KENSU DATA SECURITY GUIDE

This data security guide ("Data Security Guide") forms a part of the Master Services Agreement entered into by the parties ("Agreement") and describes the measures Kensu takes to protect Customer Data. All capitalized terms not defined in this Data Security Guide will have the meaning given to them in other parts of the Agreement.

1. SECURITY PROGRAM

While providing the Products, Kensu will maintain a written information security program of policies, procedures and controls governing the processing, storage, transmission and security of Customer Data (the "**Information Security Policy**"). The Information Security Policy includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Kensu regularly tests, assesses, and evaluates the effectiveness of the Information Security Policy and may periodically review and update the Information Security Policy to address new and evolving security technologies, changes to industry standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

2. PHYSICAL, TECHNICAL, AND ADMINISTRATIVE SECURITY MEASURES

2.1 PHYSICAL SECURITY MEASURES.

2.1.1. SYSTEMS, MACHINES AND DEVICES. **(a)** Physical protection mechanisms; and **(b)** entry controls to limit physical access.

2.1.2. MEDIA. **(a)** Industry standard destruction of sensitive materials before disposition of media; **(b)** secure safe for storing damaged hard disks prior to physical destruction; and **(c)** physical destruction of all decommissioned hard disks storing Customer Data.

2.2 TECHNICAL SECURITY MEASURES.

2.2.1. ACCESS ADMINISTRATION. Access to the Products by Kensu employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relationships. Production infrastructure includes appropriate user account and password controls (e.g., the required use of VPN connections and complex passwords with certificates expiration) and is accessible for administration.

2.2.2. SERVICE ACCESS CONTROL. The Products provide Users and role-based access controls. Customer is responsible for configuring such access controls within its instance.

2.2.3. LOGGING AND MONITORING. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering.

2.2.4. FIREWALL SYSTEM. An industry-standard firewall is installed and managed to protect Kensu systems by residing on the network to inspect all ingress connections routed to the Kensu environment.

2.2.5. VULNERABILITY MANAGEMENT. Kensu conducts periodic security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, Kensu will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with Kensu's then-current vulnerability management and security patch management

standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems.

2.2.6. PROTECTION. Kensu updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

2.2.7. CHANGE CONTROL. Kensu ensures that changes to platform, applications, and production infrastructure are evaluated to minimize risk and are implemented following Kensu's standard operating procedure.

2.2.8. DATA SEPARATION. Customer Data shall be maintained within a logical single or multi-tenant architecture on multi-tenant cloud infrastructure that is logically separate from Kensu's corporate infrastructure.

2.3 ADMINISTRATIVE SECURITY MEASURES.

2.3.1. PERSONNEL SECURITY. Kensu performs background screening on all employees and all contractors who have access to Customer Data in accordance with Kensu's then-current applicable standard operating procedure and subject to Data Protection Laws.

2.3.2. SECURITY AWARENESS AND TRAINING. Kensu maintains a security awareness program that includes appropriate training of Kensu personnel on the Information Security Policy. Training is conducted at time of hire and periodically throughout employment at Kensu.

2.3.3. VENDOR RISK MANAGEMENT. Kensu maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Customer Data for appropriate security controls and business disciplines.

3. SERVICE CONTINUITY

3.1 DATA MANAGEMENT; DATA BACKUP. Kensu will host Customer's access to and use of purchased instances of the Products in a pair of data centers that attained SSAE 18 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations) acting in an active/active capacity for the Term. Each data center includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. The production database servers are replicated in near real time to a mirrored data center in a different geographic region. Each Customer instance is supported by a network configuration with multiple connections to the Internet. Kensu backs up all Customer Data in accordance with Kensu's standard operating procedure.

4. AUDITS

4.1 AUDIT. No more than once per calendar year and upon written request by Customer, Customer shall have the right directly or through its representative(s) (provided however, that such representative(s) shall enter into written obligations of confidentiality directly with Kensu), to access all reasonable and applicable documentation (as reasonably determined by Kensu) evidencing Kensu's policies and procedures governing the security of Customer Data ("**Audit**"). Such Audit shall include a written summary report of any assessment performed by an independent third-party of Kensu's information security management system. Kensu reserves the right to refuse to provide Customer (or its representatives) with any information which would pose a security risk to Kensu or its customers, or which Kensu is prohibited to provide or disclose under applicable laws and regulations, including Data Protection Laws, or contractual obligation.

4.2 OUTPUT. Upon completion of the Audit, Kensu and Customer may schedule a mutually

convenient time to discuss the output of the Audit. Kensu may in its sole discretion, consistent with industry and Kensu's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve Kensu's Information Security Policy. The Audit and the results derived therefrom are Confidential Information of Kensu subject to the confidentiality requirements in the Agreement.

5. MONITORING AND INCIDENT MANAGEMENT

5.1 MONITORING, MANAGEMENT AND NOTIFICATION.

5.1.1. INCIDENT MONITORING AND MANAGEMENT. Kensu will monitor, analyze, and respond to security incidents in a timely manner in accordance with Kensu's standard operating procedure. Kensu's security group will escalate and engage response teams as may be necessary to address an incident.

5.1.2. BREACH NOTIFICATION. Kensu will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "**Breach**") without undue delay following determination by Kensu that a Breach has occurred.

5.1.3. REPORT. The initial report will be made to Customer security or privacy contact(s) designated in Kensu's customer support portal (or if no such contact(s) are designated, to the primary contact designated by Customer). As information is collected or otherwise becomes available, Kensu shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected data subjects, government agencies, and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the Kensu contact from whom additional information may be obtained. Kensu shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

5.1.4. CUSTOMER OBLIGATIONS. Customer will cooperate with Kensu in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s), and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted data subjects and for providing such notice.

5.2 COOKIES. When providing the Products, Kensu uses cookies to: **(a)** track session state; **(b)** route a browser request to a specific node when multiple nodes are assigned; and **(c)** recognize a User upon returning to the Products. Customer shall be responsible for providing notice to, and collecting any necessary consents from, its authorized users of the Products for Kensu's use of cookies.

6. PENETRATION TESTS

6.1 Kensu conducts regular penetration tests on its Products, including the Kensu application, to identify risks and remediation that help increase security.

6.2 BY CUSTOMER. No more than once per calendar year, Customer may request to perform, at its own expense, an application penetration test of a sub-production instance of the Products. Customer shall notify Kensu in advance of any test by submitting a request to schedule an application penetration test using Kensu's customer support portal per Kensu's then-current penetration testing policy and procedure, including entering into Kensu's penetration test agreement. Kensu and Customer must agree on a mutually acceptable time for the test; and Customer shall not perform a penetration test without Kensu's express written authorization. The test must be of reasonable duration, but in no event longer than fourteen

(14) days and must not interfere with Kensu's day-to-day operations. Promptly on completion of the penetration test, Customer shall provide Kensu with the test results including any detected vulnerability. Upon such notice, Kensu shall, consistent with industry-standard practices, use all commercially reasonable efforts to promptly make any necessary changes to improve the security of the Products. Customer shall treat the test results as Confidential Information of Kensu subject to the confidentiality requirements in the Agreement.

7. SHARING THE SECURITY RESPONSIBILITY

7.1 PRODUCT CAPABILITIES. The Products has the capabilities to: **(a)** authenticate Users before access; and **(b)** prevent access by Users with an inactive account. Customer manages each User's access to and use of the Products by assigning to each User a credential and user type that controls the level of access to the Products. Customer shall be responsible for implementing encryption and access control functionalities available within the Products for protecting all Customer Data, including the Customer Data containing, if any, personal data and sensitive data, including credit card numbers, social security and other government-issued identification numbers, financial and health information and any other personal data deemed sensitive or "special categories of personal data" under Data Protection Laws. Customer is solely responsible for its decision not to encrypt such data and Kensu will have no liability to the extent that damages would have been mitigated by Customer's use of such encryption measures. Customer is responsible for protecting the confidentiality of each User's login and password and managing each User's access to the Products.

7.2 CUSTOMER COOPERATION. Customer shall promptly apply any Update that Kensu determines is necessary to maintain the security, performance, or availability of the Products.

7.3 LIMITATIONS. Notwithstanding anything to the contrary in this Data Security Guide or other parts of the Agreement, Kensu's obligations extend only to those systems, networks, network devices, facilities, and components over which Kensu exercises control. This Data Security Guide does not apply to: **(a)** information shared with Kensu that is not Customer Data; **(b)** data in Customer's VPN or a third-party network; or **(c)** any data processed by Customer or its Users in violation of the Agreement or this Data Security Guide.