DATA PRIVACY, SECURITY AND PROCESSING AGREEMENT (“DPA”)

Customer (as defined in the Subscription Service Agreement/Order Form, the “Agreement”, hereinafter referred to as the “Customer”) and Planview (as defined in the SSA, hereinafter referred to as “Planview”) have agreed to the following terms and conditions regarding processing of Personal data and Personal Identifiable Information (“PII”) subject to the SSA

1. Subject matter and purpose of the DPA

The subject matter of Planview’s processing of PII is the execution of the services and tasks described in the SSA. This DPA establishes the instructions given by the Customer to Planview and the agreed processing activities by Planview on behalf of Customer when processing PII in connection with the tasks described in the SSA. Planview acts as a Processor and Customer acts as a Controller in relation to their own data, or (if applicable) both parties act as a Processor of their respective customers data.

The undertaking of the contractually agreed processing of PII shall be carried out in accordance with this DPA and the SSA within (i) a Member State of the European Union (EU), or (ii) within a Member State of the European Economic Area (EEA), or (iii) outside the EU/EEA, provided that the parties shall ensure compliance with the privacy regulations they are subject to and by appropriate measures. The provisions shall apply to any and all processing activities performed by Planview on behalf of the Customer, especially with regards to art. 28 of the EU 2016/679 (the “GDPR”), and in accordance with any other privacy regulation the parties are subject to.

2. How this DPA Applies

This DPA is subject to the terms of, and fully incorporated and made part of, the SSA, and shall replace any existing data processing addendum to the SSA unless otherwise explicitly stated herein. In the event of any conflict between this DPA and any other provision of the SSA with respect to PII, this DPA shall govern and apply.

3. Definitions

Any reference is made to further definitions set forth in any of the following regulations as applicable; Art. 4 of the GDPR, the California Privacy Rights Act, Cal. Civ. Code §§ 1798.100 et seq. (“CPRA”) as amended by the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. (the “CCPA”), unless otherwise stated herein.

4. Scope of Processing Activities

The processing activities comprise (i) identification of users; (ii) hosting and storing Customer data and project-related information in the Planview Product; and (iii) Support Services. Processing activities also comprise (iv) security and integrity operations; (as further described in Annex 3); (v) technological development and demonstration by Planview’s data science team; and (vi) Planview’s own administration and facilitation of the Services as established under the AOB clause of this DPA. The processing starts with the signing of this DPA and ends whenever the Customer terminates this DPA or the SSA.

5. Categories of Personal Data

The processing activities comprise in general the following categories/data types when Customer uses the Subscription Services: (i) contact details (e.g. name, address, e-mail address, contact details, local time zone information); (ii) employment details (e.g. company name, job title, grade, demographic and location data), (iii) IT and device systems information and traffic data (which may include user ID, IP address, and software usage pattern tracking information as cookies), (iv) data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, and support services, (v) any PII supplied by user to the Subscription Services.

CUSTOMER ACKNOWLEDGES PLANVIEW IS PROVIDING THE SUBSCRIPTION SERVICE WHEREAS THE CUSTOMER IS PROVIDING TO THE SUBSCRIPTION SERVICE WHATEVER DATA PREFERRED, INCLUDING PII.

6. Categories of Data Subjects

The Categories of Data Subjects comprise in general Customer employees, users invited to the Subscription Service by Customer, authorized agents/contractors, or other persons using or mentioned in the Subscription Service.

7. Technical and Organizational measures (ToM’s)

ToM’s to be taken shall guarantee a data protection level appropriate to the risk concerning confidentiality and integrity of the Customer and users PII, in accordance with availability and resilience of the IT systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons determine the actions taken into account.

Planview’s ToM’s are further specified in Annex 3 to this DPA. The ToM’s are subject to constant technical progress and further development. In this respect, it is permissible for Planview to implement alternative adequate measures. In so doing, the security of the defined measures must not be reduced. Planview shall periodically monitor the internal processes and the ToM’s to ensure that processing activities is in accordance with the requirements of applicable data protection law for the protection of the rights of the Data Subject.

8. Principles of the Processing Activities

The processing activities shall be performed at Customers instructions. Thereby, Planview may carry out, retain, rectify, erase or restrict the processing of PII only on documented instructions from the Customer, as described in this DPA, and/ or in accordance with the SSA, unless required to do so by any applicable law to which Planview is subject. In such a case, Planview shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Planview shall immediately inform Customer if, in its opinion, an instruction infringes any applicable law, including the GDPR and other European Union or member state data protection provisions. Insofar as a Data Subject contacts the Planview directly to exercise its rights as a registered, Planview will immediately instruct the Data Subject’s to submit the request with the Customer.

9. California Privacy

To the extent that Planview processes any Customer Personal Data relating to individuals who are California residents, Planview shall comply with the applicable provisions of the CCPA as amended by the CPRA. (collectively, the “California Privacy Laws”). For the purposes of the California Privacy Laws, the parties agree that Planview is a “Service Provider” in the performance of its obligations, not a “Third Party” or a “Contractor”, and that Customer is a “Business,” and that the transfer of Customer PII to Planview shall not be considered a “Sale” or “Sharing.”

To the extent required by the California Privacy Laws, Planview shall (a) provide the same level of privacy protection as is required by the California Privacy Laws; (b) grant Customer the right to take reasonable and appropriate steps to help ensure that Planview uses Customer PII in a manner consistent with Customer’s obligations under the California Privacy Laws; (c) notify Customer if Planview determines that it can no longer meet its obligations under the California Privacy Laws; and (d) grant Customer the right, upon reasonable notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Customer Personal Data.

As a Service Provider, Planview shall not (a) Sell or Share Customer PII; (b) retain, use, or disclose Customer PII for any purpose other than for the Business Purpose, including retaining, using, or disclosing Customer PII for a commercial purpose other than those Business Purposes, or as otherwise permitted by the CPRA; (c) retain, use, or disclose Customer PII outside of the direct business relationship between Planview and Customer; or (d) combine Customer PII that Planview receives from, or on behalf of, Customer with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that Planview may combine personal information to perform any Business Purpose as defined in the regulations adopted pursuant to paragraph (10) of subdivision (a) of Cal. Civ. Code § 1798.185, except as provided for in paragraph (6) of subdivision (e) of Cal. Civ. Code § 1798.140 and in regulations adopted by the California Privacy Protection Agency.

10. Other U.S. Data Protection Laws

To the extent that Planview processes any Customer PII relating to individuals who are “Consumers” as that term is defined in the Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 et seq. (“CPA”), the Connecticut Data Privacy Act, Public Act No. 22-15 (“CTDPA”), the Utah Consumer Privacy Act, Utah Code Ann. §§ 13-61-101 et seq. (“UCPA”), and the Virginia Consumer Data Protection Act, Va. Code Ann. §§59.1-575 et seq. (“VCDPA”) (collectively, the “Consumer Privacy Laws” or “CPL”), respectively, and upon the respective effective date of the applicable CPL, Planview shall comply with the CPL’s requirements.

11. Sub-Processors

Sub-processing activities comprise third-party services which relate directly to the provision of the principal Services of the SSA. Sub-processors are disposed globally. They are processing PII to provide the contracted services and identify events and activities between computers and agents (such as browsers, e.g., determining whether an action on a website is being performed by a human or a bot) or other identify patterns that may indicate malicious or fraudulent activity. Sub-processors are also used for security and operational services of information and event management systems (log data), for application infrastructure, and for email SMTP relay.

Planview may commission Sub-processors to fulfill the Services as Planview has a general authorization to engage Sub-processors for the purposes described above. Customer agrees to the commissioning of Sub-processors under condition of a contractual agreement is entered into between Planview and Sub-processor, stipulating the same requirements as Planview is subject to with regards to PII. Sub-processors are listed on Planview's Customer Success Center website. Notices of changes of sub-processors will be announced at least 30 days in advance on the Planview Status website which can be subscribed to for updates.

Planview is furthermore entitled to change existing Sub-processor with a new Sub-processor providing equivalent services when (a) Planview informs Customer of such change with appropriate advance notice; (b) The sub-processing is based on a contractual agreement, and (c) the change is not made solely for Planview's convenience, but for the necessity of provisioning the services unmodified. Customer may refuse an exchange or addition of Sub-processor in its absolute discretion resulting in the termination of processing activities, and dissolvement of the DPA and SSA.

Planview is fully liable to Customer for the performance of the Sub-processors processing activities related to Customers PII.

12. Quality Assurance and other duties of the Planview

12.1 Confidentiality. Planview entrusts only such employees who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work, to process Customer's PII. Planview shall only process PII by specific instructions from the Customer, which includes the powers granted in this DPA, unless required to do so by law.

12.2 Assistance and information. Planview shall cooperate, on request, with Customer to demonstrate and ensure compliance with a data protection supervisory authority or Data Subjects in performance of its statutory tasks.

12.3 Government Disclosure. Planview will notify Customer of any request for the disclosure of Customer PII by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or agency. In case Planview is prohibited by law from providing such notification, Planview shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable such communication. In case Planview does not consider the disclosure request to be legally binding, Planview shall not disclose any Customer data unless otherwise instructed by the Customer.

13. Data transfer scenarios and applicable transfer mechanisms

Customer is aware and understands that the global nature of the Subscription Services may comprise international transfers of PII, and both parties agree to adopt appropriate measures to ensure compliance with the international data transfer requirements under the applicable privacy regulations. This section 13 shall govern the relevant data transfer scenarios and the transfer mechanisms adopted. To the extent that the arrangement of the Services provided by Planview to Customer does not result in any of the scenarios established in this section, then the transfer mechanisms and the corresponding clause shall not apply.

13.1 Data transfers subject to the GDPR. Where Customer transfers PII subject to the GDPR to Planview or one of its affiliates located in a country which does not ensure an adequate level of data protection under the GDPR, parties shall adopt the Model Clauses set out in the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to third countries (hereinafter "EU Model Clauses") as a transfer mechanism. Where adopted between the parties, the EU Model Clauses shall follow Model Two (Controller to Processor) or (if applicable) Model Three (Processor to Processor) in the terms established herein by Annex 1, clause 1.

13.2 Onward data transfers to Sub-processors. Where, for the purposes of clause 11 of this DPA, Planview transfers Customer PII to a Sub-processor located in a country which does not ensure an adequate level of data protection under the applicable privacy and data protection law, Planview shall enter into the EU Model Clauses in Module Three (Processor to Processor) with the Sub-processors that access or otherwise process Customer PII outside of the EEA.

13.3 Data transfers subject to the Switzerland data protection law. Where Customer transfers PII subject to Swiss Privacy and Data protection law to Planview or any of its affiliates located in a country which does not ensure an adequate level of data protection under the applicable law, parties shall adopt Model Clauses as established in Annex 1, clause 2 as a transfer mechanism.

13.4 Data transfers subject to the UK GDPR. Where Customer transfers PII subject to the UK GDPR to Planview or any of its affiliates located in a country which does not ensure an adequate level of data protection under the applicable privacy and data protection law, parties shall adopt the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under Section 119A(1) Data Protection Act 2018, as updated, amended, replaced or superseded from time to time by the UK Government ("UK IDTA")as established in Annex 1, clause 3 as a transfer mechanism.

14. Privacy Contact

Planview has designated a Data Privacy Officer (DPO) authorized to ensure compliance with applicable privacy law, and to respond to inquiries concerning Planview's processing of PII. DPO can be contacted at privacy@planview.com

15. Data Breaches

Planview will notify Customer without undue delay after becoming aware of a data breach that may jeopardize the risk of confidentiality of Customers data and/or protection of PII. Planview will collaborate with Customer and fulfil all reasonable requests by Customer for updates, as long as it is not interfering with Planview's own work of investigating and limiting the effects of the breach. Planview will reply to questions Customer may have without undue delay to the extent possible and as frequently and reasonably necessary until the breach has been rectified.

16. Supervisory powers of the Customer

Planview undertakes to give Customer necessary information on request and, in particular, to demonstrate the execution of the ToM's. Evidence of such measures, which concern not only the specific DPA, may be provided by a suitable certification by IT-security or data protection auditing body. Customer shall utilize Planview's external assessment reports (ISO 27001, 27701 and/or SOC2 Type 2) for auditing, inspection and questionnaire purposes. If questions remain or additional clarification is needed, the parties will determine a mutually agreeable venue for review of any outstanding items, such as additional inspections, or to have them carried out by an auditor (under the condition such auditor is bound by a non-disclosure agreement), to be designated in each individual case upon thirty (30) days written notice to Planview (unless a shorter period is required to meet a legal requirement or request by a Supervisory Authority or government authority), and shall be conducted in a manner that minimizes any disruption of Planview's provision of the Services and other normal operations.

If Customer requires Planview to respond to privacy and security questionnaires or assessments that are not capable of being readily completed by referencing existing Planview policies and procedures, or the summary assessment results referenced herein, then Planview will have the right to charge Customer for the time of its personnel in connection therewith.

17. Termination

When the Processing activities ends, Planview shall terminate the Customers Subscription Service's account in the Planview Application and delete any access to the system by Customer and users, and if applicable, at the choice of the Customer, return or destroy all documents, processing and utilization results, and data sets related to the SSA that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. All Customer data is deleted at the earliest convenience after contract termination if Customer don't specify a specific time frame. Written assurance of deletion or destruction of any Customer information will be provided by request to DPO.

18. Miscellaneous

This DPA is governed by the law which governs the SSA and any dispute between the parties is to be handled as set out in the SSA.

Customer may terminate this DPA and/or the Agreement, in the event: a) Planview is in substantial breach of any representations or warranties given by it under this DPA and fails to cure such breach with ninety (90) days' following receipt of notice from Customer; or b) a Supervisory Authority or other regulatory authority or other tribunal or court finds that there has been a breach of any relevant laws in that jurisdiction by virtue of Planview's or Customer's processing of the PII.

AOB

Planview's processing of PII for the purpose of Planview's own administration and facilitation of the Subscription Services comprise the following categories of data:

- Customer History (for Planview's internal CRM system)
- Contract Billing and Payments Data (for Planview's internal CRM system)
- Disclosed Information (from third parties, e.g., Credit Reference Agencies or from Public Directories, for internal CRM system)
- User behavioral data (for measuring the use of the service and support)
- User performance data (for measuring the use of service to tailor better features and support)

Planview is a Controller for these processing activities. Planview is processing the data for legal obligations or legitimate interest. Processing activities may comprise third party disclosure to Processors. Additional information regarding Planview's processing of PII can be found in the Privacy Statement on the Planview website.

IN WITNESS WHEREOF, the parties' authorized signatories have duly executed this Agreement as of the Effective Date.

[“PLANVIEW ENTITY NAME”] **[“CUSTOMER ENTITY NAME”]**

Signature:	**Signature:**
Printed Name:	**Printed Name:**
Title:	**Title:**
Date:	**Date:**

ANNEX 1

Standard Contractual Clauses Terms

1. EEA Model Clauses

For the purpose of clause 13.1 of this DPA, the parties agree that the model clauses resulting from the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries (hereinafter "EU Model Clauses"), Module Two (Controller to Processor) and Module Three (Processor to Processor) shall be incorporated herein by reference. Customer is the data exporter and Planview is the data importer, and the Parties agree to the following:

1.1 Docking clause
The option under clause 7 shall not apply.

1.2 Documentation and compliance
The parties agree that the documentation and compliance requirements described in clause 8.9 of the EU Model Clauses shall be carried out in accordance with clause 14 of this DPA.

1.3 General authorization for use of sub-processors
For the purpose of clause 9 EU Model Clauses, Option 2 shall apply. For the purpose of clause 9 (a) EU Model Clauses, Planview has general authorization to engage sub-processors in accordance with clause 9 of this DPA. Planview lists the sub-processors on Planview's Customer Success Center website and any intended change to the list will be communicated to Customer at least 30 days in advance. Where Planview enters into EU Model Clauses, Module 3 (Processor to Processor) with its sub-processors, Customer grants Planview authority to provide general authorization on Customer's behalf for the engagement of sub-processors by sub-processors previously engaged in the provision of the service and also approval authority for the addition or replacement of any of such sub-processors.

1.4 New sub-processor notification and objection right
For the purpose of clause 9(a) EU Model Clauses, Customer agrees that notices of changes of sub-processors will be announced on the Planview Status website which can be subscribed to for updates as established in clause 9 of this DPA. Both parties agree that objections to an exchange or addition of sub-processor shall also be governed by clause 9 of this DPA.

1.5 Redress
The option under clause 11 shall not apply.

1.6 Supervision
For the purpose of clause 13 EU Model Clauses, the Swedish Authority for Privacy Protection (IMY) shall be the authority indicated in Annex I.C.

1.7 Notification of the data importer in case of access by public authorities
For the purposes of clause 15(1)(a) EU Model Clauses, Planview shall exclusively notify Customer (and not the Data Subjects) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

1.8 Governing Law
For the purposes of clause 17, Option 1 shall apply, and the governing law shall be the laws of Sweden.

1.9 Choice of forum and jurisdiction
The parties agree that, for the purposes of clause 18 EU Model Clauses, the applicable courts shall be the courts of Sweden.

1.10 Description of the transfer and technical and organizational measures
The information described in Annex 2 and 3 of this DPA shall be incorporated into Annex 1 and 2 of the EU Model Clauses.

2. Swiss Law

For the purpose of clause 13.3 of this DPA, the parties agree that the EU Model Clauses, Module 2 (Controller to Processor) and EU Model Clauses, Model Three (Processor to Processor) shall apply in the terms established in clause 1 of this Annex (1) with the necessary adaptations described in the following clauses. The Model Clauses shall also apply to the transfers of information relating to an identified or identifiable legal entity where such information is protected in similar terms as PII under Swiss Data Protection Law until such laws are amended to no longer cover legal entities. Customer shall be the data exporter and Planview the data importer, and the Parties agree to the following adaptations:

2.1 Supervision
For the purpose of clause 13 EU Model Clauses, the Swiss Federal Data Protection and Information Commissioner shall be the authority indicated in Annex I.C.

2.2 Applicable law for contractual claims
For the purpose of clause 17 EU Model Clauses, Swiss law shall apply.

2.3 Place of jurisdiction for actions between the parties
Pursuant to clause 18 (b), Sweden shall be the place of jurisdiction for actions between the parties.

2.4 Place of jurisdiction for actions brought by data subjects
The term 'member state' shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18 (c) EU Model Clauses.

2.5 References to the GDPR
Any reference to the GDPR shall be understood as a reference to the Swiss Federal Data Protection Act.

3. UK Law

For the purpose of clause 13.4 of this DPA, the parties agree that, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under Section 119A(1) Data Protection Act 2018, as updated, amended, replaced or superseded from time to time by the UK Government ("UK IDTA") shall be incorporated herein by reference. Customer shall be the data exporter and Planview the data importer, and the Parties agree to the following adaptations:

Part 1
3.1 Table 1

(a) The Start Date is the date on the applicable order form.
(b) The Exporter is the Customer, as established in Section 1 Annex 2. The Importer is the Planview, as established in Section 1 Annex 2
(c) The Exporter's Key Contact is the one established in Section 1 Annex 2.
(d) The Importer's Key Contact is Cajsa Weibring, Associate General Counsel & DPO, privacy@planview.com.

3.2 Table 2
The Parties choose the EU Model Clauses, including the Appendix Information and with only the following modules, clauses or optional provisions of the EU Model Clauses brought into effect for the purposes of this IDTA:

(a) Module in operation – Two and Three
(b) Clause 7 – See Section 1.1 above.
(c) Clause 9 – See Section 1.3 above.
(d) Clause 11 – See Section 1.5 above.

3.3 Table 3

(a) Annex 1A: See Annex 2.
(b) Annex 1B: See Annex 2.

(c) Annex II: See Annex 3.
(d) Annex III: N/A.

3.4 Table 4

The Importer and Exporter may end this IDTA.

Part 2

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

4. Conflict

The Model Clauses shall be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Model Clauses, the Model Clauses shall prevail.

ANNEX 2

Description of the Transfer

1. List of parties

Data exporter(s):

Name: As established in the applicable Agreement

Address: As established in the applicable Agreement

Contact person's name, position and contact details: The contact details associated with Customer's Planview account or as otherwise specified in the Agreement.

Activities relevant to the data transferred under these Clauses: Contracting the Services as further defined in the Agreement

Signature and date: As established in the applicable Agreement

Role (controller/processor): Controller (Module Two) and/or Processor (Module Three)

Data importer(s):

Name: Planview entity established in the applicable Agreement

Address: As established in the applicable Agreement

Contact person's name, position and contact details: Cajsa Weibring, Associate General Counsel & Data Privacy Officer, privacy@planview.com

Activities relevant to the data transferred under these Clauses: Execution of Services as further defined in the Agreement

Signature and date: As established in the applicable Agreement

Role (controller/processor): Processor

2. Categories of data subjects whose personal data is transferred

Employees of the Customer, consultants and other agents as further described in the SSA and related DPA (if any).

3. Categories of personal data transferred

(i) contact details (e.g. name, address, e-mail address, contact details, local time zone information); (ii) employment details (e.g. company name, job title, grade, demographic and location data), (iii) IT and device systems information and traffic data (which may include user ID, IP address, and software usage pattern tracking information as cookies), (iv) data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services, (v) any personal data supplied by users of the Subscription Services.

4. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

5. The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

On a continuous basis when the Service is used.

6. Nature of the processing

The processing activities comprise (i) identification of users; (ii) hosting and storing Customer data and project-related information in the Planview Product; and (iii) Support Services. Processing activities also comprise (iv) security and integrity operations; (as further described in Annex 3); and, (v) technological development and demonstration by Planview's data science team.

7. Purpose(s) of the data transfer and further processing

The purpose of data transfers of PII is to execute and fulfill the commitments of the SSA with Customer.

8. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the SSA.

9. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The purpose of transfer of personal data is to execute and fulfill the commitments of the SSA. Detailed information the different processing activities subject to the transfers are specified on Planview's Customer Success Center website of Sub-processors https://success.planview.com/trust/Planview_Sub-Processors

ANNEX 3

Technical and Organizational Measures

Technical and organizational measures including technical and organizational measures to ensure the security of the data.
Description of the technical and organisational measures implemented by the data importer(s) (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/