requests, or complaints:

Syyclops, Inc.
Attn: Privacy Officer
5202 Sherier Pl NW, Washington, DC 20016
Email: privacy@syyclops.com
Security: security@syyclops.com
Accessibility: accessibility@syyclops.com