1Password Privileged Access Product-Specific Terms

Customer's use of 1Password Privileged Access is subject to these Product-Specific Terms and the governing agreement between Customer and 1Password referencing these terms (the "**Agreement**").[1] Terms not expressly defined herein have the meaning given in the Agreement.

1. **Updated Definitions**

The following definitions apply to Customer's use of 1Password Privileged Access and are added to the Agreement:

(a) "**Access Flow"** means a workflow configured by Customer that governs requests for, approvals of, provisioning of, modification of, or revocation of access permissions within Connected Systems.
(b) "**Access Request**" means a user-initiated request, submitted through the Services or an integrated messaging platform, to obtain access to resources within a Connected System in accordance with a configured Access Flow.
(c) "**Connected System**" means any third-party cloud service, infrastructure, application, identity provider, database, development platform, collaboration platform, or other system integrated by Customer with the Services.
(d) "**Connector**" means software or other integration technology made available by 1Password and deployed within Customer's environment to enable communication between Connected Systems and the Services.
(e) "**Ephemeral Credential**" means a scoped credential (including a database password, API key, or similar access artifact) generated by the Services on demand in connection with an approved Access Request, surfaced to the requesting user for the duration of the approved access period, and not retained or stored by 1Password following generation.
(f) "**Service Credential**" means an administrative or integration credential required by the Services to authenticate with and perform actions within a Connected System on Customer's behalf, which is retrieved by the Services from Customer's designated secrets management vault (which may include 1Password or a third-party secrets management service) and is not stored by 1Password.

2. **Connector License**

Subject to the Agreement, 1Password grants Customer a limited, non-exclusive, non-transferable right during the Term to install, execute, and use the Connector solely as necessary to enable Customer's

---

[1] *1Password reserves the right to update or change any portion of these Product-Specific Terms at any time. We will provide you with reasonable advance notice of changes to these Product-Specific Terms that materially adversely affect your use of the Services or your rights under these Product-Specific Terms by sending an email to the primary email address in our records or by similar means. However, 1Password may make changes that materially adversely affect your use of the Services or your rights under these Product-Specific Terms at any time and with immediate effect (i) for legal, regulatory, fraud and abuse prevention, or security reasons; or (ii) to restrict products or activities that we deem unsafe, inappropriate, or offensive. Unless we indicate otherwise in our notice (if applicable), any changes to these Product-Specific Terms will be effective immediately upon posting of such updated terms in 1Password's legal center. Your continued access to or use of the Services after we provide such notice, if applicable, or after we post such updated terms, constitutes your acceptance of the changes and consent to be bound by these Product-Specific Terms as amended. If you do not agree to the amended Product-Specific Terms, you must stop accessing and using the Services.*

authorized use of the Services. Customer will not install or deploy the Connector on any device or system for which Customer does not have proper authority to do so.

3. **Connected Systems and Access Management**

Customer authorizes 1Password to access, communicate with, and perform actions within Connected Systems as necessary to provide the Services, including provisioning, modifying, approving, denying, revoking, or otherwise managing access permissions, and generating and surfacing Ephemeral Credentials to authorized users, in accordance with Customer's configured Access Flows and other instructions submitted through the Services.

Customer represents and warrants that it has obtained all rights, permissions, and authorizations necessary for 1Password to access Connected Systems and perform such actions.

4. **Customer Responsibilities**

Customer is solely responsible for:

(a) configuring and maintaining its Access Flows, approval workflows, access policies, roles, permissions, and other authorization settings;
(b) maintaining the security of Connected Systems, administrative credentials, and integration credentials;
(c) ensuring that all actions performed by the Services accurately reflect Customer's intended authorization policies;
(d) complying with all terms applicable to Connected Systems and any third-party APIs or services integrated with the Services; and
(e) complying with all applicable employment, privacy, and data protection laws in connection with its use of the Services to manage end-user access, including obtaining any required notices or consents from individuals whose access is managed through the Services.

Customer will defend, indemnify, and hold harmless 1Password and its affiliates, officers, employees, and agents from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or related to: (a) 1Password's access to and actions performed within Connected Systems in accordance with Customer's configured Access Flows and instructions; (b) Customer's misconfiguration of Access Flows, access policies, roles, or permissions; or (c) Customer's failure to obtain necessary rights, permissions, or consents for 1Password to access and act within Connected Systems.

5. **Third-Party Integrations and Automated Access Actions**

The Services interoperate with Connected Systems and third-party APIs that are not controlled by 1Password. Customer acknowledges that the availability and functionality of such integrations depend upon the continued availability of those third-party services and applicable APIs. 1Password is not responsible for the availability, performance, or functionality of Connected Systems or third-party services.

The Services are designed to automatically provision and revoke access permissions in Connected Systems in accordance with Customer's configured Access Flows, including any time-bound access durations configured by Customer. Customer acknowledges that the Services' ability to perform automated revocation of access is dependent on the continued availability, proper configuration, and functionality of the applicable Connected System and its APIs. 1Password is not responsible for any

failure to revoke access that results from the unavailability or misconfiguration of a Connected System, changes to a Connected System's APIs, or actions by Customer or third parties that interfere with the Services' ability to communicate with a Connected System. Customer is responsible for monitoring the status of access grants and independently verifying that access has been revoked as intended.

6. **Credential Handling**

Depending on the Connected System and Customer's configured Access Flows, the Services may manage access through one or both of the following mechanisms: (a) modifying identity and access management roles, permissions, or group memberships within a Connected System without generating credentials to end users; or (b) generating and surfacing Ephemeral Credentials to authorized users as part of fulfilling an approved Access Request.
Ephemeral Credentials are not retained or stored by 1Password following generation and surfacing to the end user. 1Password is not responsible for the security or use of Ephemeral Credentials after they have been surfaced to an end user. The ability to revoke or invalidate an Ephemeral Credential after generation is dependent on the applicable Connected System's capability to invalidate such credentials and is not guaranteed by 1Password.

The Services require Service Credentials to authenticate with and manage Connected Systems on Customer's behalf. Service Credentials are not stored by 1Password; they are retrieved by the Services from Customer's designated secrets management vault (which may include 1Password or a third-party secrets management service) as needed. Customer is solely responsible for maintaining, securing, and authorizing the Services to access Service Credentials in Customer's designated vault.

If Customer uses 1Password Privileged Access in conjunction with another 1Password credential management product, the applicable product-specific terms for that product govern with respect to credentials owned or managed by that product.

7. **Customer Data**

For purposes of 1Password Privileged Access, Customer Data also includes metadata, identities, permissions, Access Requests, approval records, audit logs, and other information obtained from or generated through Customer's Connected Systems in connection with Customer's use of the Services.

8. **Audit Logs and Compliance**

The Services generate audit logs of Access Requests, approvals, denials, provisioning events, and revocations. Customer is solely responsible for:

(a) exporting and retaining audit logs in accordance with Customer's applicable legal, regulatory, and contractual obligations;
(b) configuring any third-party security information and event management (SIEM), logging, or compliance systems to receive log exports from the Services; and
(c) complying with any record-retention requirements imposed by applicable law or regulation.

1Password does not represent that the Services satisfy any specific regulatory record-retention requirements. Upon expiration or termination of the Agreement, 1Password may delete Customer Data, including audit logs, in accordance with the Agreement.

9. **AI-Powered Features**

1Password Privileged Access may include features that use artificial intelligence or machine learning, including access recommendations, anomaly detection, and automated policy suggestions. Customer's use of any such AI-powered features is subject to any AI-specific terms incorporated into the Agreement. AI-powered features are provided to assist Customer's access management decisions; all final access authorization decisions remain the sole responsibility of Customer. 1Password does not warrant that AI-generated recommendations are accurate, complete, or appropriate for Customer's specific environment or compliance requirements.

10. **Termination Effects**

Upon expiration or termination of the Agreement with respect to 1Password Privileged Access, the following apply:

(a) all Connector licenses granted hereunder will immediately terminate and Customer shall promptly remove or disable all Connectors from its environment;
(b) 1Password will cease performing access management actions within Connected Systems; and
(c) any active access grants provisioned through the Services that have not yet expired or been revoked will not be automatically revoked by 1Password.

Customer is solely responsible for independently revoking any access permissions in Connected Systems that were provisioned through the Services prior to or following termination. Customer should export any Customer Data, including audit logs, from the Services prior to termination.

Last updated: *July 31, 2026*