SMARTLOG SECURITY, PRIVACY, SMARTLOG ORDER MANAGEMENT.

Thank you for putting your trust in Smartlog. We are committed to our Customers and are sharing information around the architecture, security and privacy measures and processes undertaken with respect to our Smartlog Order Management ("SOM").

I. TO WHOM DOES THIS PRIVACY POLICY APPLY?

This Privacy Policy applies to everyone who uses our Solutions and Services, but sometimes we direct parts of it toward particular groups of users. When we do, we use the following special terminology to refer to them: "Customer" or "User" means anyone who uses our Solutions and Services. "Partner" or "Subscriber" means anyone who purchases or subscribes to one or more of our Solutions and Services.

1. Security Controls

The Services include a variety of configurable security controls for the Customer's authorized administrators. These controls include, but are not limited to:

- Various user access management controls.
- Various password complexity controls.
- User access logs for the Customer's instance are available for review and export, where applicable.
- Other logical controls.

2. Security Policies/Procedures

a. Smartlog Commerce is operated under a "Shared Responsibility Security Model"; documentation is available upon request from the Smartlog Support organization. In this model, different parties have different areas of responsibilities for maintaining the security of the system. This approach allows for both flexibility and use of best-of-breed cloud technologies.

b. In addition, the Services are operated in accordance with the following policies and procedures to enhance security:

- User passwords are not transmitted unencrypted.
- User passwords are stored using a salted hash.
- Log files for the Customer's instance are available for review and export, where applicable.
- Internal system accounts are reviewed on a regular basis.
- Logs are stored securely.

- Access is logged unless specifically disabled by Customer

c. Although Customers retain the primary responsibility for security monitoring of their production instance(s), Smartlog, or an authorized third party, will monitor the Services for unauthorized intrusions using intrusion detection mechanisms. Smartlog may analyze data collected by users' web browsers (e.g. device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including for incident detection and response, to prevent fraudulent authentication, and to determine that the Services function properly.

d. All Smartlog production systems used in the Services, including firewalls, routers, operating system, log information to the respective system log facility or a centralized log collection server in order to enable security reviews and analysis.

3. **Incident Management**

a. Smartlog maintains a security incident management program. Upon detection of a security incident, Smartlog undertakes an internal investigation and where appropriate, remediation process, up to and including notification to impacted individuals, all in accordance with applicable law.

b. Without limiting the above, with respect to the Services, the Customer shall be responsible for any security incident relative to accounts provisioned by the Customer or their respective solutions integrator. For Smartlog Commerce, Customer shall remain responsible for any security incident caused by, in whole or in part, the Customer's modification or customization of Smartlog Commerce, any plug-in or non-Smartlog extension, failure to apply a security patch in a timely manner, or other negligence caused by the Customer or its solution integrator.

4. **User Authentication.**

The Services allow Customers to customize many logical access management controls to provision and manage access. Access to the Services requires a valid user ID and password combination, which are encrypted via TLS while in transmission. Passwords are hashed and salted and only the hash is stored by the Services.

5. **Physical Security.**

Production data centers used to provide the Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by remote surveillance monitoring, multi-layered access controls, badged access, and are also supported by on- site backup generators in the event of a power failure.

6. **Reliability and Backup.**

The Services architecture is designed to be highly redundant and reliable. Should a Customer's primary data center encounter a disaster that prevents it from functioning, formal processes are in place to restore the Customer's production-level Services. Customer data submitted to the Services is stored on a primary database server with a replicated copy for high availability and performance. All Customer data submitted to the Services, up to the last committed transaction, is automatically replicated daily to another location. In the event that production facilities for the Services hosting the Customer's primary data center were to be rendered unavailable, redundant hardware, software, and equipment are in place.

7. Return/Deletion of Customer Data.

Following termination or expiration of the Customer's subscription to the relevant Services, the Customer has thirty (30) days to access its account and download or export Customer data. Following such thirty (30) day period, Smartlog will promptly deprovision the Customer environment and all Customer data in Smartlog systems or otherwise in its possession or under its control shall be subject to deletion.

II. WHAT INFORMATION DO WE COLLECT?

We collect some information from all users. As part of our Solutions and Services, we use various technologies such as session log data and third-party analytics to collect and analyze information about Users. This includes things like the Users' search preferences, saved searches, aspects of their use of the Solutions and Services, and location. We use this information to better understand how you interact with our Solutions and Services, and to monitor aggregate usage and web traffic information on our Solutions and Services.

Our servers automatically record information ("Log Data") created by your use of the Solutions and Services. Log Data may include information such as your IP address, browser type, operating system, the referring web page, web pages visited, location, and search terms. We receive Log Data when you interact with our Solutions and Services, for example, when you visit our website, sign into our Solutions and Services, or interact with our email notifications. Consent: If you contact us through one of our websites, we ask you to provide certain personally identifiable information like your name, email address, or company name and telephone number ("Personal Information"). Your provision of Personal Information means you agree and consent that we may collect, use and disclose your Personal Information under this Privacy Policy.

Consent may be given expressly, by signing a document, agreeing through electronic means or verbally, or impliedly by providing Personal Information voluntarily. Certain Solutions and Services can only be offered if you provide Personal Information to us,

and if you choose not to provide us with such required Personal Information, we may not be able to offer you our Solutions and Services.

Information About You that We Obtain from Third Parties: We may sometimes obtain Personal Information about you from third parties (e.g., Facebook, Twitter, Google) and use it to re-market our Solutions and Services or provide a more tailored experience with our Solutions and Services.

Location Data: If you provide location information during the registration process or at any other time via your account settings, we will store that information and associate it with your account. In some cases we may collect and store information about where you are located, such as by converting your IP address into a rough geolocation. If you use mobile Services, we may collect location data directly from your mobile device automatically if your device allows us to do so. In some circumstances, you may have to opt into sharing your location data with us. Additionally, your mobile device may provide you with choices about how and whether location data is shared with us.

III.　　GENERAL MATTERS

Unsubscribing to Smartlog Communications: You may unsubscribe at any time from receiving non Solutions and Services related communications from Smartlog through your account settings or through the instructions included in the communication.

Children: The Solutions and Services are not directed to children under 18, and we do not knowingly collect or store any Personal Information about persons under the age of 18. If we learn that we have collected Personal Information of a child under 18, we will take steps to delete such information from our files as soon as practicable.

Third-Party Websites: Our Services may contain links to other websites and services. Any information that you provide on or to a third-party website or service is provided directly to the owner of the website or service and is subject to that party's privacy policy. Our Privacy Policy does not apply to such websites or services, and we are not responsible for the content, privacy or security practices and policies of those websites or services. To protect your information we recommend that you carefully review the privacy policies of other websites and services that you access.

Privacy Policy Changes: We may update this Privacy Policy from time to time to reflect changes to our information practices. If we make material changes to our Privacy Policy, we will notify you by prominently posting the revised Privacy Policy on this site (including the revision date). Your continued access or use of our websites constitutes your acceptance of the Privacy Policy as revised. It is your responsibility to review the Privacy Policy frequently. Contacting Us: If you have any questions or suggestions regarding our Privacy Policy, please contact us at: https://gosmartlog.com/lien-he/.