

Password Manager - Schedule CS-10

Effective Date: October 14, 2025 | Supersedes prior versions.

Service Summary

Service Provider shall provide Password Manager services to improve credential security and reduce risks from weak or reused passwords. Password Manager services enable encrypted storage, sharing, and management of passwords and other credentials within a centralized, cloud-based platform. These services strengthen Client's overall security posture but do not guarantee the prevention of account compromise.

Scope of Services

- Provisioning and management of a password manager platform for Covered Users.
- Deployment of administrative policies, including password strength requirements, secure sharing, and multi-factor authentication for vault access.
- Monitoring of license usage and platform activity through administrative dashboards.
- Assistance with end-user onboarding, enrollment, and training on basic usage.
- Documentation of enrollment and support activities in Service Provider's ticketing platform.

Exclusions

- Responsibility for end-user actions, including failure to enroll, weak or reused master passwords, insecure credential sharing, or storage of passwords outside the platform.
- Protection against account compromise due to factors outside the platform (e.g., phishing, credential harvesting, endpoint malware).
- Guarantee of availability or uptime of the third-party password management platform.
- Recovery of credentials if the Client loses master access or fails to maintain recovery options.
- Support for non-licensed users or third-party password management tools not under Service Provider management.

Client Responsibilities

- Ensure all designated users enroll in the password manager and maintain secure master passwords.
- Promptly notify Service Provider of user changes (additions, terminations) requiring license reassignment.
- Follow Service Provider's policies for password sharing, vault access, and MFA enforcement.
- Retain responsibility for accounts, systems, or credentials not stored in or managed through the password manager.

General Terms

- Password Manager services are provided as a risk-reduction control. They improve credential management but cannot guarantee protection against all unauthorized access attempts. Even the most advanced credential management systems remain subject to bypass or compromise.
- Client acknowledges that the Password Manager is one element of a layered security strategy. Service Provider strongly recommends implementing complementary safeguards – such as endpoint detection and response (e.g., Adlumin XDR), multi-factor authentication, conditional access policies in Microsoft 365/Intune/Entra ID, DNS filtering, email security, dark web monitoring, and user training – to achieve stronger overall resilience.
- All response times for service requests related to the Password Manager are governed by the Service Level Objectives in Schedule A of the Master Service Agreement.
- Fees for this Schedule are billed in accordance with the Payment Terms of the Master Service Agreement. Required platform licensing is included in Service Provider's standard service fees unless otherwise specified. Additional costs (e.g., optional hardware, custom configurations, or third-party integrations outside standard service) may apply and will be billed separately.