Technical and Organizational Measures

Description of the technical and organizational measures implemented by Planview (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Planview shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality, and integrity of Customer Data, including Personal Data (the "**Security Measures**").

1. Security Management.
Planview will maintain an effective security management program subject to executive review, support and accountability of related policies and practices, comprising:

a) A written information security policy that complies with applicable laws and regulations, meets or exceeds applicable industry standards and that, at a minimum includes defined information security roles and responsibilities, and a formal and effective risk management program;
b) Completion of risk assessments of all systems processing Customer data;
c) Completion of internal audits to measure the effectiveness of controls;
d) Review of security incidents, including effective determination of root cause and corrective action;
e) A formal controls framework based on an external standard such as, SOC 2, ISO 27001, or other relevant frameworks; and
f) A process to document non-compliance with the Security Measures, and to identify and quantify the risks and mitigation plans. The mitigation plan must be approved by the Planview Chief Information Officer (CIO), the Planview Chief Information Security Officer (CISO), or authorized Planview employee, who can accept responsibility and accountability on behalf of Planview.

2. Facilities.
Planview will ensure that its third-party data center service providers facilities that store or process Customer data have sufficient measures in place to:

a) Protect from unauthorized physical access, damage, and interference using physical security controls which can include, but are not limited to, card key access, redundant power, redundant infrastructure, and solid wall construction for all exterior walls;
b) Limit and screen all entries and exits employing measures which can include, but are not limited to, on-site security guards, badge readers, electronic locks, and monitored closed circuit television (CCTV); and
c) Ensure systems processing Customer data are physically isolated from service areas that provide access points into and out of the premises

3. Employee Access, Screening and Controls.
Planview will have and maintain policies and practices that include, at a minimum, the following controls and safeguards applied to Planview employees ("Planview Representatives"):

a) Pursuant to applicable law, and subject to *Planview's Applicant Screening and Assessment Policy*, Planview will conduct appropriate background checks on all Planview Representatives who may have access to Customer data and withhold access to Customer data to any Planview Representative who has failed to pass such background investigation;
b) Access to data is governed by Planview's *Access Control Standard*. Controls are implemented to ensure that access granted to all Planview Representatives is based on least-privilege principles and that only those Planview Representatives with an actual need-to-know will have access to Customer data including, but not limited to, the use of a formal access management process for the request, review, approval, provisioning, and revocation
c) All Planview Representatives with access to Customer data will undergo adequate training in the care, protection, and handling of Customer data;
d) Planview will maintain a disciplinary policy and process to be enforced when Planview Representatives violate any Planview security or privacy policy or access Customer data without prior authorization;
e) Access to Planview source code must be limited and controlled to only permit access to authorized Planview Representatives;
f) A separation of duties process will be followed to prevent a single Planview Representative from controlling all key aspects of a critical transaction or business process related to Customer data or systems.

4. Authentication and Access Management.
Planview will provide strong authentication and access control to protect Customer data. Such strong authentication methods can include, but are not limited to, i) complex passwords at least eight characters long; ii) maximum 90-day password lifetime; iii) unique named user IDs; iv) session time out configuration, v) multi factor authentication.

5. Change Management.
Operating procedures must be documented and managed by a change control process. Planview will have and maintain written policies and procedures to review, test and approve (as appropriate) changes affecting Planview infrastructure and systems that process Customer data. Acceptance criteria for new information systems, upgrades, and new versions must be established and suitable tests of the system(s) carried out during development and prior to acceptance.

6. Business Continuity and Disaster Recovery.
Planview must have and maintain written business continuity and disaster recovery plans, which are tested/reviewed annually at a minimum.

7. Secure Data Deletion.
Planview will maintain a process for secure destruction and deletion of Customer data to ensure Customer data cannot be practicably read or reconstructed.

8. Vulnerability Management.
Planview will have and maintain the following vulnerability management processes for all devices used to connect to the Planview network and services:

a) Configuration scanning and remediation. Planview will align to industry best practices for build out, minimization of services and secure configuration for Planview applications;
b) Vulnerability scanning and remediation. A scanning and management system to scan Planview's network, systems, and applications for vulnerabilities. Planview will regularly scan for vulnerabilities and remediate detected vulnerabilities for components in production environments;
c) Secure coding. Planview must adhere to security development best practices for development and testing for all code, API's and applications deployed and implemented in support of services including, but not limited to, security testing or review for purchased or contracted development for use in the services; and
d) Identifying malicious threats. Planview will have and maintain solutions to identify and prevent malicious attackers or code from accessing or compromising Customer data or systems that process Customer data;
e) Exceptions to vulnerability management controls must be documented and mitigated based on defined business process controls.

9. Security Incident Response.
Planview will:

a) Maintain a security incident response plan, procedures, and means to respond in a manner consistent with industry standards;.
b) Notify the Customer without undue delay once Planview confirms any known data incident or malicious incursion involving Customer data or services utilized by Customer.
c) Cooperate with Customer in investigating and remediating the data incident and mitigating any further risk to the Customer Data, or risk to data subjects, as long as such cooperation does not interfere with Planview's own investigation and remediation of the incident.
d) Provide assistance to Customer as applicable making available to Customer relevant records, logs, files, data reporting and other materials required to comply with applicable law or regulation as reasonably required by Customer, subject to third party confidentiality restrictions; at Planview's sole cost and expense;
e) Preserve evidence where possible and cooperate with Customer and legal authorities as applicable during the investigation the incident or legal subpoena pertaining to Customer data, including accessibility of information for legal cases, preservation, availability, and monitoring.

10. Security Reviews.
Planview will undertake regular reviews of its Security Measures to ensure they remain effective and appropriate for protecting Customer data, and in compliance with applicable industry standards, laws, and regulations. Risks detected in regular reviews will be mitigated by Planview in a timely manner.

When implementing, reviewing, and updating its Security Measures and policies, Planview will consider:

f) Information available from the Planview's existing vulnerability, remediation, audits, or incident related activities;
g) The changing nature of threats, exploits and actual incidents relating to compromise of information hosted on connected computing platforms;
h) The confidential nature of Customer data and potential harm which could result from accidental, unauthorized, or unlawful processing, loss, access, or damage to, or destruction of, such information;
i) Available and emerging means of detecting malicious activities and rendering them less effective or ineffective;

j) The state of technological development and the cost of implementing such measures.

11. Encryption.
Planview has and will maintain: (i) established methods to encrypt Customer data in transit and at rest; and (ii) established methods to securely store passwords following industry standard practices.

12. Media Transfer.
Where physical media transfer is permitted, Planview must transport physical media containing Personal Information in sealed containers with documented chain of custody.

13. Network and Systems Security

a) Network segments connected to the internet must be protected by firewalls configured to protect all devices behind it and properly address known security concerns according to industry best practices. Firewalls must deny all network traffic other than traffic permitted for business functionality;
b) Planview must maintain the ability to reasonably detect a potential hostile attack;
c) Planview must have defined means of securing and maintaining the confidentiality, integrity and availability of system builds for compute and network devices on the network.
d) Development and production environments must be separated to reduce the risks of unauthorized access or changes to the operational system;
e) Validation checks must be incorporated into applications to detect corruption of information through processing errors or deliberate acts; and
f) Planview must use a trusted and reliable external time source to synchronize internal system clocks.

14. System and Logging Capabilities. Planview will maintain hardware, software, and/or procedural mechanisms that record, examine, and alert (upon detection of a security event) activity in information systems that process or access Customer data, including appropriate logs and automated reports. Logs must be retained to assist in investigations and access control monitoring, including, but not limited to, end user access and activities, and information security events.

15. Compliance Program Planview will maintain a compliance program that includes independent third-party audits and/or certifications, as SOC2 Type II report, ISO 27001 certificate,* or equivalent, and make available to Customer, upon written request, copies of the most up-to-date version of the third-party certifications or reports in relation to services purchased by the Customer;

16. Privacy by Design. Planview will incorporate privacy by design and privacy by default principles into processes, services, and systems at the earliest state and throughout the lifecycle of the processing activities.

* To verify to which Planview SaaS products ISO certifications and SOC 2 reports apply to, please visit www.planview.com/trust/compliance/