PANZURA

This Panzura Security Addendum ("**Addendum**") is made a part of the Subscription Software and Services Agreement (the "**Agreement**") between Panzura and Customer found at https://panzura.com/legal. All capitalized terms used but not defined herein will have the meanings assigned to them in the Agreement. This Addendum may be updated from time to time by Panzura in its sole discretion provided that such updates will not materially reduce the security of the Software provided to Customer by Panzura.

## 1. STANDARD PANZURA SECURITY & AUDIT REQUIREMENTS

**1.1 Compliance Standards**. Panzura aligns with industry standards to ensure secure, consistent, and available Software. Panzura follows NIST security controls including, but not limited to access control, vulnerability management, secure configuration, and security monitoring. Additionally, Panzura leverages the best practices of Information Technology Infrastructure Library ("ITIL") including, for example, incident, change, and configuration management to ensure timely and consistent Software solutions. Panzura also applies continuous integration ("CI") and continuous delivery ("CD") rigor to ensure the Software is secure and provides the intended functionality to Customers. Panzura's security controls generally, ITIL practices, and CI/CD pipeline are all in scope for Panzura's annual risk assessment and the focus of Panzura's risk management program.

**1.2 Security Incident Notification.** Panzura will notify Customer within 48 hours of becoming aware of a security incident with the potential to expose Customer Data. Panzura will provide Customer with relevant root cause detail, forensics, and logs as such information becomes reasonably available.

**1.3 Audit Rights.** To assist Customer with security questionnaires, audits, or compliance activities, Panzura will permit an annual audit upon written request to Panzura at security@panzura.com. During the audit, Customer's authorized employees, auditors and agents will be permitted to view but not copy or retain confidential and proprietary documents relevant to operating controls and security policies. All audit activities will be subject to a non-disclosure agreement. In the absence of a security incident, audits may be requested no more than once per rolling 12-month period and require at least 30 days' prior written notice to Panzura for scheduling. Additional audits may be requested following any security incident involving Customer Data. Questionnaires, security reviews, and other information or documentation requested by Customer may only be provided as part of a formal audit.

## 2. DATA CENTER SECURITY & AUDIT REQUIREMENTS

**2.1 Certification and Compliance Standards**. Certain Software is delivered from a data center operated by a third-party hosting provider that maintains ongoing annual third-party audits for SSAE 18 (or then current standard as evolved by AICPA) SOC 1 (Type 2) and SOC 2 (Type 2) attestations and reports. SOC 1 and SOC 2 reports and bridge letters for Panzura's third-party hosting provider are available upon request to Panzura at security@panzura.com.

**2.2 Audit Reports.** SOC 1 and SOC 2 reports of Panzura's third-party hosting provider will be provided to Customer upon request to Panzura provided that any request will be limited to the most recent, applicable audit, capable of being provided to Panzura within a commercially reasonable amount of time and will be requested no more than once in a 12-month period, except in the case of a security incident with the potential to expose Customer Data, or if Panzura is notified of such a security incident by its third-party hosting provider.

**2.3 Data Center Location.** Unless requested by Customer in writing, Panzura will not migrate, transfer, or otherwise move Customer Data to a data center of hosting provider located in a different country from the original data center in which the applicable production environment is established. If Panzura initiates a change to the data center location, it will notify Customer promptly, without undue delay, provided that Panzura may initiate a change in a data center location without notice if: (i) reasonably necessary to prevent, mitigate, or remedy, a critical security vulnerability; or (ii) in the event of a disaster recovery event.

**2.4 Customer Data Center Access.** Customer will not be permitted access to Panzura's third-party hosting provider's locations at any time during the term of the Agreement, including Customer's auditors, agents, service providers, or other representatives.

## 3. ENCRYPTION OF CUSTOMER DATA

**3.1** Panzura will provide Customer with an industry standard level of encryption for Customer Data both in transit and at rest (**"Encryption"**) for Software as provided herein. Encryption at rest encompasses all Customer Data (disk, tape, and offsite) at the primary site, secondary site, and any offsite locations used by Panzura's third-party hosting provider for vaulting of backup media. All Customer Data at rest (disk, tape, and offsite) including database data, reporting data, file attachments, and integrations is encrypted with industry standard protection under AES 256-CBC standards, including Customer Data stored in Customer-provided object stores. All Customer

Data in transit is encrypted using TLS v1.2 or v1.3 secure protocols (e.g., HTTPS, SFTP, etc.), including between nodes within a Customer's environment. Panzura encrypts all Customer Data between the Customer and Panzura's hosted Software. Additionally, Panzura encrypts all Customer Data related to Customer support and diagnostic use.

## 4. SECURE CODING GUIDELINES & MALWARE DETECTION

**4.1** Panzura follows industry standard secure coding guidelines and takes appropriate measures to protect the Software against unauthorized modifications to the Software or the Customer Data without the consent of Customer or Panzura.

- Prior to release, Static Application Security Testing (SAST) conducted to identify potential vulnerabilities in the Panzura Software.
- Access to systems is controlled by an industry standard authentication method leveraging strong authentication with a unique User ID and strong password.
- Remote access (if applicable) is secured through multi-factor authentication.
- Passwords may never be stored in clear text.
- Secure Coding Guidelines, aligning to Microsoft SDL and OWASP

**4.2 Application Security Training.** Panzura provides its software development team with application security training on secure development and other protocols.

**4.3 Malware Detection.** Panzura uses commercially reasonable, and industry standard malware detection measures to prevent the distribution of malware upon implementation or delivery of Software. Customer is expected to maintain a secure internal network for its own purposes outside the Software. Malware, harmful code, or other invasive or unauthorized programs are not sanctioned by Panzura (**"Malware"**). Panzura will not be liable to Customer or any third-party if harm is caused by the failure of Customer's internal network to detect Malware originating from third-party products, Customer's internal network, or not otherwise within the reasonable control of Panzura.

## 5. GENERAL USER TERMS

**5.1 Definition of Terms**. Any industry standard non-defined terms in this **Section 5**, will default to those in the NIST glossary of standard information security terms, available at https://csrc.nist.gov/glossary.

**5.2 User Misuse & Credentials.** The Parties agree that Panzura does not provide onsite credentials management for Customer, and that Customer, it's Users, or holders and handlers of credentials are collectively responsible for the damage or harm caused by: (i) the use or distribution of User credentials or (ii) the misuse of Software. Customer agrees and understands that completion of annual security awareness training is necessary to prevent the harmful, unlawful, or improper release of User credentials by Customer and its Users, and any harms caused by improper release of Customer credentials or access to the Software will be the sole responsibility of Customer.

**5.3 Authentication & Credentials Management.** The Parties agree that, during the term, Customer will maintain up-to- date credentials management practices and safeguards that meet single-factor authentication. If Customer chooses to use single- factor authentication for the Software, Customer understands and agrees to the risks associated with the lack of multi-factor authentication. The Parties agree to reference NIST SP800-63B (**"Authentication Definitions"**) for definitions, and that any Panzura Software under the applicable Order may use AAL1 (as defined in the Authentication Definitions) unless noted otherwise.