ThoughtSpot Cloud Program Guide

At ThoughtSpot, we are driven to provide optimal customer support and secure infrastructure. We take a comprehensive approach to helping our customers achieve their desired tangible business value with ThoughtSpot Cloud. With worldwide support, ongoing updates to all our valued customers, and world-class security, our support and security program is delivered by experts obsessed with your success and focused on what is important to your business.

This ThoughtSpot Cloud Program Guide ("**Program Guide**") applies to ThoughtSpot software-as-a-service offerings ("**ThoughtSpot Cloud**") provided to Customer by ThoughtSpot, including ThoughtSpot's provision of technical assistance for the ThoughtSpot Cloud ("**Support**") and the written information security program of policies, procedures, and controls, governing information processing, storage, transmission, and security applicable to ThoughtSpot Cloud ("**Security Program**").

ThoughtSpot Cloud is made available by ThoughtSpot under the terms of this Program Guide as incorporated into the ThoughtSpot Cloud Subscription Agreement or other agreement that grants the right to access and use 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, or how it refers to its parties or identifies ThoughtSpot's products). This Program Guide and the Agreement into which it is incorporated 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 Program 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 Program Guide may be updated from time to time, solely with prospective effect, upon posting the new version to the Support Portal. Updates to this Program Guide will retain the material commitments, protections or overall level of service provided to Customer described herein. References in any agreement incorporating the "ThoughtSpot Subscription Service Guide" will mean this Program Guide.

This Program Guide does not apply to Team Editions, Essentials Editions, browser add-ons such as SeekWell, or any evaluation, trial, or other unpaid access to ThoughtSpot Cloud, including ThoughtSpot's "Free Trial" online offering.

This Program 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 at https://docs.thoughtspot.com/ for each version of ThoughtSpot Cloud.
2. "**Error**" means a reproducible failure of ThoughtSpot 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.

Support Program

Overview

This Program Guide describes the responsibilities of the parties regarding ThoughtSpot's provision of Support. Please refer to instructions and documentation posted on the Support Portal, as applicable, 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.

Scope of Support

During the subscription term referenced in the Agreement ThoughtSpot will provide support during the following time periods for the applicable ThoughtSpot Product:

ThoughtSpot Pro, ThoughtSpot Analytics Enterprise, and ThoughtSpot Embedded Enterprise
24 hours a day, 7 days a week, including Holidays

Note that as of January 2024, "ThoughtSpot Everywhere" is now *ThoughtSpot Embedded*.

During the Subscription Term, ThoughtSpot will: **(a)** answer Support requests registered in the Support Portal by a system administrator and supported by a Technical Contact regarding operation of ThoughtSpot; **(b)** use commercially reasonable efforts to correct any

Errors, including through the application of updates to ThoughtSpot Cloud, reported by Customer and confirmed by ThoughtSpot in accordance with the priority level assigned to the Error; and **(c)** use commercially reasonable efforts to respond to each reported Error according to the section below entitled "Support Process." Support responses may take the form of software or infrastructure updates, procedural solutions, correction of Documentation, or other remedial measures as ThoughtSpot may, in its sole discretion, determine to be appropriate. Support is provided to Customer only and not to third-party authorized users unless otherwise expressly agreed in an order form. To the extent that Customer grants access to ThoughtSpot Cloud to third parties or integrates or embeds ThoughtSpot Cloud with any product, website, software, or solution, Customer will use commercially reasonable efforts to identify, isolate, and remediate any suspected Error prior to initiating a Support request with ThoughtSpot. ThoughtSpot will have no obligation to provide Support for preview, beta or evaluation features, or third-party materials such as software, APIs, integrations, or services, or custom integrations, scripts, or code, not native to 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 ThoughtSpot Cloud. ThoughtSpot may re-assign the priority level at its sole discretion. Priority levels and target initial response times for each priority level and ThoughtSpot Product are described below.

Priority	Description	Initial Response Time Target ThoughtSpot Pro ThoughtSpot AgentSpot	Initial Response Time Target ThoughtSpot Analytics Enterprise ThoughtSpot Embedded Enterprise
P0	Production instance is unavailable; all users are blocked and productivity halted.	Within 12 hours	Within 1 hour
P1	Production instance is available; functionality or performance is severely impaired.	Within 24 hours	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. Includes requests for help on administrative tasks.	Within 48 hours	Within 4 hours
P3	Cosmetic issues or request for general information about ThoughtSpot Cloud, Documentation, processes, or procedures.	Reasonable efforts	By next business day

Service Level Agreement

The service level for ThoughtSpot Cloud will be 99.5%, or 99.9% if Customer has purchased the High Availability Add-On, in either case excluding Service Level Exclusions (defined below) ("**Service Level**"). For any calendar month in which the availability of a production instance of ThoughtSpot Cloud falls below the Service Level, as Customer's sole and exclusive remedy for such downtime, Customer may request to apply a number of credits equal to prorated amounts paid for the number of minutes 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 that ThoughtSpot 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 that Customer's affected instance(s) of ThoughtSpot Cloud was or were not available. Availability is calculated monthly as the minutes a production instance of ThoughtSpot Cloud is accessible to authorized users in a month divided by the total minutes in that month, where the calendar and clock utilized will be that used by ThoughtSpot Cloud in its hosted location.

"**Service Level Exclusions**" 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 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, or arising from any of the following: data or software received in, or submitted to, Customer's instance of

ThoughtSpot Cloud, 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 for in the Agreement; or **(e)** unavailability of evaluation, proof of concept, proof of technology, beta, or other non-production use or instances 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 Contacts are qualified to support Customer's internal teams. Technical Contacts must provide reasonable assistance to resolve Support issues, and provide updates to ThoughtSpot using the Support Portal, as applicable.
2. ThoughtSpot may collect and use usage metrics, query logs, system logs, and other data derived from operation of ThoughtSpot Cloud ("**Usage Data**"), to operate, support, improve, and develop its products and services and for industry benchmarking and analysis. ThoughtSpot will not share Usage 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 Program Guide will apply notwithstanding anything to the contrary in an agreement with the reseller; and **(b)** if ThoughtSpot does not receive payments for ThoughtSpot Cloud purchased directly, or indirectly through a reseller, 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 Program Guide.

Security Program

This Program Guide describes ThoughtSpot's policies, procedures, and controls forming the Security Program.

1. Security Program.

1.1. **Security Standards**. While providing ThoughtSpot Cloud, ThoughtSpot will maintain a Security Program aligned to ISO 27001 or a substantially equivalent standard. The Security Program includes industry-standard practices designed to protect 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.

1.2. **Security Organization**. ThoughtSpot will designate a Head of Information Security responsible for managing the Security Program.

1.3. **Policies**. ThoughtSpot's information security policies will be: **(a)** documented; **(b)** reviewed and approved by management, including after material changes to ThoughtSpot Cloud; and **(c)** published and communicated to personnel, contractors, and third parties with access to Customer's instances of ThoughtSpot Cloud, and will include appropriate remedies for non-compliance.

1.4. **Risk Assessments**. ThoughtSpot will perform information security risk assessments as part of a risk governance program (described in Section 6.2) that is established with the objective to regularly test, assess, and evaluate, the effectiveness of the Security Program. Such assessment will 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.

1.5. **Attestations**. ThoughtSpot will develop, implement, and maintain information security and data privacy controls to meet the applicable objectives stated in the ISO/IEC 27001 and the American Institute of Certified Public Accountants (AICPA) Service Organizational Control ("**SOC 2 Type II**") frameworks for the Security Program supporting ThoughtSpot Cloud. At least once per calendar year, ThoughtSpot will obtain an assessment against such standards and audit methodologies by an independent third-party auditor and make the executive reports available to the Customer upon request.

2. Audits.

2.1. **Audit**. ThoughtSpot will allow for and contribute to audits that include inspections by granting Customer (either directly or through its representative(s)) access to all reasonable and industry-recognized documentation evidencing ThoughtSpot's applicable policies and procedures governing data security and privacy under its Security Program ("**Audit**") at no additional cost. Any representative participating in an Audit must enter into written obligations of confidentiality. Audits will be limited to no more than once per year and may be of Customer's 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.

2.2. **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 (excluding all Confidential Information disclosed by ThoughtSpot) and the results derived therefrom are deemed to be the Confidential Information of both Customer and ThoughtSpot.

3. Physical and Environmental Security Measures.

3.1. **Infrastructure**. ThoughtSpot uses infrastructure-as-a-service cloud providers to support the application that processes Customer's instance of ThoughtSpot Cloud as further described in the Agreement or Documentation (each, a "**Cloud Provider**"). ThoughtSpot will require each Cloud Provider to have a SSAE 18 / II Type II attestation, ISO 27001 certification, or an industry-recognized equivalent security attestation or certification commensurate with the providers' risks, and will implement appropriate physical and environmental security measures, including: **(a)** physical access to the facilities controlled at building ingress points; **(b)** visitors required to present ID and be signed in; **(c)** physical access to servers managed by access control devices; **(d)** physical access privileges reviewed regularly; **(e)** utilization of monitoring and alarm response procedures at facilities; **(f)** use of CCTV; **(g)** fire detection and protection systems; **(h)** power back-up and redundancy systems; and **(i)** climate control systems.

3.2. **Cloud Provider Due Diligence**. During the Subscription Term, ThoughtSpot will host purchased instances of ThoughtSpot Cloud in Cloud Providers that have attained SSAE 18 / SOC 2 Type II attestation or ISO 27001 certification (or equivalent or successor attestations or certifications) as reported to ThoughtSpot.

3.3. **Location**. The hosting location of the ThoughtSpot Cloud instance is selected by Customer in the corresponding order form or as Customer otherwise configures location via ThoughtSpot Cloud or Support. Alternatively, if ThoughtSpot Cloud was purchased online such that no order form applies, then the location will be identified in the web form(s) applicable to the purchase.

4. Technical Security Measures.

4.1. **Access Administration**. Access to 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 and user ID. Individual user accounts will not be shared. Access privileges are based on job requirements using the principle of least privilege 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 secure remote access connections, complex passwords, account lock-out enabled, and a two-factor authenticated connection.

4.2. **Service Access Controls**. ThoughtSpot Cloud includes user-based and role-based access controls. Customer is responsible for configuring such access controls within its instance. ThoughtSpot supports integrations with single sign-on providers as described in the Documentation.

4.3. **Session Management and Cookies**. When providing ThoughtSpot Cloud, ThoughtSpot uses session tokens and cookies to: **(a)** validate user sessions and authorize requests; and **(b)** monitor ThoughtSpot Cloud application software and usage software. Customer will provide necessary notices to, and collect any necessary consents from, its users of ThoughtSpot Cloud for cookies used by 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 may provide a logging capability in the platform that captures login and actions taken by users in ThoughtSpot Cloud. Where logging capabilities are available in the purchased product, Customer has access to user activity audit logs within its instance(s).

4.5. **Data Encryption**. ThoughtSpot will use industry-standard encryption to encrypt data in transit over public networks to ThoughtSpot Cloud. In addition, ThoughtSpot will provide disk-level and storage-level encryption at rest capabilities. ThoughtSpot encrypts data at-rest using AES 256-bit or better encryption. ThoughtSpot uses Transport Layer Security (TLS) 1.2 or better for data in-transit over untrusted networks.

4.6. **Firewall System**. A 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.

4.7. **Vulnerability Management**. ThoughtSpot conducts security vulnerability evaluations on a schedule determined by the potential level of risk of the information asset to assess threats, determine potential vulnerabilities, and provide for remediation. Customer instances are regularly updated 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 appears to be safe for installation in all production systems.

4.8. **Intrusion Detection System**. ThoughtSpot uses an intrusion detection system to monitor the ThoughtSpot Cloud network and systems for malicious activity and policy violations. Intrusion detection activity is collected using a security information and event management system.

4.9. **Antivirus**. ThoughtSpot runs antivirus and anti-malware software on ThoughtSpot owned and managed endpoints (including employee laptops, desktops, and servers), and updates such software at regular intervals. In addition, ThoughtSpot runs antivirus and anti-malware software on production instances of ThoughtSpot Cloud.

4.10. **Malicious Code**. The ThoughtSpot Cloud application will be analyzed in an effort to detect, prevent, and remove viruses, Trojan horses, malware, worms, or similar harmful, malicious, or hidden procedures, routines, or mechanisms that may result in: **(a)** inoperability of ThoughtSpot Cloud; or **(b)** interruption or interference with the operation of ThoughtSpot Cloud (collectively, "**Malicious Code**"). If ThoughtSpot Cloud is found to contain any Malicious Code that adversely affects the performance of Customer's instance of ThoughtSpot Cloud or causes a material security risk to data received in Customer's instance of ThoughtSpot Cloud, ThoughtSpot shall, as Customer's exclusive remedy, use commercially reasonable efforts to remove the Malicious Code. Customer will be responsible for any security vulnerabilities, and the consequences of such vulnerabilities, including any Malicious Code in Customer data, software, systems, or integrations that adversely affects the performance of ThoughtSpot Cloud or causes a material security risk to Customer.

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

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

4.13. **Secure Software Development**. ThoughtSpot will 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 will perform a combination of static and dynamic testing and analysis of code prior to the release of such code to Customers.

5. Organizational Security Measures.

5.1. **ThoughtSpot Access Limitations**. ThoughtSpot employees or contractors will not do any of the following to data uploaded by Customer to ThoughtSpot Cloud without Customer's prior consent or unless as part of a functionality of ThoughtSpot Cloud initiated by or for Customer (*e.g.*, data integrations or data transferability between instances): **(a)** access the data; **(b)** move the data outside Customer's tenant (except as initiated by Customer or for Customer by a third party); or **(c)** screen-capture, copy, or record the data in video or other formats.

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's instance of ThoughtSpot Cloud in accordance with ThoughtSpot's then-current applicable standard operating procedure and subject to applicable laws. Background screening includes at least the following, as permitted by applicable law: **(a)** social security verification; **(b)** prior employment verification; **(c)** personal and professional references; **(d)** educational references; **(e)** criminal history; and, as applicable for the position, **(f)** motor vehicle records; (**g)** credit history; and **(h)** drug screening.

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's instance of ThoughtSpot Cloud. 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, for appropriate security and privacy controls and business disciplines, vendors that access, store, process, or transmit data received in Customer's instance of ThoughtSpot Cloud.

5.6. **Software Inventory**. ThoughtSpot will maintain an inventory of all software components (including open source software) used in ThoughtSpot Cloud. With the exception of free and open source software available under licenses from third parties, Customer has no rights in or entitlement to receive copies of the software used by ThoughtSpot to render ThoughtSpot Cloud.

6. Service Continuity.

6.1. **Backup**. ThoughtSpot will maintain back-ups of Customer's metadata and ThoughtSpot's service state in the same region in a different availability zone pursuant to the standard operating procedure during the Subscription Term. In addition, ThoughtSpot will take regular snapshots, to be stored in the same environment as Customer's instance of ThoughtSpot Cloud during the Subscription Term.

6.2. **Risk Management**. ThoughtSpot will: maintain a Risk Management Policy consistent with industry standards that will: **(a)** that define the process for identifying, responding to, mitigating, and reporting risks; **(b)** document and sort assets and allocate a risk determination for each; **(c)** appoint risk owners to determine the appropriate risk treatment plan and response strategy for each, considering impact rating and likelihood of exposure.

6.3. **Disaster Recovery**. ThoughtSpot will: **(a)** maintain a disaster recovery ("**DR**") plan for ThoughtSpot Cloud that is consistent with industry standards; **(b)** test the DR plan at least once per calendar 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 ThoughtSpot Cloud from being recovered in accordance with the DR plan.

6.4. **Business Continuity**. ThoughtSpot will maintain a business continuity plan ("**BCP**") to minimize the impact to its provision and support of ThoughtSpot Cloud from an event. The BCP will: **(a)** include processes intended to protect personnel and assets and restore functionality in accordance with the time frames outlined in the BCP; and **(b)** be tested annually and updated based on any deficiencies identified and recognized by ThoughtSpot during such tests.

6.5. **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 technical support operations.

6.6. **Insurance**. ThoughtSpot will maintain in effect during the Subscription Term, at ThoughtSpot's expense, the following minimum insurance coverage: **(a)** Worker's Compensation Insurance, in accordance with applicable statutory, federal, and other legal requirements; **(b)** Employers' Liability Insurance covering ThoughtSpot's employees in an amount of not less than $1,000,000 for bodily injury by accident and $1,000,000 each employee for bodily injury by disease; **(c)** Commercial General Liability Insurance written on an occurrence form and including coverage for bodily injury, property damage, products and completed operations, personal injury, and advertising injury arising out of the products or services provided by ThoughtSpot under the Agreement, with minimum limits of $1,000,000 per occurrence/$2,000,000 aggregate (personal and advertising coverage maybe provided by the Errors & Omissions/Media policy); **(d)** Commercial Automobile Liability Insurance providing coverage for hired and non-owned automobiles used in connection with the Agreement in an amount of not less than $1,000,000 per accident, combined single limit for bodily injury and property damage; **(e)** Combined Technology Errors' & Omissions Policy with a $5,000,000 per claim limit, including: **(i)** Professional Liability Insurance providing coverage for the services and software in the Agreement (which coverage will be maintained for at least two years after termination of the Agreement); and **(ii)** Privacy, Security, and Media Liability Insurance providing liability coverage for unauthorized access or disclosure, security breaches, and system attacks, as well as infringements of copyright and trademark that might result from the Agreement; and **(f)** Excess Liability over Employers' Liability, Commercial General Liability, and Commercial Automobile Liability, with a $5,000,000 aggregate limit. For the purposes of this Section 6.5, a "claim" means a written demand for money or a civil proceeding which is commenced by service of a complaint or similar pleading. A certificate of insurance reflecting the coverage amounts provided in this Section 6.5 is available to Customer upon written request.

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 incident management policy. ThoughtSpot's security group will escalate and engage response teams as ThoughtSpot deems 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's instance of ThoughtSpot Cloud (a "**Breach**") without undue delay following determination by ThoughtSpot that a Breach has occurred.

7.3. **Report**. The initial Breach 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 will provide without undue delay any further information learned by ThoughtSpot 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, the European Union's General Data Protection Regulation and the United Kingdom's General Data Protection Regulation. The Breach 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. Notwithstanding the foregoing, Customer acknowledges that because ThoughtSpot personnel do not review data uploaded by Customer to ThoughtSpot, it may be unlikely that ThoughtSpot can provide information as to the particular nature of that data, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of ThoughtSpot with Customer in connection with a Breach will not be construed as an acknowledgement by ThoughtSpot of any fault or liability with respect to the Breach. As used in this Program Guide, "**Personal Data**" means any information relating to an identified or identifiable natural person uploaded to ThoughtSpot Cloud by or for Customer or Customer's agents, employees, or contractors; and "**Processing**" means any operation or set of operations that is performed on 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.

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 take measures intended to 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 Cloud 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 ThoughtSpot Cloud without ThoughtSpot's express written authorization. Penetration testing information is available pursuant to an Audit as described in Section 2.1 (*Audit*).

9. Sharing the Security Responsibility.

9.1. **Product Capabilities**. ThoughtSpot Cloud is designed to allow Customer to: **(a)** authenticate users before accessing Customer's instance; **(b)** integrate with SAML-compatible identity provider 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: **(i)** managing each user's access to, and use of, ThoughtSpot Cloud by assigning to each user a credential and role that controls the level of access to ThoughtSpot Cloud; **(ii)** its decision to index data containing sensitive information, 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 sensitive information; **(iii)** protecting the confidentiality of administrative credential information, including each user's login and password, and managing roles, rights, maintaining user logins for each individual person, and granting each user's access to ThoughtSpot Cloud; and **(iv)** 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 information that Customer processes using ThoughtSpot Cloud.

9.2. **Industry-Specific Regulations**. Customer acknowledges that ThoughtSpot Cloud is not intended for any industry-specific use and ThoughtSpot does not review data or assess regulatory impacts. Customer is solely responsible for compliance with regulations, laws, rules, or other requirements applicable to its industry and managing indexing in ThoughtSpot Cloud to comply with such requirements. Customer acknowledges that: **(a)** ThoughtSpot is not a Business Associate and should not process patient, medical or other protected health information regulated by the U.S. Health Insurance Portability and Accountability Act unless the parties have expressly agreed otherwise in a Business Associate Addendum; and **(b)** ThoughtSpot is not compliant with Payment Card Industry Data Security Standards and Customer will not (and will not permit others to) process payment card information into ThoughtSpot Cloud.

9.3. **Improving Features**. ThoughtSpot Cloud includes certain Improving Features that interact with users and Administrative Information. Although all Administrative Information will be deleted or returned to Customer (or never stored), Customer acknowledges that the accuracy, performance, and user experience of ThoughtSpot Cloud will improve with such interactions across ThoughtSpot's customers, including Customer, and their respective users. Without limiting the terms of the Agreement, and as between the parties, nothing in this paragraph will affect Customer's sole ownership of its Administrative Information and ThoughtSpot's sole ownership of ThoughtSpot Cloud, including, without limitation to any intellectual property therein used to develop, improve, operate, or otherwise provide ThoughtSpot Cloud. If Customer is uncomfortable with the foregoing, then Customer may deactivate (or request through a Support ticket that ThoughtSpot deactivate), the Improving Feature with the understanding that its benefits will not be received. By using Improving Features, Customer expressly agrees to all terms in this Section, that improvements made to the Improving Features through user and Administrative Information interactions will be retained by ThoughtSpot, and that ThoughtSpot's provision, operation, and maintenance of Improving Features is within the scope of ThoughtSpot's obligations under the Agreement to provide ThoughtSpot Cloud. As used above, "**Improving Features**" means machine or deep learning systems, statistical learning, models (*e.g.*, language models), neural networks, and other related programs, tools, or methods and the implementation of any of those, the format, content, contextual information, weights, and combinations of input and output of data and content used with the foregoing, and their component hardware or equipment.

9.4. **Human in the Loop and Controls**. ThoughtSpot does not guarantee the generation of Output by an Improving Feature. Customer is responsible for: (a) reviewing, editing, and amending any Output before publishing, using, or relying on such Output; and (b) implementing reasonable practices, including human oversight, to guard against Outputs being used in an unsuitable or unlawful way or in violation of the rights of others. Customer shall not disable, evade, disrupt, or interfere with any content filters or safety systems that are part of Improving Features. "Output" means any response or result from an Improving Feature provided to a Customer within ThoughtSpot Cloud after processing an Input but explicitly excludes the graphical user interface elements of ThoughtSpot Cloud that may be included in Output. "Input" means any natural language statement, SQL request, prompt, or other query that an Authorized User provides to the ThoughtSpot Cloud to solicit a response or result from an Improving Feature.

9.5. **High-Risk Activity**. Customer understands that ThoughtSpot Cloud is intended for information searching and analytics, and must use ThoughtSpot Cloud within the intended business purposes described in the Documentation and not for any purpose that: (a) requires fail-safe processing performance, including stock trading, financial transaction processing such as credit card processing, business automation, electronic funds transfer, check clearing, management of hazardous facilities or applications for which failure could result in death, personal injury, or severe physical or environmental damage; (b) constitutes high or unacceptable risk relating to the use of the applicable Improving Features under applicable law or regulation; (c) would mislead anyone to believe that an Output related to Improving Features was solely human generated; (d) make Fully Automated Decisions that have an effect on individuals; or (e) would otherwise violate applicable law or regulation (collectively, "**High-Risk Activity**"). ThoughtSpot, its licensors and suppliers expressly disclaim all warranties of fitness for any such use and Customer releases and holds ThoughtSpot, its licensors and suppliers harmless from liability arising out of use of ThoughtSpot Cloud for or in relation to any High-Risk Activity. "Fully Automated Decision" means any action triggered by systems and software, including those using artificial intelligence, machine learning and other data processing techniques, without any human involvement or intervention.

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

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