Zenventory Cyber-Security Policy

Effective 1/1/2021, Last reviewed 3/1/2023

Zenventory Data Security Policy

1.1 Security Prevention Measures: Zenventory has implemented reasonable technical and organizational measures to protect Customer Data against accidental or unlawful destruction or accidental loss, alteration, or unauthorized disclosure or access. These security measures are outlined in Paragraph three (3) herein. Zenventory reserves the right to update or modify these security measures at any time. Zenventory takes reasonable measures in ensuring that all of its employees and contractors comply with the terms of Zenventory's Security Measures.

1.1.1 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. The Zenventory software programs do not require the use of Sensitive Personal Identifiable Data ("SPII") to function and such information shall not be disclosed. Such SPII 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. User agrees not to use or disclose any SPII in utilizing the software.

1.2 Security Data Detection: Zenventory has implemented a reasonable data detection policy to test and analyze its security prevention measures. In addition to the security measures put in place by Zenventory to identify and protect its networks and data centers, Zenventory also allows its customers to conduct intrusion and security testing on its web and mobile applications at their own cost. Zenventory conducts intrusion and security testing on its software applications periodically and prior to any software release. Zenventory reserves the right to update or modify these measures at any time without notice. Questions regarding our security and privacy policies and standards should be directed to support@zenventory.com or (480) 530-2100.

1.3 Security Data Response. Zenventory maintains a response program appropriate to respond to a data incident. If Zenventory has reason to believe that a Data Incident has occurred, which it reasonably believes there is a reasonable risk of harm, Zenventory will: (a) promptly investigate and take steps to remediate it and (b) notify the customer, reseller, or supplier(s) of the Data Incident without unreasonable delay following the discovery of the security incident and in some circumstances no later than 72 hours. Zenventory will provide notice either through email that has been provided to

Zenventory or by direct communication to the customer, reseller, or supplier(s). Resellers shall have the sole responsibility for fulfilling any third party notification obligations.

1.3.1 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.

Data Storage, Deletion, and Access

2.1 Data Storage: Customer data for the Zenventory web-hosted services are stored on third-party servers. Zenventory shall ensure that any third-party servers comply with the requirements set forth in ISO 27001 or have passed a SOC 2 audit and continue to hold a SOC 2 certification. Data is primarily hosted with Amazon Web Services.

2.1.1 Data from Zenventory’s United States users shall be stored and processed in the United States. Data from Zenventory’s Canadian users shall be stored and processed in Canada. Data from Zenventory’s European customers shall be stored and processed in Europe. Other countries in which Zenventory services shall have its data stored and processed in that country if available.

2.2 Deletion: During the term of the agreement for services, Zenventory will provide the end users the ability to correct, block, export, be forgotten, and delete its data in a manner consistent with the functionality of the services rendered in conformance with United States laws. Once the data is deleted, it is not recoverable. Zenventory also takes reasonable measures to delete customer data when it is no longer needed for business purposes. Upon cancellation of the services, the end user shall notify Zenventory of how to process its data. If no notice is provided within 30 days, Zenventory may delete that data and backups.

2.3 Access to Data: Zenventory will make available to customers its 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 the customer does not have ability to amend, delete, or migrate customer data – or requires Zenventory’s assistance in doing so – Zenventory will assist with any reasonable requests at the customer’s reasonable expense to the extent legally permitted by the United States.

2.4 Transfer of Data at Conclusion of Use: At the conclusion of customer’s use of the product, customer may have its data downloaded to its servers or storage device at its request. Such requests should be made within ten days of the conclusion of use. Zenventory will process such requests as outlined in paragraph 2.3 above and will

provide such storage in a commercially reasonable time. Please contact your sales associate for such requests or call Zenventory toll free at (480) 530-2100.

Security Measures

3.1 Network Security

3.1.1 Zenventory uses reasonable measures to protect its 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.

3.2 Data Center

3.2.1 Data Centers. Zenventory contracts with secure Data Centers to store its data for use of its products. Zenventory contracts with 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 or have passed a SOC 2 audit and continue to hold a SOC 2 certification. Data Centers are restricted access where authorized personnel are limited to access to the data, and visitors are required to sign into a visitor log when entering the Data Centers.

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

3.2.2 Power and Systems. The Data Centers used by Zenventory are chosen to provide high uptime availability in addition to high levels of security. This includes the use of uninterruptible 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.

3.2.3 Physical Access. Zenventory chooses Data Centers that require its 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.

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

Third Party Requests for Access to Data.

4.1 Third Party Requests: Customer is primarily responsible for responding to third-party requests. Zenventory will, at customer's reasonable expense, and only to the extent allowed by law and by the terms of the third-party request: (a) promptly notify customer of its receipt of a third-party request; (b) comply with customer's reasonable requests regarding its efforts to oppose a third-party request to the extent allowed by law; and (c) if the information is solely held by Zenventory and reasonably accessible, provide customer with the information or tools required to respond. Notwithstanding the foregoing, the previous subsections will not apply if Zenventory determines that complying with those subsections could result in a violation or legal process, obstruction of a governmental investigation, and/or lead to death or serious physical harm to an individual. Customers will first seek to obtain the information required to promptly and timely respond before requesting Zenventory to obtain such information.