ThoughtSpot Subscription Service Program Guide

At ThoughtSpot, we are driven to provide the best available customer support and secure infrastructure. We take a comprehensive approach to helping our customers use the ThoughtSpot Cloud wherever they are located and ensuring that nothing stands in the way of achieving their desired tangible business value. With 24x7 worldwide support and ongoing updates to all our valued customers, our support is delivered by experts obsessed with your success and focused on what is important to your business.

This ThoughtSpot Subscription Service Program Guide ("**Guide**") applies to ThoughtSpot's provision of technical assistance for the ThoughtSpot Cloud ("**Support**") and the written information security program of policies, procedures, and controls governing the processing, storage, transmission, and security of Customer Data ("**Security Program**") for the ThoughtSpot Cloud software-as-a-service offering ("**ThoughtSpot Cloud**") purchased by Customer directly from ThoughtSpot or from any ThoughtSpot authorized reseller.

ThoughtSpot Cloud is made available by ThoughtSpot under the terms of this Guide as incorporated into the ThoughtSpot Cloud Subscription Agreement or other agreement that grants the right to access and use the ThoughtSpot Cloud and its incorporated or referenced order forms, purchase orders, addenda, and other documents (collectively, the "**Agreement**," without regard to the name of the underlying agreement, nor how it refers to its parties or identifies ThoughtSpot's products). This Guide constitutes the complete and exclusive agreement between Customer and ThoughtSpot relating to its subject matter and supersedes all prior oral and written agreements, understandings, representations, warranties, and communications regarding its subject matter. In the event of any conflict between the terms and conditions of this Guide and the Agreement, the Agreement will govern to the extent of such conflict. As used herein, ThoughtSpot, Inc. or its affiliate that entered into the Agreement with Customer is "**ThoughtSpot**"; the other entity that is a party to the Agreement is the "**Customer**," and each is referred to herein as a "**party**" and collectively as the "**parties**." ThoughtSpot's online portal for support information and requests available at https://www.thoughtspot.com/support and its related and successor websites are collectively the "**Support Portal**." This Guide may be updated from time to time upon posting the new version to the Support Portal.

Support

Overview

This Guide describes the responsibilities of the parties regarding ThoughtSpot's provision of Support. Please refer to instructions and documentation posted on the Support Portal for detailed information on Support procedures, including contact information, submission of tickets, roles, components used, alerting, request monitoring and escalations, file server access, and other procedural matters.

Customer will automatically receive all updates and upgrades applicable to purchased ThoughtSpot Cloud product(s) that are made generally available to all customers.

This Guide utilizes the following defined terms:

1. "**Documentation**" means the then-current ThoughtSpot Cloud service operating and interface instructions (including API documentation) published by ThoughtSpot for each version at https://docs.thoughtspot.com/.
2. "**Error**" means a reproducible failure of the Cloud to perform any material function set forth in the Documentation.
3. "**Technical Contact**" means a qualified individual designated by Customer for the purpose of receiving Support.

Scope of Support

During the subscription term referenced in the Agreement ThoughtSpot will: **(a)** provide Support 24 hours a day, 7 days a week, including all holidays; **(b)** answer Support requests registered in the Support Portal by a system administrator and supported by a Technical Contact regarding the operation of the ThoughtSpot Cloud; **(c)** use commercially reasonable efforts to correct any Errors reported by Customer and confirmed by ThoughtSpot in accordance with the priority level assigned to the Error in the ThoughtSpot ticketing system, including through the application of updates to ThoughtSpot Cloud; **(d)** use commercially reasonable efforts to respond to each reported Error according to the Support Process section below. Support responses may take the form of software or infrastructure updates, procedural solutions, correction of Documentation errors, or other remedial measures as ThoughtSpot may determine, in its sole discretion, to be appropriate. Support is provided to Customer only and not to third-party authorized users unless otherwise expressly agreed in an order form. ThoughtSpot will have no obligation to provide Support for preview, beta or evaluation features, or third-party software, APIs, integrations, or services, or custom integrations, scripts, or code not native to the ThoughtSpot Cloud. Support does not include implementation, configuration, customization, integration, or training services.

Support Process

For each Error, Customer may assign in the Support Portal a priority level based on the relative impact an Error has on the use of the ThoughtSpot Cloud. ThoughtSpot may re-assign the priority level in its sole discretion. Priority levels and target initial response times for each priority level are described below.

Priority	Description	Initial Response Time Target
P0	Production instance is unavailable; all users are blocked and productivity halted.	Within 1 hour
P1	Production instance is available; functionality or performance is severely impaired.	Within 2 hours
P2	Production instance is available and usable with partial, non-critical loss of functionality, or the production instance has an occasional issue that Customer would like identified and resolved. Requests for help on administrative tasks.	Within 4 hours
P3	Cosmetic issues or request for general information about the ThoughtSpot Cloud, Documentation, process or procedures.	By next business day

Service Level Agreement

For any calendar month in which a production instance of the ThoughtSpot Cloud falls below 99%, excluding Service Level Exclusions (defined below) (the "**Service Level**"), as Customer's sole and exclusive remedy for such downtime Customer may request to apply to the next invoice for subscription fees a number of credits equal to the monetary value of the number of minutes the ThoughtSpot Cloud was not Available in the month below the Service Level, determined at the per-minute rate that ThoughtSpot charged Customer for Customer's use of the affected ThoughtSpot Cloud instance ("**Service Level Credits**"). Each Service Level Credit will extend the subscription term of Customer's affected then-current production subscription and any non-production instances purchased in the same Order Form by the number of minutes the Cloud was not available in the month. Customer must request all Service Level Credits in writing to ThoughtSpot at servicelevelcredits@thoughtspot.com within 20 days of the end of the month in which the Service Level was not met and identify the support requests relating to the period Customer's instances of the ThoughtSpot Cloud were unavailable. Availability is calculated as the minutes the ThoughtSpot Cloud is accessible to authorized users/total minutes in the month, where the calendar and clock utilized will be that used by the ThoughtSpot Cloud in its hosted location.

"**Service Level Exclusion**" means: **(a)** scheduled maintenance provided with at least 48 hours' prior written notice to the administrator user(s), posted on the Support Portal, or displayed in a conspicuous on-screen message to the administrator user(s) in the ThoughtSpot Cloud; **(b)** unavailability caused by Customer interference due to testing or audit, or Customer's integration or scripting except as described in the Documentation; **(c)** unavailability caused by general internet problems or circumstances beyond ThoughtSpot's reasonable control, arising from Customer Data or Customer's or a user's equipment, Customer's authentication software, third-party acts, or unavailability to services or systems not provided by ThoughtSpot to Customer; **(d)** suspension as provided in the Agreement; or **(e)** unavailability of evaluation, proof of concept, proof of technology, beta, or other non-production use of ThoughtSpot Cloud.

Customer Acknowledgments

ThoughtSpot's Support obligations are conditioned upon the following:

1. Customer must designate a limited number of Technical Contacts to make Support requests. Customer will use reasonable efforts to ensure that the individuals designated as Technical Contact are qualified to support the Customer teams internally. Technical Contacts must provide reasonable assistance to resolve Support issues, and to provide updates to ThoughtSpot using the Support Portal.
2. ThoughtSpot may collect and use usage metrics, query logs, and other data derived from operation of the ThoughtSpot Cloud ("**Usage Data**") to operate, support, improve, and develop its products and services and for industry benchmarking and analysis. ThoughtSpot will not share any Usage Data that includes Customer's Confidential Information or Customer Data with any third party except: **(a)** in accordance with the Agreement; or **(b)** to the extent the Usage Data is aggregated and anonymized such that Customer and Customer's users cannot be identified.
3. If Customer purchased access to ThoughtSpot Cloud from a ThoughtSpot authorized reseller: **(a)** Customer agrees that this Guide will apply notwithstanding anything to the contrary in an agreement with the partner; and **(b)** if ThoughtSpot does not receive payments for the ThoughtSpot Cloud purchased directly, or indirectly through a partner, ThoughtSpot will have the right to suspend Support until payment is received without liability for such suspension. ThoughtSpot will not be liable for any contractual obligation made by the reseller or any other third party beyond those set forth in this Guide.

Data Security

This Guide describes the responsibilities of the parties regarding ThoughtSpot's provision of the Security Program.

1. Security Program.

1.1. **Security Standards**. While providing ThoughtSpot Cloud, ThoughtSpot will maintain an information Security Program aligned to ISO27001 or a substantially equivalent standard. The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. ThoughtSpot updates the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

1.2. **Security Organization**. ThoughtSpot shall designate a Director of Information Security responsible for managing the Security Program.

1.3. **Policies**. ThoughtSpot's information security policies shall be: **(a)** documented; **(b)** reviewed and approved by management, including after material changes to the ThoughtSpot Cloud; and **(c)** published, and communicated to personnel, contractors, and third parties with access to Customer Data, including appropriate ramifications for noncompliance.

1.4. **Risk Management**. ThoughtSpot shall perform information security risk assessments as part of a risk governance program that is established with the objective to regularly test, assess and evaluate the effectiveness of the Security Program. Such assessment shall be designed to recognize and assess the impact of risks and implement identified risk reduction or mitigation strategies to address new and evolving security technologies, changes to industry standard practices, and changing security threats. ThoughtSpot shall have the risk program audited annually by an independent third party in accordance with Section 2.1 (*Attestations*).

2. Attestations and Audits.

2.1. **Attestations**. ThoughtSpot shall establish and maintain sufficient controls to meet attestation for the objectives stated in SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) for the Security Program supporting the ThoughtSpot Cloud. At least once per calendar year, ThoughtSpot shall obtain an assessment against such standards and audit methodologies by an independent third-party auditor and make the executive reports available to the Customer.

2.2. **Audit**. ThoughtSpot will allow for and contribute to audits that include inspections by granting Customer (either directly or through its representative(s)); provided that such representative(s) shall enter into written obligations of confidentiality and non-disclosure directly with ThoughtSpot), access to all reasonable and industry-recognized documentation evidencing ThoughtSpot's policies and procedures governing the security and privacy of Customer Data and its Security Program ("**Audit**") at no additional cost. Audits will be limited to no more than once per year, and may be of the Customer's own tenant web application or a representative non-production web application. The information available will include documentation evidencing ThoughtSpot's Security Program, as well as copies of attestation reports (including audits) listed above.

2.3. **Output**. Upon completion of the Audit, ThoughtSpot and Customer may schedule a mutually convenient time to discuss the output of the Audit. ThoughtSpot may in its sole discretion, consistent with industry and ThoughtSpot's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve ThoughtSpot's Security Program. The Audit and the results derived therefrom are deemed to be the Confidential Information of Customer and ThoughtSpot.

3. Physical and Environmental Security Measures.

3.1. ThoughtSpot uses infrastructure-as-a-service cloud providers as further described in the Agreement or Documentation (each, a "**Cloud Provider**"). Each Cloud Provider shall have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks. Such controls, will include, but are not limited to, the following: **(a)** Physical access to the facilities are controlled at building ingress points; **(b)** visitors are required to present ID and are signed in; **(c)** physical access to servers is managed by access control devices; **(d)** physical access privileges are reviewed regularly; **(e)** facilities utilize monitor and alarm response procedures; **(f)** use of CCTV; **(g)** fire detection and protection systems; **(h)** power back-up and redundancy systems; and **(i)** climate control systems.

4. Technical Security Measures.

4.1. **Access Administration**. Access to the ThoughtSpot Cloud is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and non-production instances. Employees are assigned a unique user account. Individual user accounts will not be shared. Access privileges are based on job requirements using the principle of least privilege access and are revoked upon termination of employment. Access entitlements are reviewed by management semi-annually. Infrastructure access includes appropriate user account and authorization controls, which will include the required use of VPN connections, complex passwords, account lock-out enabled, and a two-factor authenticated connection.

4.2. **Service Access Controls**. The ThoughtSpot Cloud includes user and role-based access controls. Customer is responsible for configuring such access controls within its instance.

4.3. **Session Management and Cookies**. When providing the ThoughtSpot Cloud, ThoughtSpot uses session tokens and cookies to: **(a)** validate user sessions and authorize requests; and **(b)** monitor the ThoughtSpot Cloud application software and usage software.

Customer shall be responsible for providing notice to, and collecting any necessary consents from, its users of the ThoughtSpot Cloud for cookies used by the ThoughtSpot Cloud.

4.4. **Logging and Monitoring**. The production infrastructure log activities are centrally collected, are secured in an effort to prevent tampering, and are monitored for anomalies. ThoughtSpot shall provide a logging capability in the platform that captures login and actions taken by users in the ThoughtSpot Cloud. Customer has access to user activity audit logs within its instance(s).

4.5. **Firewall System**. A network firewall is installed and managed to protect ThoughtSpot systems by residing on the network to inspect all ingress connections routed to the ThoughtSpot environment. ThoughtSpot-managed firewall rules are reviewed on a periodic basis, at least annually, by the ThoughtSpot security team.

4.6. **Vulnerability Management**. ThoughtSpot conducts quarterly security risk evaluations to assess threats to information assets, determine potential vulnerabilities, and provide for remediation. Software patches are regularly deployed to Customer instances to address known vulnerabilities. When software vulnerabilities are revealed and addressed by a vendor patch, ThoughtSpot will obtain the patch from the applicable vendor and apply it within an appropriate time frame in accordance with ThoughtSpot's then-current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems.

4.7. **Antivirus**. ThoughtSpot runs antivirus and anti-malware software on employee endpoints, and updates such software at regular intervals.

4.8. **Change Control**. ThoughtSpot evaluates changes to platform, applications, and production infrastructure to minimize risk and such changes are implemented following ThoughtSpot's standard operating procedure.

4.9. **Configuration Management**. ThoughtSpot shall implement and maintain standard hardened configurations for all system components within the ThoughtSpot Cloud. ThoughtSpot shall use industry-standard hardening guides, such as guides from the Center for Internet Security, when developing standard hardening configurations.

4.10. **Data Encryption**. ThoughtSpot shall use industry-standard encryption to encrypt Customer Data in transit over public networks to the ThoughtSpot Cloud. In addition, ThoughtSpot will provide disk-level and storage-level encryption at rest capabilities.

4.11. **Secure Software Development**. ThoughtSpot shall implement and maintain secure application development policies and procedures aligned with industry-standard practices such as the OWASP Top Ten (or a substantially equivalent standard). All personnel responsible for secure application design and development will receive appropriate training regarding ThoughtSpot's secure application development practices. ThoughtSpot shall perform a combination of static and dynamic testing and analysis of code prior to the release of such code to Customers.

4.12. **Malicious Code**. The ThoughtSpot Cloud application code will not contain viruses, Trojan horses, malware, worms, or similar harmful, malicious, or hidden procedures, routines, or mechanisms that may result in: **(a)** any inoperability of the ThoughtSpot Cloud; or **(b)** any interruption or interference with the operation of the ThoughtSpot Cloud (collectively, "**Malicious Code**"). If the ThoughtSpot Cloud application code is found to contain any Malicious Code that adversely affects the performance of the ThoughtSpot Cloud or causes a material security risk to Customer Data, ThoughtSpot shall, as Customer's exclusive remedy, use commercially reasonable efforts to remove the Malicious Code. Customer shall be responsible for any security vulnerabilities, and the consequences of such vulnerabilities, arising out of the Customer Data, including any viruses, Trojan horses, malware, worms or other similar harmful, malicious, or hidden procedures, routines, or mechanisms in Customer Data or Customer's scripts or integrations that adversely affects the performance of the ThoughtSpot Cloud or causes a material security risk to Customer Data.

5. Organizational Security Measures.

5.1. **ThoughtSpot Access Limitations**. ThoughtSpot employees will not, without Customer's prior consent or unless as part of a functionality of the ThoughtSpot Cloud initiated by or for Customer (*e.g.*, data integrations or data transferability between instances): access Customer Data, move Customer Data outside Customer's tenant (except as performed by Customer or for Customer by a third party), nor screen-capture, copy, record in video or other formats, Customer Data.

5.2. **Cloud Provider Review**. ThoughtSpot performs routine reviews of Cloud Providers to confirm that the Cloud Providers continue to maintain appropriate security controls necessary to comply with the Security Program.

5.3. **Personnel Security**. ThoughtSpot performs background screening on all employees and, as applicable, all contractors who have access to Customer Data in accordance with ThoughtSpot's then-current applicable standard operating procedure and subject to applicable laws.

5.4. **Security Awareness Training**. ThoughtSpot maintains a security and privacy awareness program that includes appropriate training and education of ThoughtSpot personnel, including, as applicable, any contractors that may access Customer Data. Such training is conducted at time of hire and at least annually throughout employment at ThoughtSpot.

5.5. **Vendor Risk Management**. ThoughtSpot maintains a vendor risk management program that assesses vendors that access, store, process, or transmit Customer Data for appropriate security and privacy controls and business disciplines.

5.6. **Software and Asset Inventory**. ThoughtSpot shall maintain an inventory of all software components (including, but not limited to, open source software) used in the ThoughtSpot Cloud.

6. Service Continuity.

6.1. **Data Management; Data Backup**. ThoughtSpot will host the purchased instances of the ThoughtSpot Cloud in Cloud Providers that attained SSAE 18 / SOC 1 and SOC 2 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations or certifications) acting in an active/active capacity for the Subscription Term. ThoughtSpot backs up all Customer's tenant metadata and ThoughtSpot's service state in accordance with ThoughtSpot's standard operating procedure, for which a description of applicable portions is available to Customer upon request.

6.2. **Disaster Recovery**. ThoughtSpot shall: **(a)** maintain a disaster recovery ("**DR**") plan that is consistent with industry standards for the ThoughtSpot Cloud; **(b)** test the DR plan at least once every year; **(c)** make available summary test results which will include the actual recovery point and recovery times; and **(d)** document any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the ThoughtSpot Cloud from being recovered in accordance with the DR plan.

6.3. **Business Continuity**. ThoughtSpot shall maintain a business continuity plan ("**BCP**") to minimize the impact to its provision and support of the ThoughtSpot Cloud from an event. The BCP shall: **(a)** include processes for protecting personnel and assets and restoring functionality in accordance with the time frames outlined therein; and **(b)** be tested annually and updated based on any deficiencies, identified during such tests.

6.4. **Personnel**. In the event of an emergency that renders the Support telephone system unavailable, all calls are routed to an answering service that will transfer to a ThoughtSpot telephone support representative, geographically distributed to ensure business continuity for support operations.

7. Monitoring and Incident Management.

7.1. **Incident Monitoring and Management**. ThoughtSpot will monitor, analyze, and respond to security incidents in a timely manner in accordance with ThoughtSpot's standard operating procedure. ThoughtSpot's security group will escalate and engage response teams as may be necessary to address a security incident.

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

7.3. **Report**. The initial report will be made to Customer security contact(s) designated by Customer to ThoughtSpot (or if no such contact(s) are designated, then to the primary Technical Contact designated by Customer). As information is collected or otherwise becomes available, ThoughtSpot shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected individuals, government agencies, and data protection authorities in accordance with all applicable data protection and privacy laws regulating the Processing of Personal Data, including where applicable, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (the General Data Protection Regulation, or GDPR), and repealing Directive 95/46/EC. As used herein, "**Personal Data**" means any information relating to an identified or identifiable natural person uploaded to the ThoughtSpot Cloud as Customer Data by or for Customer or Customer's agents, employees, or contractors; and "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The report will include the name and contact information of the ThoughtSpot contact from whom additional information may be obtained. ThoughtSpot shall inform Customer of the measures that ThoughtSpot will adopt to mitigate the cause of the Breach and to prevent future Breaches.

7.4. **Customer Obligations**. Customer will cooperate with ThoughtSpot by providing any information that is reasonably requested by ThoughtSpot to resolve any security incident, including any Breaches, identify its root cause(s), and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted data subjects (identified or identifiable natural persons) and for providing such notice.

8. Penetration Tests.

8.1. **By a Third Party**. ThoughtSpot contracts with third-party vendors to perform a penetration test on the ThoughtSpot application code at least four times per year to identify risks and remediation options that help increase security. ThoughtSpot shall make executive summary reports from the penetration testing available to Customer on demand.

8.2. **By Customer**. Customer shall not perform a penetration test on the ThoughtSpot Cloud without ThoughtSpot's express written authorization.

9. Sharing the Security Responsibility.

9.1. **Product Capabilities**. The ThoughtSpot Cloud allows Customer to: **(a)** authenticate users before accessing the Customer's instance; **(b)** integrate with SAML solutions; **(c)** allow users to manage passwords; **(d)** prevent access by users with an inactive account; and **(e)** select fields for exclusion from indexing. Customer is solely responsible for managing each user's access to, and use of, the ThoughtSpot Cloud by assigning to each user a credential and role that controls the level of access to the ThoughtSpot Cloud. Customer is solely responsible for: **(i)** its decision to index Customer Data containing sensitive data, including any information relating to a natural person governed by data protection laws, and ThoughtSpot will have no liability to the extent that damages would have been mitigated by Customer’s decision not to index such Customer Data; **(ii)** protecting the confidentiality of each user’s login and password and managing roles, rights, maintaining user logins for each individual person, and granting each user’s access to the ThoughtSpot Cloud; and **(iii)** reviewing ThoughtSpot’s Security Program and making an independent determination as to whether it meets Customer’s requirements, taking into account the type and sensitivity of Customer Data that Customer processes within the ThoughtSpot Cloud.

9.2. **Security Contact**. In accordance with this Guide, Customer agrees to identify and maintain appropriate security contact(s) for all information security incidents, and information security-related communication within the Support Portal.

9.3. **Limitations**. Notwithstanding anything to the contrary in this Guide or other parts of the Agreement, ThoughtSpot’s obligations herein are only applicable to the ThoughtSpot Cloud. This Guide does not apply to: **(a)** information shared with ThoughtSpot that is not Customer Data; **(b)** data in Customer’s VPN or a third-party network; and **(c)** any data processed by Customer or its users in violation of the Agreement or this Guide.