insightsoftware

SECURITY ADDENDUM

This Security Addendum is incorporated into and made a part of the written agreement between insightsoftware and Customer that references this document (the "**Agreement**") and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this Security Addendum, this Security Addendum shall govern. This Security Addendum sets forth the security controls and standards maintained by insightsoftware ("Security Program"). insightsoftware regularly tests and evaluates its Security Program, and may review and update its Security Program as well as this Security Addendum, provided, however, that such updates shall be designed to enhance and not materially diminish the Security Program.

1. **insightsoftware Corporate Security Controls.**

   a. **Administrative Controls.**

      i. **Dedicated Information Security Team.** insightsoftware's Security Program is managed by a dedicated team of information security professionals, led by the insightsoftware VP and Chief Information Security Officer.

      ii. **Security Policy**. insightsoftware maintains a written security policy based on industry standards and in compliance with applicable data protection laws ("Data Protection Laws"), which is reviewed and updated annually and made available to all insightsoftware personnel.

      iii. **Background Checks**. insightsoftware conducts criminal background screening on its employees as part of its hiring process in compliance with applicable laws. Background checks are provided for all employees in some countries and, in other countries, are available to be performed upon request.

      iv. **Security Awareness Training.** insightsoftware maintains a documented security awareness training program for its personnel, including new hire and on-going training.

      v. **Code of Conduct; Confidentiality Agreements; Information Security Policy**. insightsoftware personnel are required to acknowledge and agree to several policies and agreements that require employees to maintain the confidentiality of Customer Data and follow security processes related to Customer Data, including the insightsoftware Code of Conduct, employee confidentiality agreements and the insightsoftware Information Security Policy.

      vi. **insightsoftware Risk Management & Threat Assessment.** insightsoftware has a documented risk management process. insightsoftware's Information Security Committee meets regularly to review reports and material changes in the threat environment, identify potential control deficiencies and make recommendations for new or improved controls and threat mitigation strategies.

      vii. **External Threat Intelligence Monitoring.** insightsoftware reviews external threat intelligence feeds, including US-Cert vulnerability announcements, critical vendor security advisories and other trusted sources of vulnerability and threat information.

      viii. **Vendor Risk Management.** insightsoftware evaluates vendors that process Customer Data or are part of an insightsoftware solution, to ensure they maintain security measures consistent with insightsoftware's obligations in this Security Addendum and in compliance with Data Protection Laws.

   b. **Incident Detection and Response.**

      i. **Incident Response Plan.** insightsoftware maintains a documented incident response plan, which includes incident reporting, response, roles and responsibilities, prioritization, escalation and remediation. The plan is tested and updated periodically.

      ii. **Security Incident Reporting.** If insightsoftware becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "Security Incident"), insightsoftware shall notify Customer without undue delay, and in any case, within 48 hours after determining a Security Incident has impacted or will impact the Customer Data.

      iii. **Investigation.** In the event of a Security Incident, insightsoftware shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Any logs determined to be relevant to a Security Incident, shall be preserved for at least one year.

      iv. **Communication and Collaboration.** insightsoftware shall provide Customer timely information about the Security Incident to the extent known to insightsoftware, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by insightsoftware to mitigate or contain the Security Incident, the status of insightsoftware's investigation, and a contact point to obtain additional information.

v. **Cyber Insurance.** insightsoftware maintains a Cyber/Technology Errors & Omissions Liability insurance policy with a Policy Holder Alphabetic Category Rating of not less than "A-" and Financial Size Category Rating of not less than "VII" according to the latest edition of A.M. Best's Key Rating Guide.

c. insightsoftware Corporate Office Physical & Environmental Controls. insightsoftware's technical, administrative, and physical controls for its corporate offices covered by its ISO 27001 certification include, but are not limited to:

i. Physical access to the corporate office is controlled at ingress points;
ii. Badge access is required for all personnel and badge privileges are reviewed regularly;
iii. Visitors are required to sign in;
iv. CCTV covers building ingress points;
v. Fire detection and protection systems; and
vi. Climate control systems.

d. insightsoftware System Security.

i. Malware and Vulnerability Protection. insightsoftware laptops, desktops and production servers are protected with auto-updating anti-malware protection and vulnerability monitoring. Email, including links and attachments in emails, are scanned for malware before being delivered.
ii. Disk Encryption. insightsoftware laptop hard drives are encrypted.
iii. Patching. Security patches are reviewed and deployed at least monthly.
iv. Secure Disposal. insightsoftware follows a documented process for the secure deposal of assets which store data.
v. Multi-factor Authentication. Remote access to insightsoftware networks require multi-factor authentication.

e. Secure Software Development.

i. Security is part of the entire software development lifecycle.
ii. Development systems are separate from production systems.
iii. Customer Data is not transmitted to or stored on development systems.
iv. Application security testing is built into the software development pipeline.
v. A source code control system is utilized that authenticates and logs the person associated with all changes to the software or custom code baseline and all related configuration and build files.
vi. Source code is backed up and protected.

2. Cloud Security Controls and Safeguards.

a. Security Responsibilities. insightsoftware provides its software either (i) on an on-premise basis, whereby the software is installed on Customer's computers, or (ii) as a hosted service, whereby insightsoftware utilizes infrastructure-as-a-service cloud providers and/or secure colocation facilities to provide Customers access to the insightsoftware software (the "Cloud Environment"). With respect to insightsoftware's on-premises software, which is installed on Customer's computers, the Customer is responsible for maintaining the security of Customer's computers, including all patching, access controls, firewalls, physical security, backups and encryption. When insightsoftware's software is provided via a Cloud Environment, insightsoftware is responsible for maintaining the security controls and safeguards described below. insightsoftware maintains a comprehensive documented security program under which insightsoftware implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the software and Customer Data.

b. insightsoftware's Audits and Certifications.

i. insightsoftware maintains the audits and certifications described at https://legal.insightsoftware.com/contracts/ISO&SOC-certifications.pdf.
ii. Reports by independent third-party auditors are made available to Customer upon request.

c. **Hosting Location of Customer Data.** insightsoftware uses subservice organizations whose controls are assessed via SOC 2 audits to ensure they are suitably designed and operated to comply with insightsoftware's security requirements.

d. **Encryption.**

  i. **Encryption at Rest**. Customer data residing in the Cloud Environment are encrypted at rest.

  ii. **Encryption Key Management.** All cryptographic keys are protected from unauthorized disclosure or use.

    1. Encryption keys are created in compliance with the then current industry standard strength recommendations.
    2. Any key that becomes weak due to outdated algorithms or is suspected of compromise is retired and/or rotated with an updated key.
    3. Certificates are utilized to encrypt keys used to encrypt data.

  iii. **Encryption in transit.** Secure data transmission protocols are used to encrypt confidential data when transmitted over public networks.

e. **System and Network Security.**

  i. **Access Controls.** All insightsoftware personnel access to the Cloud Environment is via a unique user ID with a complex password and multi-factor authentication. Access to systems and data is provided to individuals when required to perform their job functions and is consistent with the principle of least privilege.

  ii. **Separation of Environments.** insightsoftware logically separates production environments from development and testing environments. The Cloud Environment is both logically and physically separate from insightsoftware's corporate offices and networks.

  iii. **Change Management.** insightsoftware maintains a documented change management program for its software.

  iv. **Firewalls/Security Groups.** insightsoftware's Cloud Environment uses industry standard firewall or security groups technology with deny-all default policies to permit only business-required network traffic protocols and to protect systems from untrusted networks.

  v. **Personnel Access Reviews & Separation.** insightsoftware reviews the access privileges of its personnel to the Cloud Environment at least quarterly and removes access on a timely basis for all separated personnel.

  vi. **Hardening.** The Cloud Environment is hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Addendum.

  vii. **Patching.** Security patches are reviewed and applied to systems on a regular basis in accordance with established policies and standards.

  viii. **Monitoring & Logging.** Monitoring tools and services are utilized to log specific activities and changes within the Cloud Environment. These logs are further monitored and analyzed for anomalies when necessary. The logs are securely stored to prevent tampering.

  ix. **Endpoint Protection**. The Cloud Environment leverages auto-updating threat detection tools to monitor for and provide protection from suspicious activities and malware (collectively, "Malicious Activity") on in-scope endpoints. insightsoftware does not monitor Customer Data for Malicious Activity.

  x. **Vulnerability Management.** Systems in the Cloud Environment are automatically evaluated for vulnerabilities, which are then prioritized for remediation based on their potential impact to insightsoftware's software.

  xi. **Penetration Testing**. insightsoftware engages one or more independent third parties to conduct penetration tests of selected software at least annually. Upon Customer's written request, insightsoftware shall provide Customer an executive summary of any such penetration test.

f. **Cloud Data Center Physical & Environmental Controls.** To ensure the Cloud Environment has appropriate physical and environmental controls for the data centers hosting the software, insightsoftware regularly reviews Cloud Environment security controls audited under by independent third-party audits and certifications. Each Cloud Environment provider has a SOC 2 Type II annual audit and ISO 27001 certification, or industry-recognized equivalent framework. Such controls include, but are not limited to, the following:

i. Physical access to the facilities and physical systems is controlled;
ii. Physical access privileges are reviewed regularly;
iii. Visitors are required to present ID and sign in;
iv. CCTV covers all ingress points;
v. Fire detection and protection systems;
vi. Power back-up and redundancy systems;
vii. Climate control systems; and
viii. Established NIST 800-88 compliant processes for decommissioning hardware assets.

g. Deletion of Customer Data by insightsoftware. Subject to applicable provisions of the Agreement, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination “retrieval period” set forth in the Agreement, insightsoftware promptly deletes any remaining Customer Data.

h. Business Continuity and Disaster Recovery. Automated backup systems perform scheduled backups of production databases. For the software for which insightsoftware maintains audits, a business continuity and disaster recovery plan is in place to ensure the resumption of time-sensitive operations and services in the event of a disastrous event that causes a significant business interruption. The business continuity and disaster recovery plan contains detailed responsibilities and specific tasks for emergency response activities and business resumption operations based upon pre-defined time frames. The plan is reviewed and tested on an annual basis to validate that documented procedures are appropriate and to ensure that personnel understand the plan and the role that they play in executing the plan.

3. Customer Audit Rights. Upon written request and at no additional cost to Customer, insightsoftware shall provide Customer, and/or its appropriately qualified third-party representative (collectively, the “Auditor“), access to reasonably requested documentation evidencing insightsoftware’s compliance with its obligations under this Security Addendum in the form of, as applicable, (i) insightsoftware’s ISO 27001 certification, (ii) insightsoftware’s SOC 2 Type II audit report and/or SOC 1 Type II audit report, (iii) insightsoftware’s most recently completed Shared Assessments Standardized Information Gathering (SIG) Questionnaire, and (iv) the most recent penetration test summary report for the relevant Software (“Audit Reports”). In the event insightsoftware is unable to provide an Audit Report, insightsoftware agrees to complete any Customer-provided information security questionnaire on an annual basis within six (6) weeks of Customer’s written request. Where the Auditor is a third-party, such third party may be required to execute a separate confidentiality agreement with insightsoftware prior to any review of Audit Reports, and insightsoftware may object in writing to such third party if in insightsoftware’s reasonable opinion the third party is not suitably qualified or is a direct competitor of insightsoftware. Any such reasonable objection by insightsoftware will require Customer to appoint another third party. Any expenses incurred by an Auditor in connection with any review of Audit Reports, or a customer-provided questionnaire shall be borne exclusively by the Auditor.