Security Policies and Procedures

(revised 12/1/2023)

Data Access and Uptime Policies

We guarantee uptime of 99.9%, inclusive of all delivery components and any outages resulting from scheduled or emergency maintenance within the software application itself or at the hosting data center.

As a cloud based Software as a Service (SaaS), our application will be available for access 24 hours per day, 7 days per week except for scheduled or emergency maintenance. We will make available access to client's own data in accordance with the terms of the agreement for services in a manner consistent with the functionality of the services provided. To the extent that our client does not have ability to amend, delete, or migrate their data – or requires our assistance in doing so – We will assist with any reasonable requests at our client's reasonable expense to the extent legally permitted.

Uptime Credit. Zenventory customers shall have the right to receive a credit based upon the applicable monthly Subscription Fee(s) as specified in the table below for any outage within the control of Zenventory. For example, if the Uptime Availability fell to 97.1% for a specific calendar month, Zenventory would credit 5% of the pro-rated amount of that calendar month's Subscription Fee(s). Uptime Availability is calculated on a rolling month basis by the following formula:

Uptime Availability Percentage = ((x - y)/x) * 100

- x = total minutes per month
- y = minutes the Services were not available, excluding scheduled downtime communicated in advance.

Percentage Of Uptime Availability	Percentage Of Monthly Subscription Fee Creditable (collectively, the "Credit")
100 to 99.5	0.00%
< 99.5 to 97.0	5%
<97.0 to 95.0	10%
<95.0	100%

The Credit, as applicable, will be deducted from the following renewal invoice. In addition, Zenventory warrants and represents that the services will be provided in a professional and workmanlike manner, consistent with industry standards.

Security Policies and Procedures

(revised 12/1/2023)

Security Policies

Customer data may be stored on third-party servers. We will ensure that any third-party servers comply with the requirements set forth in ISO 27001.

Internal procedures are in place to prevent the retention or misuse of our clients' private or personal data. Our security policies dictate that any data provided to us or created through the use of our application is accessed from our side solely to fulfill our service obligations to our client, or in accordance with contract terms. Account and user data is viewed by our team only in the course of providing support to our client, fulfilling a direct request of our client, or in the course of data center operations.

Encryption: Encryption is deployed within the application to ensure the security of sensitive data and prevent it from being viewed by unauthorized parties. Security for the browser session between the user and the application will be provided by a Secure Sockets Layer (SSL) from a trusted certificate authority. All data is encrypted at rest, in transit, and while stored. Data is transmitted to and from the site over HTTPS using 256-bit encryption and at rest using AES256 encryption.

Customer Data: Customer Data includes the data that is inputted by the user to properly use the software. Such information may include the user's name, location (which may include address), email address, and client information. Our software programs do not require the use of Sensitive Personal Identifiable Data ("SDII") to function and such information shall not be disclosed. Such SDII includes – but is not limited to - the user's social security number, health care information, financial information, biometric information, and information regarding the user's ethnicity. Users agree not to use or disclose any SDII in utilizing the software.

Security Data Detection: We have implemented a reasonable data detection policy to test and analyze our security prevention measures. In addition to the security measures put in place by us to identify and protect our networks and data centers, we also allow our customers to conduct intrusion and security testing on our web and mobile applications at their own cost. We conduct intrusion and security testing on our software applications periodically and prior to any software release. We reserve the right to update or modify these measures at any time without notice.

Security Data Response: We maintain a response program appropriate to respond to a data incident. If we have reason to believe that a Data Incident has occurred, where we reasonably believe there is a risk of harm, we will: (a) promptly investigate and take steps to remediate it and (b) notify the client of the Data Incident without unreasonable delay following the discovery of the security incident. We will provide notice either through email that has been provided to us or by direct communication to designated client personnel. The client shall have the sole responsibility for fulfilling any third party notification obligations.

- Definition: "Data Incident" shall mean any unlawful or unauthorized destruction, loss, alternation, access, use, or disclosure of personal data that compromises the security, privacy, or confidentiality of the personal data.

Security Policies and Procedures

(revised 12/1/2023)

Network Security: We use reasonable measures to protect our network and keep it secure. Such measures include the use of firewall protection that encompasses intrusion prevention services, virus scanning, packet filtering, and web blocking. In addition, all employee computers must be secured when not in use and be protected with passwords. Logs for security-related events are reviewed on a bi-weekly basis.

Personnel Security, Hiring Procedures: Our personnel are required to conduct themselves in a manner consistent with the company's policies regarding security and ethics. Our employees are provided an opportunity to review and question our policies in addition to yearly testing on company security policies. We conduct reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations at the time of hiring. Our employees are required to execute and acknowledge receipt of, and compliance with, our policies. Personnel handling customer data are required to complete additional requirements appropriate to their role (i.e. certifications). Our personnel will not process customer data without authorization.

Personnel Security, Termination Procedures: As all Zenventory application & user data resides in the cloud, we can terminate individual access remotely without any cooperation required by the team member when necessary. In the event of a team member voluntarily leaving the employ of Zenventory, access to all company systems and resources will be removed on or before their last day of employment. In the event of an involuntary termination initiated by Zenventory, access to all company systems and resources is removed prior to notification of the team member.

Storage and Backup Policies and Procedures

Data Centers: To store data for use of our products, we contract with secure 3rd party Data Centers that acknowledge that the protection of data is of the utmost importance. Accordingly, these Data Centers comply with the requirements of ISO 27000 Security Framework. Data Centers are restricted access facilities where authorized personnel are limited to access to the data.

- Definition: "Data Center" shall mean a secure server farm used for the remote storage, processing, or distribution of data used by our software.

Power and Systems: Our Data Centers provide high uptime availability in addition to high levels of security. This includes the use of uninterruptable power supplies at the Data Centers, which are inspected and serviced regularly. In addition, Data Centers may use diesel generators to minimize the risk of any long-term power outage. The Data Centers are equipped with redundant HVAC Units, smoke detectors, fire detectors, flood water detectors, fire detectors, and suppression systems.

Physical Access: We choose Data Centers that require their employees to wear identification badges and use a two-factor authentication system. These Data Centers only allow authorized employees into the data center facilities. Data Center facilities are also maintained by the Data Center's employees 24 hours a day, 7 days a week.

Backup Frequency: Client data is backed up every four hours, with any changed data overwriting old data with each backup event. Backup data will be retained for the lesser of seven (7) years, or the date of service termination in any scenario described in the contract that requires data sanitization.

Level of Support Service

We provide the following technical support services for the duration of your subscription:

- Technical assistance for individuals and/or groups;
- Troubleshooting of software defects;
- Scheduled web-based training available upon request for individuals and/or groups;
- On-going maintenance, application of updates, and notification on new features.

Availability: The Support Team is available during regular business hours (except for recognized holidays), Monday through Friday, from 7:00 a.m. to 5:00 p.m. Arizona time. The most efficient way to request support for non-urgent issues is to create a ticket with a detailed description of the request and/or problem using the in-application "Help" page. You may also contact the Support Team by phone at (480) 530-2100 x1 for any time-sensitive support needs. In the event the Support Team staff are unavailable during business hours, you may leave a voice mail message; voice mails will be responded to within one business day.

- By ticket: Using our application's "Help" section
- By phone: (480) 530-2100 x1
- By email: support@zenventory.atlassian.net
- Self-service: Access to an online Knowledge Base containing articles, walkthroughs, and screenshots is also available from the application's "Help" section.
- On site support: Not included by default but may be provided in special cases for a fee (per day). See your account representative for a quote on this option.

Security Policies and Procedures

(revised 12/1/2023)

Incident Response Times:

Upon receipt of a support request from a validated account user, we shall use reasonable commercial efforts to resolve reported Incidents according to the following schedule:

Priority	Title & Explanation	Resolution Time*
1	**Fatal** – Incident preventing all useful work from being done. This condition is generally characterized by complete system failure or data destruction.	4 Operation Hours
2	**Severe Impact** – Incident disabling major functions from being performed. This condition exists when the products are partially inoperative, but are still usable, and the impact is one of inconvenience.	2 Business Days
3	**Degraded Operations** – Incident disabling only certain nonessential functions. This condition exists when the products are usable, but with limited functions	5 Business Days
4	**Minimal Impact** – Includes all other Incidents. This condition exists when the products are usable and the Incidents result in a minor failure that involves individual components of the products	10 Business Days

*Resolution Time is calculated from the time the Incident is reported by the user

Vulnerability Remediation Times:

Upon detection of a vulnerability, we shall use reasonable commercial efforts to resolve reported vulnerabilities according to the following schedule:

Priority	Title & Explanation	Resolution Time*
1	**Critical** – Vulnerabilities likely to result in root-level compromise of servers or infrastructure devices are patched or mitigated as quickly as possible. Exploitation is usually straightforward and can be conducted without a privileged user performing any special functions.	2 Business Days
2	**High** – Vulnerabilities that are difficult to exploit but could result in elevated privileges and where exploitation could result in a significant data loss or downtime.	30 Business Days
3	**Medium** – Vulnerabilities where exploitation provides only very limited access or requires user privileges for successful exploitation.	Based on staff availability
4	**Low** – Vulnerabilities that have little impact on the system or the business. Exploitation of such vulnerabilities usually requires local or physical system access.	Based on staff availability

*Resolution Time is calculated from the time the vulnerability is reported or detected

Definitions

1.1 "Business Day" means Monday through Friday from 7:00 a.m. to 5:00 p.m. Arizona time, excluding holidays (New Year's, Memorial Day, Fourth of July, Labor Day, Thanksgiving, and Christmas).

1.2 "Off hours" shall be Monday-Friday 5:01 pm-6:59 am 9am Arizona time, Saturday and Sunday. We shall, whenever practical, limit system maintenance or application updates/upgrades to Off Hours.

1.3"Validated Account User" means a user that contacts the Support Team through a pre-authenticated channel to ensure account security, such as through our application's ticketing system.

1.4 "Incident" means a reproducible malfunction that degrades or impairs Your use of the functionality included within the Program, excluding changes made without Our consent.

1.5 "Operation Hour" means a full hour that occurs during a Business Day.

1.6 "Uptime Availability" means an end-user is able to access and use the products 24 x 7 x 365, excluding routine maintenance and downtime from interruption, termination, or failed operation of the Internet, private intranet, or of third party telecommunication services and force majeure events.