TREASURE DATA

STATEMENT OF TREASURE DATA'S SECURITY PRACTICES FOR CUSTOMER INFORMATION

June 2016

Introduction

Treasure Data, Inc. is committed to protecting the information of its customers and preventing unauthorized disclosure, use, modification, or access of or to the information customers store within the Treasure Data Service. We recognize the importance of appropriate information security policies and procedures to protect the security of customer data. We have therefore created this document to describe Treasure Data's security policies, procedures, and technologies. This statement is not itself the Treasure Data Security Policy, but does summarize the controls embodied in the Security Policy and some specific information concerning encryption, access control, and the authentication of users and administrators.

Treasure Data maintains different types of documentation in support of its information security program. In specific, Treasure Data maintains:

- Policies, such as the Treasure Data Security Policy, which are statements regarding Treasure Data's commitment to certain goals and statements of high level security requirements.
- Procedures, which are documented methods showing how Treasure Data meets the requirements set in policies.
- Standards, which detail the specifications for the technology or facilities that Treasure Data uses.
- Guidelines and other training materials, which provide information to educate workers and users about following the procedures established by Treasure Data to meet the goals set in its policies.

By "customer information," we are referring to information and data we receive, process, create, maintain, or transmit on behalf of a customer when delivering the Treasure Data service to a customer or other information and data customers otherwise provide to Treasure Data. For instance, customer information includes data customers upload, analyze, and store within the Treasure Data service. It also includes personal information about customer representatives.

In carrying out Treasure Data's commitment to protect the security of customer information, Treasure Data takes precautions to protect the confidentiality, integrity, and availability of customer information. Treasure Data protects customer information from loss, misuse, and authorized access, disclosure, alteration, or destruction by employing industry standard safeguards to implement the control objectives described in the Treasure Data Security Policy. More specifically, Treasure Data intends to maintain reasonable and appropriate administrative, physical, and technical safeguards to:

- Provide assurances of the integrity and confidentiality of customer information,

- Protect against any reasonably anticipated threats or hazards to the security or integrity of customer information, and unauthorized uses or disclosures of customer information, and
- Maintain compliance with the legal framework of requirements for the privacy and security of customer information.

Administrative Safeguards

Treasure Data maintains and periodically will update the Treasure Data Security Policy and the subordinate documentation described above to govern the security of its Treasure Data Service. Treasure Data trains its employees and, as applicable, contractors and vendors with access to customer information to understand and comply with the Security Policy and subordinate documentation.

Treasure Data regularly assess the threats to the confidentiality, integrity, and availability of customer information. It manages such risks by implementing specific safeguards that are, in light of the risks, reasonable and appropriate to protect customer information.

Treasure Data has designated a single individual to be the primary coordinator of, and accountable for, the information security function within the company. Treasure Data has established security-relevant roles and responsibilities and holds its personnel accountable for performing them. Such accountability includes imposing consequences for violations of security policies and procedures up to and including termination if appropriate.

Treasure Data uses appropriate agreements with members of its workforce and service providers acting as subcontractors in order to require them to protect the confidentiality of customer information. Under such agreements, Treasure Data requires any workers or service providers receiving customer information to maintain security controls over such customer information that are at least as stringent as those required by this security statement.

Treasure Data maintains policies concerning the acceptable uses of computing devices and media used to collect, use, store, archive, and dispose of customer information.

Members of the Treasure Data workforce with access to customer information have trusted roles within the company. Treasure Data implements screening procedures to provide assurances that workers hired to carry out trusted roles are trustworthy and competent for the roles they perform.

Treasure Data limits the access of members of its workforce to customer information. Workers with trusted roles are given access to customer information only if they need such access to perform their job responsibilities and the access they receive is the minimum needed to perform their roles. Members of Treasure Data's workforce with

limited access to customer information include personnel that provide customer support requiring such access, and they obtain such access only upon customer request.

Treasure Data maintains a program of security awareness and training for its workforce. Such training is required for personnel with trusted roles.

Treasure Data maintains termination procedures so that upon termination of a worker or service provider, Treasure Data will promptly remove all rights to access customer information, and obtain the return of media or devices that contain customer information.

Through appropriate agreements and management oversight, Treasure Data oversees the security of activities undertaken by service providers on behalf of Treasure Data. Treasure Data currently uses a variety of industry-leading third party data hosting companies as providers of storage and platform services. Our service providers have been certified as meeting the requirements under ISO 27001, as well as SOC 1/SSAE 16/ISAE 3402 (Previously SAS 70 Type II) and SOC 2.

Treasure Data will maintain and implement procedures to facilitate timely, effective, and orderly reporting and response to suspected or known information security incidents or breaches.

Treasure Data will maintain and periodically test disaster recovery and business continuity plans and procedures for responding to man-made threats and natural disasters that could damage systems that contain customer information or make them unavailable.

Treasure Data will audit or otherwise assess the security of Treasure Data's information systems containing customer information on a regular basis and check for compliance with the Security Policy, procedures implemented pursuant to the Security Policy, and technical standards.

Physical and Environmental Controls

As mentioned above, Treasure Data uses a variety of industry-leading third party data hosting companies to provide hosting services. These service providers host the Treasure Data Service in their data centers. These data centers maintain infrastructure in secured zones in accordance with the service providers' physical security control standards. These service providers protect their infrastructure against physical intrusion, loss, theft, damage, and reasonably anticipated natural disasters, such as floods and storms.

Our service providers host customer data at scalable, high-performance, and high-resilience data centers. They have security certifications under assessment frameworks such as ISO 217001 and Service Organization Control (SOC) 1, and SOC 2. These data centers maintain our customers' data in secured zones that protect against

physical intrusion, loss, theft, damage, and reasonably anticipated natural disasters, such as floods and storms. Their high availability and business continuity services provide assurances of continued reliability of our service. Our service providers operate multiple data centers, and customer information is replicated across data centers to enhance reliability.

Treasure Data's offices, in which personnel may access customer information using their workstations and computing devices are protected by physical security barriers, including walls and locked doors, as well as alarms and supervision by operational personnel, in accordance with Treasure Data's physical security control procedures and standards. Treasure Data trains its workers to prevent the theft or loss of computers, mobile devices, and media holding customer information, as well as unauthorized access to such devices and media.

Treasure Data maintains and enforces procedures and technical standards for the secure deletion of customer information from servers, computers, mobile devices, and media before it disposes of them or otherwise repurposes them. The third party data hosting service companies have similar procedures for the secure deletion of data from their infrastructure.

Technical Security Controls

Treasure Data maintains technical standards and procedures for hardware and software procurement and operations to minimize the risk of malicious software. Treasure Data will also use software and maintain procedures to detect, prevent security incidents, and recover from incidents involving malicious software. Treasure Data's security awareness and training also covers these procedures.

Treasure Data maintains controls used to update system and application software.

Treasure Data uses appropriate hardware and software, in accordance with its technical standards, to protect its networks against intrusion and data loss.

Treasure Data maintains the capability for its systems collecting, using, storing, and archiving customer information to produce and maintain audit logs of user activities, exceptions, and information security-relevant events. Treasure Data will maintain and implement technical standards relating to the generation, review, and storage of audit logs.

Treasure Data maintains reasonable and appropriate access control and authentication safeguards to control access to customer information. These safeguards provide assurances that only those Treasure Data personnel given access to customer information by management can, in fact, access such data. Information processing facilities will authenticate users seeking to obtain access to customer information in accordance with the procedures and technical mechanisms consistent with Treasure Data's authentication procedures and technical standards.

Treasure Data's Service permits customers to control access to customer information by its users. Data stored in tables in the Treasure Data Service are protected by permissions that can be set on a user-by-user basis. Tables can be grouped into collections called databases, and any non-administrator user in a customer's account can be set to have: No Access, Write-Only Access, Read-Only Access, or Read/Write Access to the tables in each database. This gives a customer the ability to assign different members of its work teams to work on different projects, where each project is a collection of tables in a database, and where each team only has access to its own project.

The Treasure Data Service has built-in integration with SAML-based SaaS Single-Sign-On (SSO) services such as OneLogin (www.onelogin.com). These services replace the traditional password-based authentication when logging into the Treasure Data Service.

Treasure Data maintains technical specifications for technology and will maintain procedures to provide assurances of the integrity of customer information over time to maintain the data's reliability and authenticity. Such technology and procedures will be used to protect customer information from undetected alteration, corruption, loss, or destruction.

All data sent from the Treasure Data collectors (td-agent, Mobile SDKs, Javascript SDK, bulk import tool, and data connector) is sent to the Treasure Data Service through an encrypted transport layer security (TLS v1) tunnel by default. Data sent from the Treasure Data Service to external destinations are also sent through encrypted tunnels when the destination is setup for TLS/SSL encryption by default. Where encrypted transport is not default and requires additional configuration for the customer, encrypted transport is optional. Encryption algorithms and key lengths will be consistent with Treasure Data's policies on encryption:

- We use TLS/SSL sessions to secure its data transmissions by default.
- The default certificates for these sessions have RSA-2048 keys, use SHA-256 digests, and facilitate AES-256 symmetric key encryption.

Regarding the portion of the Treasure Data Service hosted by third party data hosting companies, these service providers maintain similar technical safeguards protecting customer information. These third party data hosting services use firewalls and other devices to maintain an external network boundary to prevent unauthorized access and intrusion. They employ continuous monitoring systems to detect suspicious or unauthorized activities. Our customers' administrators can provision and manage user accounts within their organization.

Although we provide our services on a centralized basis to allow our customers to share our infrastructure, the Treasure Data Service keeps each customer's customer information separate from the customer information of every other customer by our implemented access control policies. In turn, our service providers use security controls to segregate the Treasure Data Service from their other customers' data by maintaining

the Treasure Data Service in its own protected environment. Our security controls provide assurances against unauthorized access to customers' accounts, whether by those who do not use the Treasure Data Service or other Treasure Data customers.

Treasure Data manages the security lifecycle of the application supporting the Treasure Data Service and all other in-house developed software in order to prevent, detect, and correct security weaknesses.

Contact Information and Resolving Disputes

If you would like to discuss this security statement or provide us with feedback, questions, or concerns about our security statement, please contact us by email at ar@treasure-data.com. You may also write us at:

Treasure Data, Inc.
2565 Leghorn Street
Mountain View, CA 94043
Attention: Security

If you have a complaint about our customer information security practices, you may submit a complaint to us at the above contact information. Our security team will look into your complaint and provide a response. You will need to provide sufficient information for us to evaluate your complaint and we may ask you to provide additional information as a condition of evaluating your complaint.

Changes to This Security Statement

We reserve the right to make changes to this security statement from time to time. If we make a change to the security statement, we will post a new copy of it on our website. Your continued use of the Treasure Data Service after such notification indicates your continued agreement to the terms of this security statement as amended. Please review this security statement to review the latest information about our security practices for handling customer information.