VISIER CUSTOMER DATA SAFEGUARDS POLICY

Last Updated: March 11, 2025

This document sets forth the Customer Data Safeguards Policy ("Safeguards Policy") referenced in the Visier Master Software as a Service Agreement entered into by and between Visier and Customer ("MSA"). This Safeguards Policy is governed by the MSA and all provisions of the MSA apply to this Safeguards Policy. If there is any conflict between this Safeguards Policy and the MSA, the MSA will prevail with respect to matters within its scope. Capitalized terms not otherwise defined herein have the meanings assigned to them in the MSA. For purposes of this Safeguards Policy, the terms "We/we", "Us/us", and "Our/our" shall refer to Visier, and the terms "You/you" and "Your/your" shall refer to Customer.

1. Customer Data Submission Requirements

   In order to maintain a high level of data security, Visier adheres to a well-defined process for handling submissions of Customer Data. Customer's compliance with this process is required for Visier to accept submissions of Customer Data. You will only use the following methods to submit Customer Data to Visier:

   a. by manually initiated upload to Visier's servers through the Visier People application using the encrypted browser protocol (HTTPS);

   b. by automated or manually initiated file upload to Visier's servers using the secure file transfer protocol (sFTP), encrypted with Customer's public/private SSH key, to the encrypted storage folder designated by Visier for Customer's data uploads; or

   c. by an API POST call with a JSON or attachment with a data stream once a data model is defined;

   d. Customer-configured automated data connection workflow for a supported Source System via API (configuration options are available to Authorized Users with administrative-level access to the SaaS Services); or

   e. by forms made available within the applicable SaaS Services.

   Any data provided by You to Visier in contravention of this Section shall not be considered Customer Data.

2. Organizational Security

   a. Visier has implemented and will maintain security and privacy programs that follow the National Institute of Standards and Technology (NIST) Cybersecurity framework and International Standards Organization (ISO) 27001. These programs consist of policies, procedures and personnel training to assess and manage administrative and technical measures to safeguard Customer Data.

   b. Visier has implemented and will maintain procedures that require all personnel authorized by Visier to access Customer Data to have successfully completed, prior to being granted such access, an enhanced background check that, to the extent permitted by country specific laws and regulations, verifies identity, legal right to work in the jurisdiction, education (most recent), employment history (most recent and relevant, up to 7 years where available), criminal history, credit history (role specific), and sanctioned party checks. Visier will not authorize access to Customer Data if a criminal history check discloses a conviction for theft, robbery, fraud, or violence where (i) such offence is legally permitted to be considered, (ii) a pardon has not been granted, and (iii) said offence was committed within the past (10) years or, if the individual was a minor at the time the offense was committed, then within the past (5) years. Should Visier later become aware that any of its personnel with access to Customer Data has a criminal conviction that, in Visier's sole determination, would have precluded such individual from receiving authorization for access based on the terms of this paragraph, Visier will revoke such individual's access unless and until Customer provides its written consent.

   c. Visier has implemented measures that require all personnel authorized to access Customer Data to confirm their understanding and compliance with Visier's policies, including, at minimum, maintaining confidentiality, privacy requirements and security incident reporting.

   d. Visier has implemented privacy and security awareness programs that provide general user and role-based education training to personnel authorized to access Customer Data.

e. Visier has implemented measures for annual compliance training that requires all personnel authorized to access Customer Data to complete assigned internal policies, privacy and security training.

f. Visier has implemented third party risk management programs that assess cloud providers to ensure adequate processes are in place for any planned outsourced services. The assessments include security, reviews of independent audit reports and or certifications, penetration testing results, privacy programs, integrations with other systems, results of the proof of concept, etc. prior to onboarding the cloud providers. Additional measures are in place to monitor the performance of these contractual agreements in accordance with service level agreements.

g. Visier at least annually conducts internal assessments on the design and operating effectiveness of its internal controls for the Customer-facing environments. These assessments on a rotation basis may include reviews of segregation of duties, conformance to internal policies such as authentication standards, change management, personnel onboarding and off-boarding procedures, incident management, etc. Any non-compliance matters identified are communicated to stakeholders and remediation plans are established.

h. Visier will retain an independent third-party auditor to perform a SOC2 Type II (or equivalent) audit at least annually covering the Trust Service Principles of security, confidentiality and availability. At Customer's request, Visier will provide a report of its recently completed SOC2 Type II audit (or equivalent audit).

3. Logical Security

a. Visier limits access to Customer Data to personnel who need to know such information and who have met the enhanced background check requirements.

b. Visier has implemented technical and organizational identity and access controls to minimize the potential of unauthorized access to Customer Data, including, without limitation, the following:

i. formal procedures and processes for requesting, granting, revoking, reviewing, and auditing access profiles used by personnel to provide the SaaS Services;

ii. unique identification of the user or service account accessing the systems;

iii. prohibition of the use of shared accounts;

iv. restricted allocation of privileged and administrator access at the application, database, operating system, and network components in line with segregation of duties;

v. use of individual user ID and passwords in-line with internal policies that consider minimum length, complexity, history, and lockout functionality; and

vi. use of strong authentication protocols such as single-sign on (SSO) with at least two factor authentication (2FA) for all authorized personnel including any remote access to Visier systems and Customer environments.

c. Visier's Customers have a choice in using SSO or 2FA authentication methods. Any Customers not using SSO will automatically have 2FA enabled, unless explicitly requested by you in writing to disable 2FA.

d. Visier has implemented periodic access reviews of all personnel authorized with access to Customer Data to ensure user access is commensurate with their roles and responsibilities.

e. Visier has implemented measures to logically separate its Customer's Data from the data of other customers through use of technical controls.

f. Visier has implemented measures to restrict access to its Customer Data through role-based access across its products.

g. Visier has implemented measures to identify and detect any logins or access provisions for administrator access using automated alerts.

4. Network and Endpoint Security

a. Visier has implemented network security access controls to protect against unauthorized access through both user accounts and devices such as segmentation of production and non-production environments, configuration of firewalls and other network boundary devices to restrict and or re-direct traffic.

b. Visier has deployed measures on intrusion prevention and detection systems (IPS/IDS) to identify and detect any indicators of attack.

c. Visier has implemented anti-virus/malware protection for its end points (such as laptops, servers, etc.) with automated signature updates, identification, and quarantine of any endpoint malware.

d. Visier has implemented a vulnerability management policy and patch management standard to ensure critical patches are deployed to endpoints in line with its risk assessment and change management practices.

e. Visier has implemented content filtering mechanisms on email to detect any virus/malware.

f. Visier has implemented processes for retention and investigation of event logs identified through its IPS/IDS or other monitoring tools.

5. Threat and Vulnerability Monitoring and Assessments

a. Visier has implemented and will maintain risk, vulnerability, and threat management policies and procedures to periodically assess the security and risks associated with the SaaS Services, including, but not limited to:

i. penetration testing of the SaaS Services at least annually by a qualified third-party security assessment firm engaged by Visier (a report of the results of such tests, including Visier's response and mitigation plans, will be made available to Customer upon request);

ii. internal vulnerability assessments, performed on a regular basis, of the infrastructure and applications used to provide the SaaS Services; and

iii. remediation plans implemented based on the perceived risk and potential harm that may result from the identified vulnerabilities, as determined by Visier in its sole discretion.

b. Visier will monitor the systems used to deliver the SaaS Services for unauthorized access to or misuse of Customer Data by:

i. logging user activities, exceptions, unauthorized information processing activities and suspicious activities;

ii. protecting logging facilities and log information against unauthorized access;

iii. retaining logs as reasonably necessary for up to 7 years or as required by applicable law; and

iv. performing frequent reviews of logs and taking reasonably necessary actions to protect against unauthorized access or misuse, as determined by Visier.

6. Encryption

Visier has implemented and will maintain the following encryption policies and procedures:

a. Customer Data stored in data centers will be encrypted in media using, at minimum, AES256-bit encryption;

b. Customer Data supplied by Customer or otherwise transferred to an authorized third-party service provider to be encrypted by Visier in transit using the following methodologies:

i. through the Service using, at minimum, TLS 1.2 AES 128-bit encryption and perfect forward secrecy when using HTTPS; or

ii. through secure file transport protocol (sFTP), at minimum, AES 128-bit encryption;

c. Customer Data transmitted between data centers or between Visier personnel and a data center will be encrypted with, at minimum, AES 256-bit; and

d. Hard drives on all end user devices are encrypted prior to being assigned to any personnel.

7. Physical Access and Environmental Security

a. Visier's data centers are hosted by cloud service provider(s) that have controls such as security cameras, physical ID passes for its authorized personnel, access control mechanisms to the infrastructure, environment controls such as uninterruptible power supply, temperature control, fire suppressant mechanisms, etc.

b. Visier has implemented measures whereby no personnel are authorized to access the cloud service providers' data center other than their employees.

c. At least annually, Visier will review and validate the controls and contracts of its data center provider(s) to assess the operating effectiveness and identify any control deficiencies as evidenced by each data center provider's annual SOC2 Type II audit report (or equivalent). Such reports are available to the Customer upon request, subject to any additional confidentiality terms required by the data center provider's auditor.

d. Visier has implemented measures to restrict access to its office locations through use of keycard pass. Procedures are in place to request approvals to grant, modify and revoke access keycard pass.

e. Visier has implemented and will maintain procedural controls to restrict the use of hardcopy Customer Data including workspace security restrictions configured to prevent Visier personnel from copying, printing, or exfiltrating Customer Data.

f. Visier provides for secured on-site locked boxes for shredding of sensitive hardcopy materials.

g. Visier has implemented and will maintain procedural controls pertaining to physical security of hardware including limiting physical access to office space through secure means.

8. System Maintenance

Visier has implemented and will maintain documented change control procedures for:

a. planning, documenting, testing and approving modifications to the environments (e.g., application, operating system, and hardware level changes) used to provide the SaaS Services to protect the confidentiality, availability, and security of information systems;

b. granting, monitoring, and removing emergency access; and

c. introducing unscheduled changes to the SaaS Services environment.

Separation of duties will exist to ensure that changes are recorded and properly authorized (e.g., developers can not directly update programs, job control parameters, or other components of the Service environment). Where separation of duties cannot be maintained for practical reasons, mitigating controls, including monitoring of the affected personnel, will be implemented.

9. Customer Penetration Testing

a. No more than twice per calendar year, on Customer's reasonable request, Visier will provide appropriate support to Customer to perform penetration tests against Visier-provided test servers for the SaaS Services, provided that such tests are performed:

i. at the sole expense of Customer;

ii. under supervision by Visier personnel;

iii. on a schedule agreed in advance between Customer and Visier; and

iv. in a responsible manner consistent with test guidelines provided by Visier prior to testing; and

v. not against production servers.

b. Customer may engage a third party to perform such penetration tests on Customer's behalf ("Testing Provider"), provided that:

i. Customer obtains Visier's prior written consent;

ii. Testing Provider agrees to abide by the terms of this Section applicable to Customer; and

iii. Testing Provider agrees to terms of confidentiality reasonably acceptable to Visier;

c. Promptly after completion of each penetration test, Customer (or its Testing Provider, if applicable) must provide a full, detailed report of its test results to Visier.

10. Security Incident Response

"Security Incident" means a compromise of Visier's systems in which Customer Data has been accessed or acquired by one or more unauthorized persons or parties or that Visier reasonably suspects may have resulted in such unauthorized access, or the receipt of a threat of such an incident that, in Visier's opinion, is credible, imminent and reasonably likely to occur.

a. Upon discovery or notice of any Security Incident, Visier will:

   i. immediately commence an investigation of such Security Incident; and

   ii. notify Customer of such Security Incident within twenty-four (24) hours following confirmation.

b. Visier's receipt of a threat from a third party to cause a Security Incident that Visier believes, in its sole discretion, to be credible will be investigated and evaluated in the same manner as if discovered by Visier.

c. Visier's notification to the Customer of a Security Incident as required in this Safeguards Policy will consist of a telephone call and/or e-mail to the Security Contact. Such notification will include the following information, to the extent known by Visier at the time of providing notice:

   i. the nature and extent of the Customer Data potentially involved in the Security Incident;

   ii. identification of the individuals whom Visier knows or reasonably believes to have improperly used, disclosed, or accessed Customer Data;

   iii. a description of where Visier knows or reasonably believes the affected Customer Data to have been improperly transmitted; and

   iv. a description of the probable cause(s) of the Security Incident.

d. Promptly following discovery or notice of any Security Incident, Visier will:

   i. take corrective action to mitigate any risks or damages involved with such Security Incident and to protect the SaaS Services and Customer Data from any further compromise; and

   ii. take any other actions that are required by applicable law as a result of such Security Incident.

e. Within ten (10) business days where feasible following discovery or notice of any Security Incident, Visier will provide the Security Contact a written report of measures planned and taken to prevent, halt, and/or contain the Security Incident.

11. Business Continuity and Disaster Recovery

a. Visier has implemented and will maintain: (i) Business Continuity Policy; and (ii) Disaster Recovery Plan. These will be reviewed and updated periodically to reflect changes in the environment.

b. Visier has implemented and will maintain near real-time replication technologies within each of its data center regions to support both operational and disaster recovery requirements of the SaaS Services.

c. Visier tests the ability to recover all components of the SaaS Services at least annually by performing multiple discrete component validation and recovery tests periodically throughout the year.

d. Visier will invoke its Business Continuity Policy and Disaster Recovery Plan upon its declaration of a Major Disruption with the objective of recovering critical functions within the recovery time objectives set forth in the table below.

Critical Functions/Systems	Recovery Time Objectives	Recovery Point Objective
Data transform and load services	48 hours	Resume transform and load activities for data transfers completed more than 48 hours prior to the occurrence of the Major Disruption
Voice response services	24 hours	Ability to answer telephone calls

Critical Functions/Systems	Recovery Time Objectives	Recovery Point Objective
Customer Experience reps	24 hours	Ability to answer telephone calls and access services to assist callers
SaaS application services	24 hours	Re-establish facilities or provide alternate means to enable access to Customer Data published to the SaaS Services more than 24 hours prior to the occurrence of the Major Disruption

"Major Disruption" means a business interruption or failure of sufficient severity that Visier is unable to perform the SaaS Services as required by the Agreement, and the SaaS Services are not reasonably expected to be recoverable or remedied within the applicable recovery time objectives without recourse to the Business Continuity Policy and Disaster Recovery Plan.

e. The recovery of critical functions does not require that the critical functions perform in strict accordance with the Documentation, but that the critical functions will be substantially usable and accessible to the Customer.

f. Visier will not charge any additional fees under the Agreement for responding to a Major Disruption in accordance with its Business Continuity Policy and Disaster Recovery Plan. However, Visier reserves the right to charge additional fees where Customer requests services outside the scope of the Business Continuity Policy and Disaster Recovery Plan.

12. Personal Data not otherwise comprising Customer Data

Through the ordinary interaction between Customer and Visier, Customer could provide to Visier limited Personal Data other than through Customer's transfer of Customer Data (e.g., email signatures, business contact information, and similar). Such Personal Data is Customer's Confidential Information and may be processed by Visier in connection with its delivery of the SaaS Services. Visier has implemented reasonable and appropriate physical, technical, and organizational safeguards to protect such information, including implementation of measures to mitigate risk to, maintain confidentiality of, and to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, such information, taking into consideration the likelihood and severity of the risk to the rights and freedoms of the affected consumers/data subjects.

13. Removal of Data

Upon expiration or termination of the Agreement, or upon receipt of Customer's written request signed by a duly authorized representative of Customer, Visier will delete and/or destroy, using methods consistent with NIST SP800-88r1, the Customer Data from its systems and storage media and any offsite storage and third-party facilities under its control within thirty (30) days. Upon request following such removal, Visier will provide Customer with a written certification of such removal within thirty (30) days. Backups created during the term of the Agreement are retained for up to ninety (90) days and thereafter are automatically deleted and/or destroyed in accordance with the methods identified in this Section. The foregoing notwithstanding, Visier may retain portions of Customer Data in accordance with its procedures implemented to comply with applicable law or regulation, litigation hold requirements or audit logging requirements, provided that such portions of Customer Data remain subject to the terms of the Agreement and this Safeguards Policy and may not be used except for such compliance purposes.

14. Policy Updates

Visier may update this Safeguards Policy from time to time in its sole discretion by posting the updated Safeguards Policy to Visier's Trust Site. Updates to this Safeguards Policy posted during the term of an Order will not serve to modify the version of this Safeguards Policy applicable to you during the remainder of such term. Upon renewal, the version of this Safeguards Policy current as of the renewal date will become effective with respect to the SaaS Services.

End Visier Customer Data Safeguards Policy