FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions
Treasure Data Response, June 2020

Control Guidelines		
1. Internal Control		
Guidelines	**Applicability**	**Treasure Data Response**
(1) Policy/Plan		
C1	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 5.1.1 (Security Policies) SOC 2: CE-01 Description: Management maintains a set of policies and standards that is made available to staff on the Treasure Data intranet, and all policies are assigned a document owner and are reviewed or updated and approved at least annually. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
C2	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 5.1.1 (Security Policies) SOC 2: CE-01, CE-10 Description: Management maintains a set of policies and standards that is made available to staff on the Treasure Data intranet, and all policies are assigned a document owner and are reviewed or updated and approved at least annually. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.

C3	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 14.2 (System acquisition, development and maintenance) SOC 2: CM-01, CM-05 Description: Treasure Data maintains a comprehensive Information Security Management System, including risk management practices. We follow a Secure Software Development Lifecycle process with the Engineering. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.

(2) Organizational Structure		
C4	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 5.1 (Security Policies), 6.1.1, 6.1.2, 6.1.5 (Organization of information security), 7.2.1 (Human resource security), 15.1.1 (Supplier relationships), 16.1.1 (Information security incident management), 14.1.1, 14.2.5, 14.2.6 (System acquisition, development and maintenance) SOC 2: CE-01, CE-10, IC-06 Description: Treasure Data maintains a comprehensive Information Security Management System, including risk management practices. We follow a Secure Software Development Lifecycle process with the Engineering. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
C5	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.1, 12.6.1 (Operations security), 13.1.1 (Communications security), 16.1.1(Information security incident management) Description: Treasure Data maintains a comprehensive Information Security Management System, including risk management practices. We follow a Secure Software Development Lifecycle process with the Engineering. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.

	C6	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.1, 12.1.2, 12.1.4 (Operations security), 13.1.1 (Communications security) Description: We maintain an Information Security Management System policy along with Change control and configuration Management Plan and Information Classification and Protection policy. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
	C7	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 6.1.2 (Operations security), 9.1.1(Access control), 13.2.1, 13.2.3 (Communications security), 14.1.3 (System acquisition, development and maintenance), 17.2.1 (Information security aspects of business continuity management) Description: Treasure Data has a mature and highly scalable data management system that can be used for data unification, transformation, and activation towards the Customer Data platform. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
	C8	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 6.1.2 (Operations security), 9.1.1, 9.1.2 (Access control), 13.1.1, 13.1.2 (Communications security) Description: Treasure Data has a Network Security Management process in place. It maintains Change control and configuration Management Plan and Information Classification and Protection policy. AWS Virtual Private Cloud and Security Groups are used to perform the firewall function. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
	C9	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 6.1.1, 6.1.2 (Operations security) Description: Treasure Data has an Information Security Management System in place with well-defined roles and responsibilities. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the development of operational guidance.

C10	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 17.1.1, 17.1.2 (Information security aspects of business continuity management) SOC 2: AV-06, AV-07, AV-08 Description: The recovery process for compute nodes follows the standard deployment process which is performed daily. Restore testing of transaction data backups is performed annually in a non-production environment. The disaster recovery procedures are maintained internally and documented in the Disaster Recovery Management Plan and Backup Management Plan. Treasure Data is based on Amazon AWS infrastructure. The RTO/RPO is dependent on the type and scale of the disaster and largely relies on Amazon's ability to recover. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
C11	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 7 (Human Resources Security) SOC 2: CE-02, IC-06 Description: Treasure Data has a Code of Conduct, Social Media, Anti Bribery, etc. policies in place and acknowledged by all staff members. Security awareness training is required upon new hire on-boarding and thereafter, all employees must complete security awareness training annually. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the development of operational guidance.

C12	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 5.1.1 (Security Policies) SOC 2: CE-01, CE-10 Description: Management maintains a set of policies and standards that is made available to staff on the Treasure Data intranet, and all policies are assigned a document owner and are reviewed or updated and approved at least annually. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the development of operational guidance.
(3) Evaluation of management status		

C13	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 5.1.1 (Security Policies), 7.2.1, 7.2.2 (Human resource security), 15.1.1, 15.2.1 (Supplier relationships), 18.2.1, 18.2.2, 18.2.3 (Compliance) SOC 2: CE-01, CE-10, RA-04, RM-01, RM-02 Description: Management maintains a set of policies and standards that is made available to staff on the Treasure Data intranet, and all policies are assigned a document owner and are reviewed or updated and approved at least annually. Treasure Data has a Code of Conduct, Social Media, Anti Bribery, etc. policies in place and acknowledged by all staff members. Security awareness training is required upon new hire on-boarding and thereafter, all employees must complete security awareness training annually. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the development of operational guidance.
(4) Personnel (Staffing/Training)		
C14	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 7.2.1, 7.2.2 (Human resource security) SOC 2: CE-01, IC-06 Description: Security awareness training is required upon new hire on-boarding and thereafter, all employees must complete security awareness training annually.

C15	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 7.2.2 (Human resource security) SOC 2: CE-16 Description: Security awareness training is required upon new hire on-boarding and thereafter, all employees must complete security awareness training annually. An internal training curriculum for departmental-specific courses is maintained by HR.
C16	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 7.2.2 (Human resource security) SOC 2: CE-16 Description: Security awareness training is required upon new hire on-boarding and thereafter, all employees must complete security awareness training annually. An internal training curriculum for departmental-specific courses is maintained by HR.

C17	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 7.2.2 (Human resource security) SOC 2: CE-16 Description: Security awareness training is required upon new hire on-boarding and thereafter, all employees must complete security awareness training annually. An internal training curriculum for departmental-specific courses is maintained by HR.
C18	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 7.2.1, 7.2.2 (Human resource security) SOC 2: CE-02 Description: Treasure Data has a Code of Conduct, Social Media, Anti Bribery, etc. policies in place and acknowledged by all staff members. Security awareness training is required upon new hire on-boarding and thereafter, all employees must complete security awareness training annually. An internal training curriculum for departmental-specific courses is maintained by HR. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including human resource management.
C19	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 7.2.1, 7.2.2 (Human resource security) SOC 2: CE-02 Description: Every employee is provided with the Company’s Code of Business Conduct and Ethics and completes periodic Security Awareness training which requires an acknowledgment to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies.
2. External control		
Guidelines	**Applicability**	**Treasure Data Response**
(1) Outsourcing management		

	C20	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 7.1.1 (Human resource security), 15.1.1, 15.1.2, 15.1.3 (Supplier relationships) SOC 2: IC-01, RA-04, RM-02, RM-03 Description: Treasure Data suppliers are evaluated based on the type of service they provide and the type of data that they may store or process on behalf of Treasure Data. Contracts are structured to require an appropriate minimum level of security. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
	C21	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 13.2.4 (Communication security), 15.1.1, 15.1.2 (Supplier relationships) SOC 2: IC-01, IC-08, RM-03 Description: Treasure Data suppliers are evaluated based on the type of service they provide and the type of data that they may store or process on behalf of Treasure Data. Contracts are structured to require an appropriate minimum level of security. Non-Disclosure Agreements are signed between the supplier and Treasure Data with Data Handling and confidentiality clause included. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
	C22	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 15.1.1, 15.1.2, 15.2.1 (Supplier relationships) SOC 2: RA-04, RM-01, RM-02 Description: Treasure Data suppliers are evaluated based on the type of service they provide and the type of data that they may store or process on behalf of Treasure Data. Contracts are structured to require an appropriate minimum level of security. We have defined controls in our Security and Privacy Questionnaire to which the supplier needs to comply with.
	C23	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 15.2.1, 15.2.1 (Supplier relationships) SOC 2: RA-04, RM-01,RM-02 Description: Treasure Data suppliers are evaluated based on the type of service they provide and the type of data that they may store or process on behalf of Treasure Data. Contracts are structured to require an appropriate minimum level of security. Non-Disclosure Agreements are signed between the supplier and Treasure Data with Data Handling and confidentiality clause included. We have a Third-Party Security Assessment Monitoring tool to monitor the performance of suppliers regularly.

(2) Use of cloud services		
C24	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: SOC 2: RM-01 Description: Treasure Data suppliers are evaluated based on the type of service they provide and the type of data that they may store or process on behalf of Treasure Data. Contracts are structured to require an appropriate minimum level of security. We have Third-Party Security and Privacy Assessment for all the cloud providers performed where the risk level is determined, monitored and remediated if required. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
(3) Shared data center		
C25	N/A	Treasure Data CDP solution will be hosted on AWS and cannot be deployed on-premise. We are a cloud solution.
(4) Services on financial institutions' mutual system network		
C26	N/A	Treasure Data does not maintain financial transaction software for customers. The responsibility of maintaining CD/ATM networks remains with the customer.

Practice Guidelines

1. Information security

Guidelines	Applicability	Treasure Data Response
(1) Data protection		
P1	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9.3.1, 9.4.3 (User responsibilities) SOC 2: LP-07, LP-08 Description: Treasure Data has a variety of security and privacy features for managing personal identifiers. First, as your data processor, we have a suite of tools that help you achieve GDPR compliance. Our onsite tracking code can easily be configured to prevent the collection of cookie IDs and other P2 data. Password policy on your Treasure Data account is provided as a feature for Administrators to govern and maintain. Complexity, length, aging, session length, expiration period, number of previous passwords remembered, maximum attempts are all features that you can set for your Treasure Data account. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.

P2	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9 (User responsibilities) SOC 2: LP-07, LP-08 Description: Treasure Data has a variety of security and privacy features for managing personal identifiers. First, as your data processor, we have a suite of tools that help you achieve GDPR compliance. Our onsite tracking code can easily be configured to prevent the collection of cookie IDs and other P2 data. Password policy on your Treasure Data account is provided as a feature for Administrators to govern and maintain. Complexity, length, aging, session length, expiration period, number of previous passwords remembered, maximum attempts are all features that you can set for your Treasure Data account. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
P3	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 8.3.1, 8.3.3 (Asset management), 9.1.1 (User responsibilities), 10.1.1 (Cryptography), 11.2.6 (Physical and environmental security), 18.1.3 (Compliance) SOC 2: CA-4, CE-10, LP-18, LP-20, RM-03 Description: Treasure Data Customer Data is stored in secure buckets and is only used for the purposes described in the ToS and/or MSA. Customer data is not removed from the system without prior consent. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the development of appropriate encryption measures.

P4	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 10.11 (Cryptography), 13.1.1, 13.1.2, 13.2.3 (Communication security), 14.1.2,14.1.3 (System acquisition, development and maintenance), 15.1.3 (Supplier relationships), 18.1.3 (Compliance) SOC 2: CF-01 Description: Treasure Data Customer Data is stored in secure buckets and is only used for the purposes described in the ToS and/or MSA. Customer data is not removed from the system without prior consent. All data is encrypted at rest and in transit. Encryption protocols are TLS/SSL, AES, Bcrypt, AES-256. We provide additional encryption options at the application level such as Encryption, Hashing, MD5, SHA128, and SHA256. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the development of appropriate encryption measures.

P5	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9.1.1, 9.1.2, 9.2.1, 9.2.5 (Access control) SOC 2: CA-04, LP-06, LP-09 Description: Treasure Data includes policy-based access control that allows admins to create specific access policies and apply them to multiple sets of Treasure Data users in bulk. Access policies can be defined at a fine grain of control, allowing administrators to set read/write privileges across the analyst console, databases, segments, and master segments (audiences). Segregation of duties, including administrator-level access, is enforced at the level of the user directory service, where user group membership determines an employee's access to systems. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.
P6	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 14.1.3 (System acquisition, development and maintenance) SOC 2: SO-03 Description: CDP REST APIs support secure transfer over HTTPS to avoid tampering and disclosure of data. Customer Data is encrypted at rest by default and transferred over encrypted channels (HTTPS/TLS). All data transfers, inbound or outbound, are secured as occurring through HTTPS. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.

P7	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 14.1.3 (System acquisition, development and maintenance) SOC 2: SO-03 Description: CDP REST APIs support secure transfer over HTTPS to avoid tampering and disclosure of data. Customer Data is encrypted at rest by default and transferred over encrypted channels (HTTPS/TLS). All data transfers, inbound or outbound, are secured as occurring through HTTPS. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.
(2) Prevention of unauthorized use		

P8	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9.2.4, 9.3.1, 9.4.2, 9.4.3 (Access control) SOC 2: LP-07, LP-08 Description: Treasure Data has a variety of security and privacy features for managing personal identifiers. First, as your data processor, we have a suite of tools that help you achieve GDPR compliance. Our onsite tracking code can easily be configured to prevent the collection of cookie IDs and other P2 data. We can also integrate with your existing consent management platform to comply with GDPR policies. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
P9	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9.1.1, 9.4.2, 9.4.3 (Access control) SOC 2: LP-07, LP-08, CA-04 Description: Treasure Data has a variety of security and privacy features for managing personal identifiers. First, as your data processor, we have a suite of tools that help you achieve GDPR compliance. Our onsite tracking code can easily be configured to prevent the collection of cookie IDs and other P2 data. We can also integrate with your existing consent management platform to comply with GDPR policies. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
P10	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9 (Access control) SOC 2: LP-12, SO-03 Description: Treasure Data includes policy-based access control that allows admins to create specific access policies and apply them to multiple sets of Treasure Data users in bulk. Access policies can be defined at a fine grain of control, allowing administrators to set read/write privileges across the analyst console, databases, segments, and master segments (audiences). Segregation of duties, including administrator-level access, is enforced at the level of the user directory service, where user group membership determines an employee's access to systems. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
P11	Yes	Treasure Data customers retain the right and responsibility to restrict transactions.
P12	Yes	Treasure Data customers retain the right and responsibility to restrict transactions.

P13	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 10.1.1 (Cryptography), 12.1.2 (Operations security) SOC 2: LP-08 Description: Treasure Data has Encryption policy and Technical standard in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the development of appropriate encryption measures.
(3) Set up functions for protection against unauthorized access from external network		
P14	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.2 (Operations security), 13.1.1, 13.1.2, 13.1.3 (Communications security), 14.1.2 (System acquisition, development and maintenance) SOC 2: LP-01, LP-03, LP-09 Description: Treasure Data has a Network Security Management process in place. It maintains Change control and configuration Management Plan and Information Classification and Protection policy. AWS Virtual Private Cloud and Security Groups are used to perform the firewall function. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.

P15	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 13.1.1, 13.1.2, 13.1.3 (Communications security) SOC 2: LP-05 Description: Treasure Data has a Network Security Management process and Remote Working Standard in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
(4) Measures to detect unauthorized access		

P16	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.4.1, 12.4.2, 12.4.4 (Operations security), 13.1.1 (Communications security) SOC-2: LP-02,LP-12 Description: Treasure Data has an Access Management Plan in place. It has established formal policies, procedures to delineate the minimum standards for logical access to Treasure Data resources. We have controls in place to manage access provisioning to Treasure Data resources. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
P17	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.4.1, 12.4.2, 12.4.4 (Operations security), 13.1.1 (Communications security) SOC-2: LP-02,LP-12 Description: Treasure Data has an Access Management Plan in place. It has established formal policies, procedures to delineate the minimum standards for logical access to Treasure Data resources. We have controls in place to manage access provisioning to Treasure Data resources. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
P18	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.4.1, 12.4.2, 12.4.4 (Operations security), 13.1.1 (Communications security) SOC-2: LP-02,LP-12 Description: Treasure Data has an Access Management Plan in place. It has established formal policies, procedures to delineate the minimum standards for logical access to Treasure Data resources. We have controls in place to manage access provisioning to Treasure Data resources. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
(5) Response measures for unauthorized access		

P19	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 16.1.1, 16.1.2, 16.1.3, 16.1.4, 16.1.5 (Information security incident management) SOC 2: LP-01, LP-04, LP-06 Description: Treasure Data has controls in place to monitor unauthorized access and report non-compliances. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
(6) Measures against malicious programs		
P20	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.2.1, 12.6.1 (Operations security) SOC 2: LP-23 Description: Treasure Data has monitoring controls in place to detect, prevent and recover from potential malicious activity and if requiring an incident response, the Incident Response Plan would be activated.
P21	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9.1.1 (Access control), 12.2.1, 12.4.1, 12.6.1 (Operations security) SOC 2: LP-23 Description: Treasure Data has monitoring controls in place to detect, prevent and recover from potential malicious activity and if requiring an incident response, the Incident Response Plan would be activated.

P22	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 16.1.1, 16.1.2, 16.1.3, 16.1.4, 16.1.5 (Information security incident management) SOC 2: LP-01, LP-04 , LP-06 Description: Treasure Data has monitoring controls in place to detect, prevent and recover from potential malicious activity and if requiring an incident response, the Incident Response Plan would be activated.

2. Common guidelines for system operations

Guidelines	Applicability	Treasure Data Response
(1) Documentation		
P23	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.1 (Operations security) Description: Treasure Data has monitoring controls in place to detect, prevent and recover from potential malicious activity and if requiring an incident response, the Incident Response Plan would be activated. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the development of operational guidance.
P24	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.1, 17.1.1, 17.1.2 (Operations security) SOC 2: AV-06 Description: The disaster recovery procedures are maintained internally and documented in the Disaster Recovery Management Plan and Backup Management Plan. Treasure Data is based on Amazon AWS infrastructure. The RTO/RPO is dependent on the type and scale of the disaster and largely relies on Amazon's ability to recover. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the development of operational guidance.
(2) Management of access rights		
P25	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 8.1.2 (Asset management), 9.1.1, 9.2.2, 9.2.3, 9.4.1 (Access control) SOC 2: CE-10 Description: Treasure Data has policy-based access control, similar in feature set to role-based permissions. Along with an SSO based authentication mechanism. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the development of operational guidance.

P26	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9.4.3 (Access control) SOC 2: LP-07, LP-08 Description: Password policy on Treasure Data account is provided as a feature for Administrators to govern and maintain. Complexity, length, aging, session length, expiration period, number of previous passwords remembered, maximum attempts are all features that you can set for Treasure Data account. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
P27	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013: Annex 9.1.1, 9.2.1, 9.2.2, 9.2.3, 9.2.5, 9.2.6, 9.4.1 (Access control) SOC 2: CE-10, LP-01, LP-06, LP-09 Description: Treasure Data has an Access Management plan, Information classification and protection policy in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
(3) Data management		

P28	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 8.1.2, 8.3.2 (Asset management) SOC 2: CF-01 Description: Treasure Data does not store files on our platform, but the actual data from the files. The rules around encryption and archival of that data follow the same rules as all other data. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support input management activities.

P29	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.3.1 (Operations security) SOC 2: CF-01 Description: Treasure Data has Backup Management Plan in place, and engineering does yearly system restore. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support input management activities.
P30	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 10.1.2 (Cryptography) Description: Treasure Data has Encryption Policy and Technical Standard in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing cryptographic key management processes.
(4) Operation proficiency		
P31	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 7.2.2 (Human resource security) SOC 2: IC-06 Description: Security awareness training is required upon new hire on-boarding and thereafter, all employees must complete security awareness training annually. An internal training curriculum for departmental-specific courses is maintained by HR.
(5) Computer Antivirus protection		

P32	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.2.1 (Operations security) SOC 2: LP-23, LP-25 Description: Treasure Data systems, we have extensive virus protection, and disc level encryption to safeguard data. We mitigate the risk of viruses through strict package management, firewalls, HIDS, and monitoring suspicious logs on the servers. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including configuring appropriate protective measures against viruses.
(6) External connection management		
P33	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 13.1.2, 13.2.2 (Communications security), 14.1.2 (Securing Application Service on Public Networks) Description: At Treasure Data by default, data in motion is protected by HTTPS/TLS 1.2 and data at rest is encrypted by AES 256 encryption. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment including management of external connections.
P34	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 6.2.2 (Organization of information security), 14.1.2 (Securing Application Service on Public Networks) Description: Treasure Data has a remote working standard in Place. By default, data in motion is protected by HTTPS/TLS 1.2 and data at rest is encrypted by AES 256 encryption. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment including the management of external connections.

3. Operation management

Guidelines	Applicability	Treasure Data Response
(1) Management of operations		

	P35	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9 (Access control) Description: Treasure Data has implemented various methods of internal communication to help employees understand their roles and responsibilities. These methods include orientation and training programs for newly hired employees, regular management meetings of updates on business performance and electronic means such as video conferencing, electronic mail messages and the posting of information via the Treasure Data Intranet. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
	P36	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9 (Access control) Description: Treasure Data has implemented various methods of internal communication to help employees understand their roles and responsibilities. These methods include orientation and training programs for newly hired employees, regular management meetings of updates on business performance and electronic means such as video conferencing, electronic mail messages and the posting of information via the Treasure Data Intranet. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
	P37	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9 (Access control) Description: Treasure Data has implemented various methods of internal communication to help employees understand their roles and responsibilities. These methods include orientation and training programs for newly hired employees, regular management meetings of updates on business performance and electronic means such as video conferencing, electronic mail messages and the posting of information via the Treasure Data Intranet. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.

P38	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 9 (Access control) Description: Treasure Data has implemented various methods of internal communication to help employees understand their roles and responsibilities. These methods include orientation and training programs for newly hired employees, regular management meetings of updates on business performance and electronic means such as video conferencing, electronic mail messages and the posting of information via the Treasure Data Intranet. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.
(2) Data file management		
P39	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.3.1 (Backup) Description: Treasure Data system is backed by a highly available and highly fault-tolerant infrastructure within Amazon Web Services. This data is backed up daily per the Backup Management Plan. Data is retained for 14 days and recovery from backup takes approximately 30 minutes. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.
(3) Program File management		
P40	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, A: 9.4.5 (Access control) Description: Treasure Data has an Access Management Plan in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to data and associated program files, including developing a process to support program file management activities.

P41	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.3.1 (Operations security) SOC 2: AV-02 Description: Treasure Data system is backed by a highly available and highly fault-tolerant infrastructure within Amazon Web Services. This data is backed up daily per the Backup Management Plan. Data is retained for 14 days and recovery from backup takes approximately 30 minutes. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support program file management activities.
(4) Network Configuration management		
P42	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 13.1.1 (Communications security) Description: Treasure Data has Change Control Management Plan in Place. Additionally, AWS Networks are managed, we use features such as VPC, security groups to protect and restrict access. Changes to network configuration are change controlled. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
P43	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.3.1 (Backup) Description: Treasure Data system is backed by a highly available and highly fault-tolerant infrastructure within Amazon Web Services. This data is backed up daily per the Backup Management Plan. Data is retained for 14 days and recovery from backup takes approximately 30 minutes. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
(5) Document management during operation		

P44	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.1 (Operations security), 18.1.3 (Compliance) SOC: Partially CE-10 Description: Treasure Data has Change Control and Configuration Management Plan in Place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities of their data and associated procedures for storage management of data.
P45	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.3.1 (Backup) Description: Treasure Data system is backed by a highly available and highly fault-tolerant infrastructure within Amazon Web Services. This data is backed up daily per the Backup Management Plan. Data is retained for 14 days and recovery from backup takes approximately 30 minutes. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support forms management.
(6) Monitoring of operations		
P46	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.4.1, 12.4.3 (Operations security) SOC 2: LP-12, LP-13 Description: We provide system monitoring dashboards within the product, so customers can understand their account utilization. We maintain an alerting framework for our system status which aids us in observing and operating the system at all times. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
4. Facilities management		
Guidelines	**Applicability**	**Treasure Data Response**
(1) Resource management		

P47	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 8.1.1 (Asset management), 12.1.3 (Operations security) SOC 2: AV-01, IC-02, IC-03 Description: Treasure Data has Capacity management control in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including resource management.
(2) Device management		
P48	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 8.1.1, 8.1.2, 8.1.3 (Asset management) SOC 2: IC-02, IC-03, AV-04 Description: Treasure Data CDP is a cloud-hosted, software-as-a-service (SaaS) solutions provider. No hardware or software is required, other than what is needed to connect to the internet with a web browser. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
P49	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 8.1.2 (Asset management), 11.1.1, 11.2.1, 11.2.6 (Physical and environmental security) Description: Treasure Data has Facilities Security Policy and Acceptable Use Policy in Place for device management. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
P50	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1, 11.2.3 (Physical and environmental security) Description: Treasure Data has AWS Virtual Private Cloud and Security Groups that are used to perform the firewall function. All data is encrypted in transit and at rest. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.

P51	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A:11.2.4 (Physical and environmental security) Description: Treasure Data has Facilities Security Policy and Acceptable Use Policy in Place for device management.
P52	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.4 (Physical and environmental security) Description: Treasure Data has Facilities Security Policy and Acceptable Use Policy in Place for device management.
(3) Maintenance and management of computer-related equipment		
P53	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.1, 11.1.2, 11.1.5, 11.2.1 (Physical and environmental security), 12.1.1(Operation Security) Description: Treasure Data has Facilities Security Policy in Place for managing computer-related equipment. It monitors electrical, mechanical, physical security and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed by the IT to maintain the continued operability of equipment.
P54	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.4 (Physical and environmental security) Description: Treasure Data has Facilities Security Policy in Place for managing computer-related equipment. It monitors electrical, mechanical, physical security and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed by the IT to maintain the continued operability of equipment.
P55	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.3 (Operations security) Description: Treasure Data has the Capacity Management control in place to check the capacities and usage of computer-related equipment. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
(4) Physical access control (building and rooms)		

P56	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.2, 11.1.3 (Physical and environmental security) Description: Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.
P57	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.2 (Physical and environmental security) Description: Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.
P58	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.3 (Physical and environmental security) Description: Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.
P59	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.5 (Physical and environmental security) Description: Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic Information Security training which requires an acknowledgment to complete.
(5) Monitoring		
P60	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1, 11.2.3 (Physical and environmental security) Description: Treasure Data monitors electrical, mechanical, physical security and life support systems and equipment so that any issues are immediately identified. It has video surveillance for continuous monitoring.

5. Use of systems

Guidelines	Applicability	Treasure Data Response
(1) Transaction management		
P61	N/A	Treasure Data Customers retain the ownership for their data and associated measures of transaction management.
P62	N/A	Treasure Data Customers retain the ownership for their data and associated measures of transaction management.
P63	N/A	Treasure Data Customers retain the ownership for their data and associated measures of transaction management.
P64	N/A	Treasure Data Customers retain the ownership for their data and associated measures of transaction management.
(2) Input/output management		
P65	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 14 (System Acquisition, Development and Maintenance) Description: Treasure Data has an Information Security Management System Policy, Change Control and Configuration Management Plan, Information Security Policy, Information Classification and Protection Policy, Secure Software Development Lifecycle in place. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including developing a process to support input management activities.
P66	N/A	Treasure Data Customers retain the ownership for their data and associated measures or management of handling output information.
(3) Forms management		
P67	N/A	Treasure Data Customers retain control and ownership of their data and associated forms.
P68	N/A	Treasure Data Customers retain control and ownership of their data and associated forms.
(4) Protection of customer data		

P69	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 17.2 (Redundancies), 12.3 (Backup) SOC 2: LP-18 Description: The system accepts the data in the form that it is uploaded by the customer and we protect all data to the same level of security and confidentiality. That is, we do not identify P2 within customer data sets. Rather we treat all data as if it required the highest level of security and confidentiality. All data is encrypted in transit and at rest. Only appropriate authorized personnel may access customer data, and typically only at the request of the customer. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
6. Emergency responses		
Guidelines	**Applicability**	**Treasure Data Response**
(1) Measure for handling failures and disasters, Responsive measures		
P70	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 16.1.1, 16.1.2 (Information security incident management) SOC 2: AV-08 Description: The recovery process for compute nodes follows the standard deployment process which is performed nearly daily. Restore testing of transaction data backups is performed annually in a non-production environment. The disaster recovery procedures are maintained internally and documented in the Disaster Recovery Management Plan and Backup Management Plan. Treasure Data is based on Amazon AWS infrastructure. The RTO/RPO is dependent on the type and scale of the disaster and largely relies on Amazon's ability to recover. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

P71	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 17.1.1, 17.1.2 (Information security aspects of business continuity management), 12.3.1 (Operations security) Description: The recovery process for compute nodes follows the standard deployment process which is performed nearly daily. Restore testing of transaction data backups is performed annually in a non-production environment. The disaster recovery procedures are maintained internally and documented in the Disaster Recovery Management Plan and Backup Management Plan. Treasure Data is based on Amazon AWS infrastructure. The RTO/RPO is dependent on the type and scale of the disaster and largely relies on Amazon's ability to recover. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
P72	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 16.1.1, 16.1.2 (Information security incident management) SOC 2: AV-08 Description: Treasure Data security incident response process is a multi-step process that involves, among other things, notification of the security incident response team, verification and evaluation of the incident, documentation of actions, determination of timeline and scope, and further notification of appropriate personnel. Following those initial actions, the impact is evaluated, the evidence is collected and preserved, corrective measures are determined and executed, and learnings are recorded. Response to any security incident follows our documented Security Incident Management Plan. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
(2) Formulation of contingency plans		

P73	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 17.1.1 (Information security aspects of business continuity management) Description: At Treasure Data, the Business Continuity Management Plan is maintained internally in conjunction with the Disaster Recovery Management Plan. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including developing appropriate contingency plans.
(3) Backup centers		

P74	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 17.2.1 (Information security aspects of business continuity management) SOC 2: AV-09 Description: The Treasure Data CDP is backed by a highly available and highly fault-tolerant infrastructure within Amazon Web Services' provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones as distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.

7. System development and modification

Guidelines	Applicability	Treasure Data Response
(1) Management of the development and modification of the systems		
P75	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 6.1.5 (Organization of information security), 12.1.1,12.1.2,12.5.1 (Operations security), 14.2.1, 14.2.2, 14.2.4, 14.2.5, 14.2.6 (System acquisition, development and maintenance) Description: Treasure Data has Vendor Management Policy, Information Security Management System Policy, Change Control and Configuration Management Plan, Information Security Policy, Information Classification and Protection Policy, Secure Software Development Lifecycle in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.

P76	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.4 (Operations security) Description: The TREASURE DATA multitenant system can provide the necessary tenant isolation that is necessary to segregate production and non-production (one or more) workloads. Separate databases, workflows, and API keys can be created to separate a development environment and a production environment Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.

P77	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.1 (Operations security), 14.2.2, 14.2.8, 14.2.9 (System acquisition, development and maintenance) SOC 2: CM-01, CM-04 Description: Treasure Data has Vendor Management Policy, Information Security Management System Policy, Change Control and Configuration Management Plan, Information Security Policy, Information Classification and Protection Policy, Secure Software Development Lifecycle in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment.
(2) Document management during development and modification		
P78	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.2 (Operations security) Description: Treasure Data has an Information Security Management System Policy and Change Control, and Configuration Management Plan in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the management of system documents.
P79	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 5 (Operations security), 6 (Organization of information security) SOC 2: CM-01, CM-04 Description: Treasure Data has an Information Security Management System Policy and Change Control, and Configuration Management Plan in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including storage management procedures.
(3) Package installation		
P80	N/A	Treasure Data Customers retain control of their own guest operating systems, software and applications and are responsible for managing packages.
P81	N/A	Treasure Data Customers retain control of their own guest operating systems, software and applications and are responsible for managing packages.
(4) Disposal of systems		

P82	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 8.3.2 (Asset Management), 11.2.7 (Physical and environmental security) SOC 2: AV-09 Description: Treasure Data has an Information Classification and Protection Policy Facilities Security Policy and Acceptable Use Policy in place for the disposal plan for the system.
P83	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 8.3.2 (Asset Management), 11.2.7 (Physical and environmental security) Description: Treasure Data has an Information Classification and Protection Policy Facilities Security Policy and Acceptable Use Policy in place to prevent leakage during the system disposal.

8. Measures to improve system reliability

Guidelines	Applicability	Treasure Data Response
(1) Backup for hardware		
P84	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 17.1.1, 17.1.2, 17.2.1 (Information security aspects of business continuity management) Description: The Treasure Data Customer Data Platform is backed by a highly available and highly fault-tolerant infrastructure within Amazon Web Services. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

	P85	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 17.1.1, 17.1.2, 17.2.1 (Information security aspects of business continuity management) Description: The Treasure Data CDP is backed by a highly available and highly fault-tolerant infrastructure within Amazon Web Services. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
	P86	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 17.1.1, 17.1.2, 17.2.1 (Information security aspects of business continuity management) Description: The Treasure Data CDP is backed by a highly available and highly fault-tolerant infrastructure within Amazon Web Services. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
	P87	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 17.1.1, 17.1.2, 17.2.1 (Information security aspects of business continuity management) Description: The Treasure Data CDP is backed by a highly available and highly fault-tolerant infrastructure within Amazon Web Services. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

P88	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 17.1.1, 17.1.2, 17.2.1 (Information security aspects of business continuity management) Description: The Treasure Data CDP is backed by a highly available and highly fault-tolerant infrastructure within Amazon Web Services. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. Treasure Data Customers retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
(2) Measures to improve the quality of software		
P89	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.5.1 (Operations security), 14.1.1, 14.2.1, 14.2.5 (System acquisition, development and maintenance) Description: Treasure Data has a process in place for monitoring the unauthorized software and maintains a whitelist of the software's also have Information Security Management System Policy and Information Classification and Protection Policy in place to apply security measures for the software installed. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, Including managing their system development process.
P90	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 14.1.1, 14.2.1 (System acquisition, development and maintenance) Description: Treasure Data has Information Security Management System Policy, Change Control, and Configuration Management Plan, Secure Software Development Lifecycle, and Information Classification and Protection Policy in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.

	P91	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.5.1 (Operations security) ,14.2.1, 14.2.5 (System acquisition, development and maintenance) Description: Treasure Data has Information Security Management System Policy, Change Control and Configuration Management Plan, Secure Software Development Lifecycle and Information Classification and Protection Policy in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
	P92	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 14.2.8, 14.2.9 (System acquisition, development and maintenance) Description: Treasure Data has Information Security Management System Policy, Change Control and Configuration Management Plan, Secure Software Development Lifecycle and Information Classification and Protection Policy in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment. Including managing their system development process.
	P93	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.5.1 (Operations security) Description: Treasure Data has Information Security Management System Policy, Change Control and Configuration Management Plan, Secure Software Development Lifecycle and Information Classification and Protection Policy in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment including managing their system development process.
	P94	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.5.1 (Operations security) Description: Treasure Data has a process in place for monitoring the unauthorized software and maintains a whitelist of the software's also have Information Security Management System Policy and Information Classification and Protection Policy in place to apply security measures for the software installed. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.

	P95	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.2 (Operations security), 14.2.2 (System acquisition, development and maintenance) Description: Treasure Data has a process in place for monitoring the unauthorized software and maintains a whitelist of the software's also have Information Security Management System Policy and Information Classification and Protection Policy in place to apply security measures for the software installed. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including managing their system development process.
	P96	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.2 (Operations security), 14.2.2, 14.2.3, 14.2.4 (System acquisition, development and maintenance) SOC 2: CM-04, CM-06 Description: Treasure Data has a process in place for monitoring the unauthorized software and maintains a whitelist of the software's also have Information Security Management System Policy and Information Classification and Protection Policy in place to apply security measures for the software installed. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
	P97	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.2 (Operations security), 14.2.2, 14.2.3, 14.2.4 (System acquisition, development and maintenance) SOC 2: CM-04, CM-06 Description: Treasure Data has a process in place for monitoring the unauthorized software and maintains a whitelist of the software's also have Information Security Management System Policy and Information Classification and Protection Policy in place to apply security measures for the software installed. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.

P98	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.2 (Operations security), 14.2.2, 14.2.3, 14.2.4 (System acquisition, development and maintenance) SOC 2: CM-04, CM-06 Description: Treasure Data has Information Security Management System Policy, Change Control and Configuration Management Plan, Secure Software Development Lifecycle and Information Classification and Protection Policy in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including the configuration of specific monitoring to detect false or unverified data.
(3) Measure to improve operational reliability		
P99	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A:14.2 (System acquisition, development and maintenance) SOC 2: CM-04, CM-06 Description: Treasure Data has Information Security Management System Policy, Change Control and Configuration Management Plan, Secure Software Development Lifecycle and Information Classification and Protection Policy in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.
P100	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 14.2 (System acquisition, development and maintenance) SOC 2: CM-04, CM-06 Description: Treasure Data has Information Security Management System Policy, Change Control and Configuration Management Plan, Secure Software Development Lifecycle and Information Classification and Protection Policy in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.

P101	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 14.2 (System acquisition, development and maintenance) SOC 2: CM-04, CM-01 Description: Treasure Data has Information Security Management System Policy, Change Control and Configuration Management Plan, Secure Software Development Lifecycle and Information Classification and Protection Policy in place. Treasure Data Customers using the Customer Data Platform retain all rights and responsibilities to configure and manage their environment, including system development procedures.
(4) Functions for early failure detection and recovery		
P102	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.4.1, 12.4.3 (Operations security) Description: Treasure Data has Information Security Management System Policy, Change Control and Configuration Management Plan, Secure Software Development Lifecycle and Information Classification and Protection Policy in place.
P103	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 16.1.1, 16.1.2, 16.1.4 (Information security incident management) Description: The security incident response process is a multi-step process that involves, among other things, notification of the security incident response team, verification, and evaluation of the incident, documentation of actions, determination of timeline and scope, and further notification of appropriate personnel. Following those initial actions, the impact is evaluated, the evidence is collected and preserved, corrective measures are determined and executed, and learnings are recorded. This process is documented in the Security Incident Management Plan.
P104	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 16.1.1, 16.1.2, 16.1.4 (Information security incident management) Description: The security incident response process is a multi-step process that involves, among other things, notification of the security incident response team, verification, and evaluation of the incident, documentation of actions, determination of timeline and scope, and further notification of appropriate personnel. Following those initial actions, the impact is evaluated, the evidence is collected and preserved, corrective measures are determined and executed, and learnings are recorded. This process is documented in the Security Incident Management Plan.

P105	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 16.1.1, 16.1.2, 16.1.4 (Information security incident management) Description: The security incident response process is a multi-step process that involves, among other things, notification of the security incident response team, verification, and evaluation of the incident, documentation of actions, determination of timeline and scope, and further notification of appropriate personnel. Following those initial actions, the impact is evaluated, the evidence is collected and preserved, corrective measures are determined and executed, and learnings are recorded. This process is documented in the Security Incident Management Plan.
P106	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 16.1.5 (Information security incident management) Description: The security incident response process is a multi-step process that involves, among other things, notification of the security incident response team, verification, and evaluation of the incident, documentation of actions, determination of timeline and scope, and further notification of appropriate personnel. Following those initial actions, the impact is evaluated, the evidence is collected and preserved, corrective measures are determined and executed, and learnings are recorded. This process is documented in the Security Incident Management Plan.

9. Individual operations and services

Guidelines	Applicability	Treasure Data Response
(1) Card transaction service		
P107	N/A	Treasure Data Customers retain control and ownership of their data and associated controls for managing cards.
P108	N/A	Treasure Data Customers retain control and ownership of their data and associated controls for managing cards.
P109	N/A	Treasure Data Customers retain control and ownership of their data and associated controls for managing financial transactions.
P110	N/A	Treasure Data Customers retain control and ownership of their data and associated controls for managing financial transactions.
P111	N/A	Treasure Data Customers retain the right and responsibility to manage controls and measures for financial cards.
(2) Internet and mobile services		
P112	N/A	Treasure Data Customers Responsibility for financial services using open networks rests with the customer and is out of scope for the CDP platform.
P113	N/A	Treasure Data Customers Responsibility for financial services using open networks rests with the customer and is out of scope for the CDP platform.
P114	N/A	Treasure Data Customers Responsibility for financial services using open networks rests with the customer and is out of scope for the CDP platform.
P115	N/A	Treasure Data Customers Responsibility for financial services using open networks rests with the customer and is out of scope for the CDP platform.
P116	N/A	Treasure Data Customers Responsibility for financial services using open networks rests with the customer and is out of scope for the CDP platform.
P117	N/A	Treasure Data Customers are responsible for the validation of identity.
(3) Management of handheld terminals		
P118	N/A	Treasure Data Customers are responsible for handheld terminals.

(4) Management of CD/ATM and unmanned branch		
P119	N/A	Treasure Data Customers are responsible for CD/ATM and unmanned branches and are out of scope for Treasure Data.
P120	N/A	Treasure Data Customers are responsible for CD/ATM and unmanned branches and are out of scope for Treasure Data.
P121	N/A	Treasure Data Customers are responsible for CD/ATM and unmanned branches and are out of scope for Treasure Data.
P122	N/A	Treasure Data Customers are responsible for CD/ATM and unmanned branches and are out of scope for Treasure Data.
P123	N/A	Treasure Data Customers are responsible for CD/ATM and unmanned branches and are out of scope for Treasure Data.
P124	N/A	Treasure Data Customers are responsible for the validation of remote control functions for CD/ATM and are out of scope for Treasure Data.
(5) In-store branches		
P125	N/A	Treasure Data Customers are responsible for in-store branches and are out of scope for Treasure Data.
(6) Convenience store ATMs		
P126	N/A	Treasure Data Customers are responsible for ATMs in convenience stores and are out of scope for Treasure Data.
P127	N/A	Treasure Data Customers are responsible for ATMs in convenience stores and are out of scope for Treasure Data.
P128	N/A	Treasure Data Customers are responsible for ATMs in convenience stores and are out of scope for Treasure Data.
P129	N/A	Treasure Data Customers are responsible for ATMs in convenience stores and are out of scope for Treasure Data.
P130	N/A	Treasure Data Customers are responsible for ATMs in convenience stores and are out of scope for Treasure Data.
P131	N/A	Treasure Data Customers are responsible for ATMs in convenience stores and are out of scope for Treasure Data.
(7) Debit card services		
P132	N/A	Treasure Data Customers are responsible for Debit Cards and are out of scope for Treasure Data.
P133	N/A	Treasure Data Customers are responsible for Debit Cards and are out of scope for Treasure Data.
P134	N/A	Treasure Data Customers are responsible for Debit Cards and are out of scope for Treasure Data.
P135	N/A	Treasure Data Customers are responsible for Debit Cards and are out of scope for Treasure Data.
(8) Prepaid payment method		
P136	N/A	Treasure Data Customers retain the ownership for their data and associated measures of transaction management.
P137	N/A	Treasure Data Customers are responsible for managing controls and measures for their financial cards.
(9) Use of e-mails and intranet		
P138	Yes	Treasure Data has an Acceptable Use Policy in Place. Treasure Data Customers retain the ability and the responsibility to manage their e-mail operations policy.
P139	Yes	Treasure Data has an Acceptable Use Policy in Place. Treasure Data Customers retain the ability and the responsibility to manage their e-mail operations policy.
(10) Biometric authentication		

P140	N/A	Treasure Data Customers are required to secure their user's biometrics data when used.
P141	N/A	Treasure Data Customers retain the right and responsibility to manage and restrict unauthorized use of their IDs.
(11) QR code payment		
P142	N/A	QR Card Code Payment is out of scope for Treasure Data.
P143	N/A	QR Card Code Payment is out of scope for Treasure Data.
P144	N/A	QR Card Code Payment is out of scope for Treasure Data.

Facility Guidelines

1. Computer centers

Guidelines	Applicability	Treasure Data Response
(1) Buildings (Environment)		
F1	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan.TREASURE DATA site-reliability engineers and DevOps engineers own the responsibility of scaling the platform and making sure that the platform deployment is serving our customers' hosted accounts on that deployment in the most optimal way. Our engineers take care of adding more VMs, adding more storage, managing backups. The RTO/RPO is dependent on the type and scale of the disaster and largely relies on Amazon's ability to recover.
(2) Buildings (Surroundings)		
F2	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan.TREASURE DATA site-reliability engineers and DevOps engineers own the responsibility of scaling the platform and making sure that the platform deployment is serving our customers' hosted accounts on that deployment in the most optimal way. Our engineers take care of adding more VMs, adding more storage, managing backups. The RTO/RPO is dependent on the type and scale of the disaster and largely relies on Amazon's ability to recover.

F3	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.6 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, fire alarm, Security Alarms, video surveillance, intrusion detection systems, and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F4	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, fire alarm, Security Alarms, video surveillance, intrusion detection systems, and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F5	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, fire alarm, Security Alarms, video surveillance, intrusion detection systems, and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F6	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.3 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, fire alarm, Security Alarms, video surveillance, intrusion detection systems, and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

	F7	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Environmental controls to provide assurances of the continuity of vital services such as heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power, and humidity control will be implemented in facilities in accordance with risk assessments. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	F8	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.1 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Treasure Data personnel are all charged with keeping Treasure Data's offices secure and protecting corporate information assets by safeguarding facilities, practices, computer assets, and carefully handling sensitive data/information. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	F9	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.3 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Treasure Data personnel are all charged with keeping Treasure Data's offices secure and protecting corporate information assets by safeguarding facilities, practices, computer assets, and carefully handling sensitive data/information. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	(3) Buildings (Structures)		

	F10	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Environmental controls to provide assurances of the continuity of vital services such as heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power, and humidity control will be implemented in facilities by risk assessments. All sites provide robust fire protection, detection, and prevention. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

	F11	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Environmental controls to provide assurances of the continuity of vital services such as heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power, and humidity control will be implemented in facilities by with risk assessments. All sites provide robust fire protection, detection, and prevention. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	F12	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Environmental controls to provide assurances of the continuity of vital services such as heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power, and humidity control will be implemented in facilities by risk assessments. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F13	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.1, 11.1.4 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Environmental controls to provide assurances of the continuity of vital services such as heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power, and humidity control will be implemented in facilities by risk assessments. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
(4) Buildings (Openings)		
F14	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. Environmental controls to provide assurances of the continuity of vital services such as heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power, and humidity control will be implemented in facilities by risk assessments. All sites provide robust fire protection, detection, and prevention. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F15	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F16	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.2 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F17	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F18	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F19	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.2 (Physical and environmental security) Description: Access badges and door keys are the exclusive property of Treasure Data. The Facilities Manager of a Treasure Data facility and its designees are the only people entitled to provision, duplicate, deactivate, reuse, or destroy access badges or door keys. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
(5) Buildings (Interior finish)		

	F20	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	F21	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.1, 11.1.3 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations)and from unauthorized physical access. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	(6) Computer room and data storage room (location)		
	F22	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.1, 11.1.3 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS Datacenters are housed in nondescript facilities. AWS data centers incorporate physical protection against environmental risks. Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations)and from unauthorized physical access. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F23	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS Datacenters are housed in nondescript facilities. AWS data centers incorporate physical protection against environmental risks Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F24	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS Datacenters are housed in nondescript facilities. AWS data centers incorporate physical protection against environmental risks. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F25	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.1 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS Datacenters are housed in nondescript facilities. AWS data centers incorporate physical protection against environmental risks. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F26	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.1 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS Datacenters are housed in nondescript facilities. AWS data centers incorporate physical protection against environmental risks. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

(7) Computer room and data storage room (opening)		
F27	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.2 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F28	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.3, 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Access badges and door keys are the exclusive property of Treasure Data. The Facilities Manager of a Treasure Data facility and its designees are the only people entitled to provision, duplicate, deactivate, reuse, or destroy access badges or door keys. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F29	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.3, 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F30	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
(8) Computer room and data storage room (Structure and interior finish)		
F31	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS data centers incorporate physical protection against environmental risks. Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F32	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013: Annex A: 11.1.4, 11.2.1 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS data centers incorporate physical protection against environmental risks. Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F33	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS data centers incorporate physical protection against environmental risks. Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F34	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4, 11.2.1 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS data centers incorporate physical protection against environmental risks. Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F35	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4, 11.2.1 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations)and from unauthorized physical access. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F36	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A:11.1.4, 11.2.1 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations)and from unauthorized physical access. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
(9) Computer room and data storage room (facilities)		
F37	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, Fire alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F38	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data maintains procedures for communications in the event of an emergency or office unavailability, e.g, due to natural disasters, adverse weather conditions, pandemic, or other widespread illness.

F39	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F40	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.3 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F41	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F42	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F43	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F44	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F45	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.1, 11.1.2 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, Fire alarms, video surveillance, intrusion detection systems, and other electronic means. Access badges and door keys are the exclusive property of Treasure Data. The Facilities Manager of a Treasure Data facility and its designees are the only people entitled to provision, duplicate, deactivate, reuse, or destroy access badges or door keys. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F46	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1 (Physical and environmental security) Description: Environmental controls to provide assurances of the continuity of vital services such as heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power, and humidity control will be implemented in facilities by risk assessments. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F47	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4, 11.2.1 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, security alarms, video surveillance, intrusion detection systems, and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

(10) Computer room and data storage room (Computer equipment, fixtures, and furnishings)		
F48	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS data centers incorporate physical protection against environmental risks. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F49	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1 (Physical and environmental security) Description: Environmental controls to provide assurances of the continuity of vital services such as heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power, and humidity control will be implemented in facilities by risk assessments. All sites provide robust fire protection, detection, and prevention. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F50	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4, 11.2.1 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F51	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, Fire alarms, video surveillance, intrusion detection systems, and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

(11) Power room and air conditioning room		
F52	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F53	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F54	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data is a cloud-hosted multi-tenant environment where several customers are hosted on specific Treasure Data deployment in any of the three AWS data center geographic locations in the U.S. East Coast, Germany, or Japan. AWS data centers incorporate physical protection against environmental risks. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F55	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, Fire alarms, video surveillance, intrusion detection systems, and other electronic means. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F56	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, Fire alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection and prevention. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F57	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, Fire alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection and prevention. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F58	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, Fire alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection and prevention. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F59	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F60	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.3 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
(12) Power supply facilities		
F61	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.1.3 (Operations security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F62	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

	F63	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	F64	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	F65	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	F66	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4, 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

	F67	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1, 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	F68	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1, 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	F69	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
	F70	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.1, 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F71	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
(13) Air-conditioning facilities		
F72	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4, 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F73	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F74	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4, 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F75	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F76	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F77	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F78	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4, 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F79	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.4, 11.2.2 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
(14) Monitor and control systems		
F80	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F81	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
(15) Line-related systems		

F82	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.3 (Physical and environmental security) Description: Treasure Data property and facilities will be protected appropriately by risk assessments from damage due to environmental factors (e.g. fire, flood, explosion, other natural or man-made disasters, power, and temperature or humidity variations) and from unauthorized physical access. Sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity, humidity, and cleanliness. Access badges and door keys are the exclusive property of Treasure Data. The Facilities Manager of an Treasure Data facility and its designees are the only people entitled to provision, duplicate, deactivate, reuse, or destroy access badges or door keys. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.
F83	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.1.3, 11.2.3 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, fire alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

F83-1	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 11.2.3 (Physical and environmental security) Description: Physical security controls include but are not limited to perimeter controls such as walls, fencing, security staff, badge access to enter and exit, fire alarms, video surveillance, intrusion detection systems, and other electronic means. All sites provide robust fire protection, detection, and prevention. Treasure Data Datacenter Physical security is maintained by Amazon Web Services.

2. Head offices and branch offices

Guidelines	Applicability	Treasure Data Response
(1) Buildings (Surroundings)		
F84	N/A	Out of Scope for Treasure Data
(2) Buildings (Structures)		
F85	N/A	Out of Scope for Treasure Data
F86	N/A	Out of Scope for Treasure Data
F87	N/A	Out of Scope for Treasure Data
F88	N/A	Out of Scope for Treasure Data
(3) Buildings (Openings)		
F89	N/A	Out of Scope for Treasure Data
F90	N/A	Out of Scope for Treasure Data
F91	N/A	Out of Scope for Treasure Data
F92	N/A	Out of Scope for Treasure Data
F93	N/A	Out of Scope for Treasure Data
(4) Buildings (Interior finish)		
F94	N/A	Out of Scope for Treasure Data
F95	N/A	Out of Scope for Treasure Data
F96	N/A	Out of Scope for Treasure Data
F97	N/A	Out of Scope for Treasure Data
F98	N/A	Out of Scope for Treasure Data
(5) Buildings (Facilities)		
F99	N/A	Out of Scope for Treasure Data

F100	N/A	Out of Scope for Treasure Data
F101	N/A	Out of Scope for Treasure Data
F102	N/A	Out of Scope for Treasure Data
F103	N/A	Out of Scope for Treasure Data
(6) Buildings (Line-related systems)		
F104	N/A	Out of Scope for Treasure Data
F105	N/A	Out of Scope for Treasure Data
F106	N/A	Out of Scope for Treasure Data
(7) Buildings (Power supply facilities)		
F107	N/A	Out of Scope for Treasure Data
F108	N/A	Out of Scope for Treasure Data
F109	N/A	Out of Scope for Treasure Data
(8) Buildings (Air-conditioning facilities)		
F110	N/A	Out of Scope for Treasure Data
(9) Buildings (ATM room)		
F111	N/A	Out of Scope for Treasure Data
F112	N/A	Out of Scope for Treasure Data
F113	N/A	Out of Scope for Treasure Data
F114	N/A	Out of Scope for Treasure Data
F115	N/A	Out of Scope for Treasure Data
F116	N/A	Out of Scope for Treasure Data
F117	N/A	Out of Scope for Treasure Data
(10) Buildings (Terminal devices)		
F118	N/A	Out of Scope for Treasure Data
F119	N/A	Out of Scope for Treasure Data
F120	N/A	Out of Scope for Treasure Data

(11) Server installation site (location)		
F121	N/A	Out of Scope for Treasure Data
F122	N/A	Out of Scope for Treasure Data
F123	N/A	Out of Scope for Treasure Data
F124	N/A	Out of Scope for Treasure Data

(12) Server installation site (structure/interior, etc.)		
F125	N/A	Out of Scope for Treasure Data
F126	N/A	Out of Scope for Treasure Data
F127	N/A	Out of Scope for Treasure Data
(13) Server installation site (facilities)		
F128	N/A	Out of Scope for Treasure Data
F129	N/A	Out of Scope for Treasure Data
F130	N/A	Out of Scope for Treasure Data
F131	N/A	Out of Scope for Treasure Data
F132	N/A	Out of Scope for Treasure Data
F133	N/A	Out of Scope for Treasure Data
F134	N/A	Out of Scope for Treasure Data
(14) In-store branches		
F135	N/A	Out of Scope for Treasure Data
F136	N/A	Out of Scope for Treasure Data
(15) Convenience store ATMs		
F137	N/A	Out of Scope for Treasure Data

Audit Guidelines

1. System auditing

Guidelines	Applicability	Treasure Data Response
(1) System auditing		
A1	Yes	Treasure Data is certified to the ISO 27001:2013 Standard and verified by third-party accredited external auditors for SOC 2 Type 2. Controls that support the Guideline: ISO 27001:2013, Annex A: 12.7.1 (Operations security), 15.2.1 (Supplier relationships) Description: Treasure Data has Information systems audit controls in place.