UNCONTROLLED COPY – WEBSITE VERSION GOVERNS

Acceptable Use Policy (AUP)

This Acceptable Use Policy (**"AUP"**) forms part of and is incorporated by reference into the Master SaaS Subscription Agreement (the **"Agreement"**) between the entity identified as "Provider" in the applicable Order Form (**"Provider"**) and the customer entity identified in the applicable Order Form (**"Customer"**).

This AUP may be made available or hosted on one or more Carrier or Carrier-affiliated brand webpages or portals for convenience; however, the branding or hosting location does not determine the contracting parties. The "Provider" is solely the Provider entity identified in the applicable Order Form.

Capitalized terms used but not defined in this AUP have the meanings given in the Agreement or, where applicable, the Data Processing Agreement (the **"DPA"**).

This Acceptable Use Policy ("**AUP"**) forms part of and is incorporated by reference into the Master SaaS Subscription Agreement (the "Agreement") between [Provider Name] (**"Provider"**) and the customer entity that has executed an Order Form (**"Customer"**). Capitalized terms used but not defined in this AUP have the meanings given in the Agreement or the Data Processing Agreement (the "DPA").

1. Scope and Applicability

1.1. **Applicability.** This AUP applies to all access to and use of the Services by Customer and its Authorized Users. The Services include the subscription-based software, cloud services, platforms, modules, features, and related offerings identified in the applicable Order Form(s) and any applicable Product Appendices, whether branded as Abound™, Lynx™, SensiWatch®, Automated Logic®, Nlyte®, or otherwise made available by Provider (each, a **"Module"** and collectively, the **"Services"**).

1.2. **Conflicts.** Privacy, data protection, subprocessors, international data transfers, security incident notification, and technical and organizational measures (TOMs) are governed exclusively by the DPA. In the event of a conflict between this AUP and the DPA concerning processing of Personal Data, the DPA controls. In the event of a conflict between this AUP and the Agreement on matters other than Personal Data, the Agreement controls.

1.3. **Responsibility for Users.** Customer is responsible for the acts and omissions of any person who accesses the Services under Customer's accounts or on

Customer's behalf, including employees, contractors, agents, and service providers (collectively, **"Authorized Users"**).

2. Definitions

2.1. **"AI Features"** means features of the Services that use machine learning, statistical modeling, rules engines, or other artificial intelligence techniques to generate predictions, scores, classifications, recommendations, or natural-language outputs.

2.2. **"Content"** means any data, information, text, images, video, audio, software, or other materials submitted to, uploaded to, generated in, or transmitted through the Services by or on behalf of Customer, including Customer Data, Customer Inputs, and AI Outputs.

2.3. **"Customer Inputs"** means prompts, instructions, configurations, thresholds, labeled examples, training feedback, or other content Customer submits to any AI Features.

2.4. **"External Inputs"** means data originating from Customer's systems, devices, controllers, sensors, refrigeration units, vehicles, facilities, gateways, third-party platforms, or networks (including cellular, satellite, and GPS) that the Services ingest, poll, or receive via APIs or protocols (e.g., SNMP, Modbus, BACnet).

3. General Prohibited Conduct

Customer and its Authorized Users shall not, and shall not permit any third party to:

3.1. Use the Services in violation of applicable law, including export controls, sanctions, anti-corruption, competition, or privacy laws; or to support activities of restricted parties or in embargoed jurisdictions.

3.2. Access or attempt to access accounts, systems, or data without authorization; probe, scan, or test the vulnerability of any system or network; breach or circumvent any security or authentication measures; or intentionally introduce malware, ransomware, spyware, or other malicious code.

3.3. Interfere with or disrupt the integrity or performance of the Services or any third-party network (including cellular, satellite, GPS, or internet backbones), including via excessive API calls, traffic flooding, or resource exhaustion.

3.4. Misrepresent identity or affiliation; engage in fraud, deception, or other abusive practices; or use false headers or identifiers to conceal origin of requests or Content.

3.5. Upload, store, process, or transmit Content that is unlawful, defamatory, harassing, obscene, hateful, or infringes, misappropriates, or violates any intellectual property, privacy, or publicity rights.

3.6. Use or access the Services to build, train, or improve a substantially similar or competitive product or service, or publish product benchmarks or comparative tests without Provider's prior written consent.

3.7. Sell, resell, sublicense, lease, or provide the Services to third parties (including operation as a service bureau or managed service) unless expressly permitted in the Agreement.

3.8. Share or reuse credentials except as expressly permitted; fail to maintain the confidentiality and security of credentials; or permit multiple individuals to use a single-named account.

3.9. Use messaging or notifications features to send spam, unlawful marketing, or other unsolicited communications; fail to provide legally required opt-outs and sender identification.

4. Data and Privacy Guardrails

4.1. **DPA Controls.** Personal Data processing, including roles (controller/processor), purpose limitation, TOMs, subprocessors, international transfers, audit rights, and return/deletion, is governed exclusively by the DPA.

4.2. **Lawful Basis and Notices.** Customer will only submit Personal Data to the Services with a lawful basis and will provide required notices to data subjects. Customer is responsible for accuracy, minimization, and configuration of retention and geolocation settings in the Services.

4.3. **Special Categories.** Customer will not submit special categories of personal data (including health, biometric, precise geolocation tied to an identifiable person, or children's data) unless expressly permitted in a Product Appendix and the DPA with appropriate safeguards in place.

4.4. **Third-Party Data Rights.** Customer is responsible for obtaining all rights, licenses, and consents necessary for any third-party data or External Inputs it contributes or connects to the Services.

5. API, Integration, and Data Handling Rules

5.1. **Documented APIs; Credentials**. Customer will use only documented APIs with issued credentials and will comply with usage limits, pagination, concurrency, and rate limiting. Automated scraping or crawling of user interfaces is prohibited.

5.2. **No Unauthorized Collection**. Customer will not intercept, packet-capture, or otherwise collect data from other customers or from unauthorized endpoints; man-in-the-middle techniques and device "shims" are prohibited.

5.3. **Third-Party Systems.** Customer is responsible for API keys, device credentials, and any licenses or fees for third-party systems and devices integrated with the Services. The AUP applies to those connections and integrations.

5.4. **Caching and Storage.** Customer will not cache or store data contrary to documentation, retention guidance, or the DPA and will promptly remove data when access is revoked.

6. IoT/OT and Remote Command Safety

6.1. **Site Safety.** Where Modules enable remote actions (e.g., BAS setpoints, reefer TRU start/stop or setpoint changes), Customer must maintain human-in-the-loop controls, role-based permissions, and rollback policies and will follow lock-out/tag-out (LOTO) and site safety practices.

6.2. **Protective Limits.** Customer will not disable or bypass safety interlocks, alarms, or protective thresholds designed to prevent equipment harm or unsafe conditions.

6.3. **Instrumentation.** Customer is responsible for sensor selection and placement, calibration, firmware updates, physical security of devices and gateways, and local network segmentation and firewall policies.

7. AI Feature Use (If Enabled)

7.1. **Advisory Outputs.** AI predictions, scores, recommendations, summaries, and generative outputs (collectively, **"AI Outputs"**) are advisory and may be probabilistic or non-deterministic. Customer will validate AI Outputs appropriate to the use case and will not rely on AI Outputs as the sole basis for decisions producing legal or similarly significant effects about an individual without appropriate human review.

7.2. **Prohibited AI Uses.** Customer will not: (a) attempt to remove, disable, or circumvent safety filters; (b) generate or disseminate unlawful, deceptive, or harmful content; (c) train or retrain competitive models using the Services or AI Outputs except as permitted by the Agreement; or (d) misrepresent AI Outputs as human-generated where such misrepresentation would violate law or rights of others.

7.3. **Inputs and Outputs**. Customer is responsible for the legality of its Customer Inputs and its downstream use of AI Outputs, including compliance with sectoral obligations (e.g., GxP and SOPs for life sciences).

8. Service-Specific Provisions

8.1. **Abound™ HVAC Performance and BAS Cloud**. These Modules are not a substitute for onsite mechanical/electrical safety procedures. Automated overrides must not violate OEM limits or site SOPs.

8.2. **Lynx™ Fleet**. Customer will respect geofencing rules and road/port/carrier regulations and will not use geolocation to track individuals without a lawful basis and required notices. Remote reefer control must follow documented fleet policies and permissions.

8.3. **Lynx™ Logix & Lynx™ Factor.** Risk predictions are probabilistic and not guarantees. Customer remains responsible for logistics decisions. Publication of model performance, benchmarks, or comparative evaluations requires Provider's prior written consent.

8.4. **SensiWatch®**. Excursion flags support compliance; Customer's quality management system (QMS) governs final quality decisions and regulatory reporting. Customer will configure retention/approvals consistent with SOPs.

8.5. **DCIM Module.** The DCIM Module is informational and not a real-time control system. Customer is responsible for change approvals and physical execution of work orders and must validate environmental/electrical readings with independent instrumentation where safety-critical.

9. Network and Connectivity; Fair Use

9.1. **Third-Party Networks.** Cellular, satellite, GPS, and internet backbones are outside Provider's control. Customer will not use the Services to overload or attack networks or to impair other users. Network availability, coverage, latency, and accuracy may vary by region and provider.

9.2. **Fair Use.** Abusive usage patterns that materially degrade service for others are prohibited. Provider may apply rate limits, quotas, and traffic shaping to protect platform stability.

10. Security Responsibilities

10.1. **Account Security.** Customer will implement strong passwords, SSO/MFA where available, least-privilege role-based access control (RBAC), and timely revocation of access for separated personnel. Customer is responsible for activities under its accounts.

10.2. **Testing; Disclosure**. Security testing (including penetration tests) requires Provider's prior written approval and must follow Provider's coordinated vulnerability disclosure process. Customer will not conduct denial-of-service or resource-exhaustion testing.

11. Reporting Suspected Violations or Security Issues

Customer will promptly report any suspected violations of this AUP or security issues to Provider using the contact information specified in the applicable Order Form or otherwise designated by Provider. Such reports should include, to the extent reasonably available, applicable timestamps (UTC), affected Module(s), tenant identifier, and a description of the observed behavior.

12. Enforcement; Suspension; Termination

12.1. **Investigation.** Provider may investigate any suspected violation of this AUP or the Agreement, including by reviewing Customer's use of the Services and Content as permitted by the Agreement and applicable law.

12.2. **Remedial Actions.** Provider may remove or disable access to Content; throttle requests; isolate environments; or suspend access to any Module where reasonably necessary to (a) protect the Services or third parties, (b) address a security, safety, or legal risk, or (c) comply with law or requests of governmental authorities.

12.3. **Notice and Cure.** Where feasible and lawful, Provider will provide prior notice and an opportunity to cure before suspension. Provider may implement immediate suspension without prior notice if urgent action is required to address security, safety, or legal risks.

12.4. **Repeat or Egregious Violations**. Provider may terminate the affected Order Form(s) or the Agreement for repeated or egregious violations, in accordance with the Agreement.

13. Law Enforcement and Government Requests

Provider may disclose basic subscriber information or Content to governmental authorities only as required by applicable law, regulation, legal process, or to protect life, safety, or property. Where legally permitted, Provider will provide notice to Customer prior to disclosure and will limit disclosure to the minimum necessary to comply with law.

14.Sanctions; Export; High-Risk Uses

Customer will not access or use the Services in violation of U.S. or other applicable export control or sanctions laws, or permit access by restricted parties or in embargoed jurisdictions. The Services are not designed for life support, emergency response, or other high-risk uses where failure could reasonably result in severe injury, environmental harm, or significant property damage without appropriate safeguards.

15. Modifications; Survival

15.1. **Modifications.** Provider may update this AUP from time to time. Material changes will be notified at least thirty (30) days in advance and will not materially

diminish Customer's core contractual protections during a then-current Subscription Term.

15.2. **Survival.** Sections 1.3, 3 through 15 survive any termination or expiration of the Agreement to the extent necessary to enforce their terms.

16. Contact

Questions regarding this AUP should be directed to Provider at the contact information specified in the applicable Order Form.

International Supplement to Acceptable Use Policy (AUP)

Effective Date: [Insert Effective Date]

1. Purpose; Incorporation; Order of Precedence

1.1 International Supplement. This International Supplement (the **"Supplement"**) forms part of and is incorporated into the Acceptable Use Policy (the **"AUP"**) that is incorporated by reference into the Master SaaS Subscription Agreement (the **"Agreement"**) between the entity identified as "Provider" in the applicable Order Form (**"Provider"**) and the customer entity identified in the applicable Order Form (**"Customer"**).

1.2 Applicability. This Supplement applies to Customer's and its Authorized Users' access to or use of the Services outside the United States, or in any jurisdiction where local law imposes requirements addressed by this Supplement, regardless of where Customer is organized.

1.3 Order of Precedence. Privacy, data protection, subprocessors, international data transfers, Security Incident notification, and technical and organizational measures are governed exclusively by the Data Processing Agreement (the **"DPA"**). In the event of a conflict between this Supplement (or the AUP) and the DPA with respect to Processing of Personal Data, the DPA controls. For all other conflicts, the Agreement controls.

1.4 No Separate AUP. This Supplement supplements (and does not replace) the AUP's general prohibited conduct, security responsibilities, enforcement, and other baseline requirements, which remain fully applicable worldwide

2. Definitions

2.1 "Applicable Local Laws" means laws and regulations applicable to Customer's use of the Services in the relevant jurisdiction(s), including (where applicable) privacy/data protection, employment/labor, telecommunications, mapping/geolocation, content/platform governance, cybersecurity, sanctions/export, and consumer protection laws.

Capitalized terms not defined in this Supplement have the meanings in the Agreement or the DPA.

3. Global/Regional Law Compliance (Customer Obligations)

3.1 Compliance with Applicable Local Laws. Customer is responsible for ensuring that its configuration and use of the Services (including enabling features, collecting inputs, and using outputs) complies with Applicable Local Laws in each jurisdiction where Customer operates or uses the Services.

3.2 Lawful Basis; Notices; Minimization (Personal Data). To the extent Customer submits or makes available Personal Data to the Services, Customer will ensure it has a lawful basis and provides required notices (and obtains consents where required), and will limit Personal Data to what is necessary for Customer's instructed purposes, consistent with Customer responsibilities described in the DPA.

3.3 Prohibited Data; Special Categories; Children. Customer will not submit or otherwise make available to the Services: (a) special categories of Personal Data or other prohibited data; or (b) Personal Data relating to children. The Services are not intended for use by or in connection with children, and Provider does not knowingly process children's Personal Data.

4. Worker/Driver Monitoring; Works Councils; Geolocation

4.1 Worker/Driver Monitoring Requirements. Where Customer uses the Services to monitor employees, contractors, or drivers (including through identifiers or geolocation), Customer will comply with Applicable Local Laws governing workplace monitoring, including (where applicable) consultation, notice, consent, works council approvals, union requirements, and restrictions on tracking and retention.

4.2 Geolocation Controls. Customer is responsible for configuring geolocation, retention, and access controls in the Services in a manner consistent with Applicable Local Laws and Customer's internal policies.

5. Telecommunications / Connectivity / Import-Use Rules (Outside U.S.)

5.1 Telecom and SIM/Device Rules. Customer will comply with Applicable Local Laws relating to telecommunications connectivity, SIM registration, spectrum rules, import/use approvals, mapping/geofencing restrictions, and any local licensing obligations for devices, gateways, or connectivity components Customer deploys or connects to the Services.

6. International Data Transfers (DPA-Driven)

6.1 Transfers Governed by DPA. Where the DPA applies, international transfers of Personal Data (including from the EEA, UK, or Switzerland) are governed exclusively by the DPA's transfer mechanism provisions (including SCCs, the UK Addendum, and the Swiss Addendum, as applicable).

6.2 No Expansion. Nothing in this Supplement expands Provider's obligations regarding transfers beyond those set forth in the DPA.

7. Government / Regulatory Requests and Disclosures (Personal Data)

7.1 Compelled Disclosures Governed by DPA. If Provider receives a legally binding request for Personal Data processed on Customer's behalf, Provider's obligations to

assess, challenge/narrow, notify (where permitted), and minimize disclosure are governed by the DPA.

7.2 Customer Cooperation. Customer will reasonably cooperate with Provider's lawful efforts to respond to valid governmental requests consistent with the DPA and applicable law, including by providing information reasonably necessary to validate Customer's relationship to the requested data.

8. Security Testing; Vulnerability Scanning; Regional Restrictions

8.1 No Security Testing Without Written Approval. Customer will not conduct penetration testing, vulnerability scanning, or other security testing of the Services except as expressly permitted in writing by Provider in accordance with the Agreement and consistent with the DPA's restrictions.

8.2 Local Law Compliance. Where Customer is authorized to perform any security testing, Customer must comply with Applicable Local Laws that restrict unapproved scanning, encryption testing, or interference with networks/systems.

9. Security Incidents (Personal Data) – DPA Controls

9.1 Personal Data Security Incidents. Security Incident notification timelines and content for incidents affecting Customer Personal Data are governed exclusively by the DPA (including the DPA's notice timing and required contents).

9.2 Reporting to Provider. Customer will promptly report suspected AUP violations or security issues using the contact information specified in the applicable Order Form or otherwise designated by Provider, and will include (to the extent reasonably available) timestamps (UTC), affected Module(s), tenant identifier, and a description of observed behavior, consistent with the AUP.

10. Content / Platform Governance; Notice-and-Takedown (Where Applicable)

10.1 Unlawful Content. Customer will not use the Services to store, transmit, or disseminate unlawful content and will comply with Applicable Local Laws regarding illegal/harmful content restrictions, notice-and-takedown obligations, and cooperation with competent authorities, to the extent applicable to Customer's use case

11. Sanctions / Export / Restricted Parties (Multi-Jurisdictional)

11.1 Sanctions and Export Compliance. Customer will not access or use the Services in violation of applicable export control or sanctions laws and will not provide access to restricted parties or in embargoed jurisdictions, consistent with the AUP baseline.

12. Language; Localization; Local Supplements

12.1 English Controls; Convenience Translations. This Supplement and the AUP are drafted in English. Translations may be provided for convenience; in the event of a conflict, the English version controls unless prohibited by Applicable Local Laws.

12.2 Local Supplements. Provider may publish jurisdiction-specific supplements addressing mandatory local requirements. Where a local supplement expressly applies, it will govern solely for the covered jurisdiction and only to the extent of any conflict with this Supplement.

13. Contact

Questions regarding this Supplement should be directed to Provider using the contact information specified in the applicable Order Form or otherwise designated by Provider.