Last revised: 1/20/2026

PROJECTMANAGER.COM, INC.
CUSTOMER DATA SECURITY EXHIBIT

The obligations in this Customer Data Security Exhibit ("**Exhibit**") provide further details about and are a part of ProjectManager's security obligations for Customer Data under the ProjectManager Terms of Service governing Customer's access to and use of the ProjectManager project management platform (the "**Agreement**"). Capitalized terms used but not otherwise defined in this Exhibit will have the meanings ascribed to them in the Agreement.[1] This Exhibit is incorporated into and made subject to the Agreement.

1. Measures of pseudonymization and encryption of Customer Data

All Customer Data will be encrypted at rest and when transmitted by ProjectManager or the ProjectManager cloud based project management platform (the "**ProjectManager Platform**") across any public network, using industry-standard measures in conformance with ProjectManager's then current "ISMS Standards" (defined below). ProjectManager will encrypt backups containing Customer Data using industry-standard measures in conformance with the ISMS Standards. Given the nature of ProjectManager's cloud services (the "**Services**"), ProjectManager does not pseudonymize Customer Data.

2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

a) Background checks: ProjectManager will not permit its personnel to access Customer Data unless they have passed a criminal and employment background check.

b) Ongoing confidentiality: ProjectManager will ensure that its personnel are subject to obligations of confidentiality with respect to Customer Data.

c) Security training: At least on an annual basis, ProjectManager will require all ProjectManager employees ("**ProjectManager Personnel**") with access to Customer Data, to the extent applicable to the respective roles and responsibilities of the ProjectManager Personnel, to complete training on ProjectManager's information security policies relevant to Customer Data.

d) Security certification and attestation: ProjectManager is and will remain in compliance with its SOC-2 statement (the "**ISMS Standards**") throughout the Subscription Term. (ProjectManager's SOC-2 audit and certification is scheduled for completion before the end of 2023.) ProjectManager will cause its independent ISMS Standards certification auditors to verify the adequacy of the controls that ProjectManager applies to the Services at least annually. ProjectManager will provide Customer with copies of its ISMS Standards certifications applicable to ProjectManager's provision of Services, upon request by Customer. For Annual Plan Customers, ProjectManager will in addition provide such information regarding its information security systems, policies and procedures as Customer may reasonably request relating to Customer's due diligence and oversight obligations under applicable laws and regulations.

3. Measures for ensuring the ability to restore the availability and access to Customer Data in a timely manner in the event of a Security Breach

a) Incident Management: ProjectManager has in place an incident response plan that includes procedures to be followed in the event of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data in ProjectManager's possession or under

[1] The ProjectManager Terms of Service are available for review at https://ProjectManager.com/legal .

its control (a "**Security Breach**"). The procedures in ProjectManager's security incident response plan include:

i) Roles and responsibilities: formation of an internal incident response team with a response leader;

ii) Investigation: assessing the risk the incident poses and determining who may be affected;

iii) Communication: internal reporting as well as a notification process in the event of a Security Breach;

iv) Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and

v) Audit: conducting and documenting a root cause analysis and remediation plan.

b) Notification, management and remediation of Security Breaches: ProjectManager will notify Customer of any Security Breach within 48 hours of ProjectManager's confirmation of the nature and extent of the same or when required by applicable law, whichever is earlier. Each party will reasonably cooperate with the other with respect to the investigation and resolution of any Security Breach including, in the case of ProjectManager, prompt provision of the following, to the extent then known to ProjectManager: (i) the possible cause and consequences of the Security Breach; (ii) the categories of Customer Data involved; (iii) a summary of the possible consequences for the relevant Users; (iv) a summary of the unauthorized recipients of the Customer Data; and (v) the measures taken by ProjectManager to mitigate any damage. Upon confirmation of any vulnerability or breach of ProjectManager's security affecting Customer Data in ProjectManager's custody and control, ProjectManager will modify its processes and security program as necessary to mitigate the effects of the vulnerability or breach upon such Customer Data. Insofar as the Security Breach relates to Customer, and except to the extent required otherwise by applicable law, Customer will have approval rights on notifying its Users and any third-party regulatory authority of the Security Breach. All security breach or security compromise notifications will be to Customer's technical support contact via email or ProjectManager's support platform.

c) Disaster recovery and business continuity: During any period in which Customer is subscribed to the Services, ProjectManager will comply with its then current applicable Business Continuity and Disaster Recovery Plans. ProjectManager will test such plans at least once a year. ProjectManager will provide Customer with summaries of such plans and test results upon written request. ProjectManager may not modify such plans to provide materially less protection to Customer without Customer's prior written consent, which may not be unreasonably conditioned or withheld.

4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of processing

a) Access controls: ProjectManager will:

i) Follow the principles of least privilege through a role-based access model when granting ProjectManager Personnel access to Customer Data. Except in the case of an emergency, ProjectManager personnel will not access Customer Data unless Customer has approved such access.

ii) Limit access to Customer Data to ProjectManager Personnel with a legitimate need to access Customer Data to provide the Services in accordance with the Agreement.

iii) Periodically review ProjectManager Personnel's access to Customer Data.

iv) Promptly terminate an ProjectManager Personnel's access to Customer Data if such individual's access is no longer required.

b) Network controls: ProjectManager will implement and maintain measures designed to secure, control, and manage access to ProjectManager's networks and systems used to provide the ProjectManager Platform, including (i) firewalls and other technology and authentication controls, and (ii) intrusion detection or prevention systems to monitor all such networks. ProjectManager will maintain incident response and recovery plans to respond to potential security threats to such networks and systems.

c) Vulnerability management and patch management: ProjectManager will implement and maintain a vulnerability management program designed to identify and remediate vulnerabilities affecting networks

and production systems for the ProjectManager Platform in the form made available by ProjectManager to Customer. Such program will include:

i) Annual penetration tests conducted by an independent third party on the ProjectManager Platform, and more frequent tests conducted by an ProjectManager internal red team. Upon Customer's reasonable written request, ProjectManager will provide Customer an executive summary of the independent third party test results, no more than annually. Customer will treat such information as ProjectManager's confidential information in accordance with the confidentiality provisions of the Agreement; and

ii) Routine vulnerability scans on all infrastructure components of ProjectManager's service environment for the ProjectManager Platform and applications used by ProjectManager to access Customer Data.

If vulnerabilities are detected from such tests and scans, ProjectManager will remediate and apply applicable and necessary updates or patches as soon as reasonably practicable and in accordance with its documented vulnerability remediation and response policy. Such policy will include factors for determining the scheduling of updates or patches, including criticality of the ProjectManager systems being updated, expected time taken to install the updates (and requirements for service outages to users, if any), degree of risk associated with any vulnerabilities that are closed by the updates, coordination of the updating of related components of the ProjectManager infrastructure, and dependencies between updates.

d) ProjectManager Platform Development Practices: With respect to the development of the ProjectManager Platform, ProjectManager will maintain and follow a written software development life cycle program based on the Open Web Application Security Project (OWASP) Top 10 standards. ProjectManager's security team provides ProjectManager Personnel who are responsible for secure application design, development, configuration, testing, and deployment appropriate (based on role) training regarding ProjectManager's secure application development practices.

e) Malware controls: ProjectManager will install and maintain reasonable and current controls designed to protect ProjectManager networks, systems, and devices used by ProjectManager to access Customer Data from malware and unauthorized software.

5. Measures of user identification and authorization

a) Network controls: ProjectManager will implement and maintain measures designed to secure, control, and manage access to ProjectManager's networks and systems used to provide the ProjectManager Platform, including (i) firewalls and other technology and authentication controls, and (ii) intrusion detection or prevention systems to monitor all such networks.

b) Intrusion detection and performance assurance: ProjectManager monitors the ProjectManager Platform generally for unauthorized intrusions using traffic and activity-based monitoring systems.

6. Measures for the protection of data during transmission

a) Encryption: As specified in Section 1 above.

7. Measures for the protection of data during storage

a) Encryption: As specified in Section 1 above.

b) Data segregation: ProjectManager will keep Customer Data logically segregated from data belonging to ProjectManager's other customers and will implement measures and controls designed to ensure that Customer Data is not accessible by ProjectManager's other customers.

8. Measures for ensuring physical security of locations at which Customer Data are processed

a) Data center security: ProjectManager uses data centers operated by third parties, for example Amazon Web Services, to provide the Services and requires such third parties to maintain controls that provide reasonable assurance that access to physical servers at the data center is limited to properly-authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. These controls include:

   i) Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;

   ii) Camera surveillance systems at critical internal and external entry points to the data center;

   iii) Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and

   iv) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

9. Measures for ensuring events logging

a) Logging: ProjectManager will regularly log and monitor the details of all ProjectManager Personnel's access to Customer Data on networks, systems, and devices that are used to provide the Subscription Services. Such logs will be maintained by ProjectManager in accordance with its data retention policies.

10. Measures for ensuring system configuration, including default configuration

a) Change and Configuration Management: ProjectManager maintains policies and procedures for managing changes to ProjectManager's production systems, applications, and databases which process Customer Data. Such policies and procedures include:

   i) A process for documenting, testing and approving the promotion of changes into production;

   ii) A security patching process that requires patching systems in a timely manner based on a risk analysis; and

   iii) A process for ProjectManager to perform security assessments of changes into production.

11. Measures for internal IT and IT security governance and management

a) Information security measures: ProjectManager will implement and maintain commercially reasonable technical and organizational security measures designed to meet the following objectives: (i) ensure the security and confidentiality of Customer Data in the custody and under the control of ProjectManager; (ii) protect against any anticipated threats or hazards to the security or integrity of such Customer Data; (iii) protect against unauthorized access to or use of such Customer Data; and (iv) ensure that ProjectManager's return or disposal of such Customer Data is performed in a manner consistent with ProjectManager's obligations under items (i)-(iii) above. Customer is solely responsible for consequences of Customer's decision not to adopt updates or best practices that ProjectManager makes available to Customer.

b) Modifications: ProjectManager may modify its security controls and processes from time to time, so long as, taking into account updates to industry standards and best practices in ProjectManager's sector, such modifications: (a) do not materially reduce the overall level of protection afforded by ProjectManager to Customer Data, and (b) are consistent with ProjectManager's then current SOC-2 statement.

c) Oversight: ProjectManager will designate one or more employees to maintain ProjectManager's information security program, and ProjectManager's senior management and leadership team will review and approve any material changes to the information security program. ProjectManager will review the information security program at least annually or upon a material change in ProjectManager's business practices.

12. Measures for certification/assurance of processes and products

a) Security certifications and attestations: As specified in Section 2(d) above.

13. Measures for ensuring data minimization

a) Measures for ensuring data minimization: With the exception of some form of user or device identification and password or equivalent, customers control the nature and scope of the Customer Data that they choose to input into the ProjectManager Platform.

14. Measures for ensuring data quality

a) Measures for ensuring data quality: Customer is solely responsible for the accuracy, quality and integrity of the Customer Data that Customer or its Users input into the ProjectManager Platform.

15. Measures for ensuring limited data retention

a) Retrieval of Customer Data: During the Subscription Term, Customers may export Customer Data at any time using features and functionality of the ProjectManager Platform. If Customer is unable to do so using the functionality of the ProjectManager Platform, then ProjectManager will reasonably assist Customer with the export.

a) Deletion during and after termination or expiration of the Subscription Term: Until the expiration or termination of the Agreement or Sales Order as applicable (the "Data Access Period") Customer may export or delete Customer Data from the ProjectManager Platform. ProjectManager will reasonably assist Customer in such efforts where Customer is unable to do so using the functionality of the ProjectManager Platform. During the Subscription Term and the Data Access Period, Customer may add, change or delete Customer Data stored on the ProjectManager Platform. Within 180 days following the earlier of (i) the end of the Data Access Period or (ii) Customer's notification that it no longer requires retention of Customer Data, ProjectManager will delete any Customer Data remaining on the ProjectManager Platform, subject to retention of backup copies for up to 30 days; such backup copies will continue to be subject to this Exhibit until deleted.

b) Secure deletion: Customer Data in ProjectManager's possession or under its control will be deleted using techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization"). Following expiration or termination of the Agreement or Sales Order as applicable, ProjectManager will certify the deletion of Customer Data in accordance with paragraph (a) above, upon Customer's written request.

16. Measures for ensuring accountability

a) Liability for acts, errors and omissions of sub-processors: ProjectManager will require its sub-processors to comply with terms that are substantially no less protective of Customer Data than those imposed on ProjectManager in the Agreement (to the extent applicable to the services provided by the sub-processor). ProjectManager will be liable for any breach of its obligations under the Agreement that is caused by an act, error or omission of a sub-processor.

b) Disciplinary policy: ProjectManager will maintain and enforce a disciplinary policy for violations of ProjectManager's information security program by ProjectManager personnel.

17. Measures for allowing data portability and ensuring erasure

a) Storage on portable devices: ProjectManager will not store any Customer Data on portable devices or removable media, including laptops, smartphones and tablets, without Customer's prior written approval.