DeepFabric

DEEPFABRIC SECURITY MEASURES

Version: 2026-11-10

These Security Measures are incorporated into the DeepFabric Master Service Agreement identified in the applicable Order Form and establish the contractual security safeguards described in Section 6.1 of that MSA.

1. Purpose and Scope.

These Security Measures describe Provider's baseline security measures applicable to the Services and Customer Data in Provider's possession or control. Provider maintains commercially reasonable administrative, technical, and organizational safeguards designed to protect Customer Data in Provider's possession or control against accidental or unlawful loss, unauthorized access, unauthorized disclosure, unauthorized alteration, and destruction.

These Security Measures apply only to Customer Data in Provider's possession or control in connection with the Services. These Security Measures do not apply to Customer systems, Customer-selected Third-Party Services, Customer configurations, Customer credentials, Customer networks, Customer-managed integrations, or any data, systems, tools, or environments not controlled by Provider. These Security Measures do not create hard service levels, recovery time objectives, recovery point objectives, customer audit rights, customer penetration testing rights, regulated-data commitments, or service-credit rights unless expressly stated in an applicable Order Form, data processing addendum, business associate agreement, or other applicable written addendum incorporated into the Agreement.

The applicability of particular safeguards may depend on the nature of the Services, the applicable Order Form, the customer-enabled features, the Customer Data processed, the integrations configured, and Provider's then-current technical and operational environment.

2. Security Program.

Provider maintains a written information security program designed to protect Customer Data in Provider's possession or control. Provider's security program includes commercially reasonable administrative, technical, and organizational safeguards appropriate to the nature of the Services, the Customer Data processed by Provider, and Provider's then-current operating environment. Such safeguards may include, as applicable, policies and practices addressing access control, authentication, encryption, cloud security, vulnerability management, patch management, logging and monitoring, incident response, business continuity and disaster recovery, personnel security, third-party service provider management, data retention, and secure disposal.

Provider reviews and updates its information security policies and practices from time to time to address changes in the Services, business operations, legal requirements, security risks, and industry practices. Provider may update, modify, replace, or supplement its security measures from time to time, provided that Provider will not materially diminish the overall level of protection for Customer Data during the applicable Subscription Term.

3. Access Controls.

Provider maintains access controls designed to limit access to Customer Data to authorized personnel, systems, and service accounts with a legitimate business need to provide, secure, support, maintain, troubleshoot, configure, improve, or operate the Services. Provider's access-control practices may include, as applicable, unique user accounts, role-based access control, least-privilege access, access approval workflows, access modification or removal when personnel no longer require access, privileged-access restrictions, logging of privileged or administrative activity, and periodic access reviews.

Provider uses multi-factor authentication for administrative access to material production systems where technically supported and commercially reasonable. Provider may also use password controls, account lockout controls, remote access controls, and other authentication safeguards designed to reduce unauthorized access risk. Customer is responsible for administering Customer's Authorized Users, Customer systems, Customer credentials, Customer networks, Customer-selected Third-Party Services, Customer-managed integrations, and Customer-side access decisions.

4. Tenant Isolation and Enterprise Service Separation.

Provider delivers the Services as an enterprise SaaS offering and uses logical tenant separation designed to keep Customer identities, configurations, permissions, and Customer Data logically separated from other customers. Provider's tenant-isolation practices may include tenant-scoped administrative roles, tenant-specific role assignments and permissions, tenant-scoped resources, authentication and authorization controls, role-based access controls, tenant-context validation, and deny-by-default handling of unauthorized or inconsistent cross-tenant access attempts.

5. Encryption.

Provider uses commercially reasonable encryption measures designed to protect Customer Data in transit and at rest, as applicable to the Services and Provider's hosting environment. Provider requires HTTPS using TLS 1.2 or higher for protected Service endpoints, including the web application, APIs, and file upload/download pathways exposed by Provider. Provider does not support plaintext HTTP for protected Service endpoints.

Provider uses commercially reasonable measures designed to encrypt Customer Data at rest where supported by Provider's cloud infrastructure, storage systems, databases, or hosting environment. Provider manages certificates and related transport-security configurations using commercially reasonable operational practices, which may include cloud-provider certificate management tools, restricted administrative access, renewal, rotation, and periodic review of transport-security posture.

Customer is responsible for ensuring that Customer browsers, API clients, gateways, scripts, proxies, and network configurations support the applicable encryption protocols and properly validate certificates.

Customer is responsible for any TLS inspection, interception, proxying, or similar customer-managed network controls.

6. Authentication, API Credentials, and Integration Tokens.

Where the Services support APIs, service accounts, integrations, access tokens, refresh-style session mechanisms, or API keys, Provider maintains commercially reasonable controls designed to reduce risks associated with credential leakage, long-lived credentials, and unauthorized reuse. Such controls may include short-lived access tokens, configurable expiration controls, API key expiration where supported, credential rotation, credential revocation, administrative restrictions on credential lifecycle actions, and logging of credential creation, modification, use, expiration, and revocation at an appropriate operational level.

Customer is responsible for Customer-side governance, storage, distribution, rotation, and protection of credentials, API keys, tokens, secrets, and integration credentials within Customer systems and Customer-managed environments. Customer will not store credentials in insecure locations, including public repositories, unencrypted files, shared documents, or collaboration tools.

7. Cloud Infrastructure, Third-Party Services, and AI Model Providers.

Provider may use Third-Party Services, including cloud infrastructure, hosting providers, AI model providers, security tools, analytics tools, support tools, file-processing tools, and integration providers, to provide, secure, support, maintain, and improve the Services. Provider uses commercially reasonable vendor management and cloud security practices designed to evaluate and manage Third-Party Services that process Customer Data on Provider's behalf, taking into account the nature of the Third-Party Service, the Customer Data processed, and the services provided.

Provider will use commercially reasonable measures designed to ensure that Third-Party Services used by Provider to process Customer Data are subject to confidentiality, security, data protection, breach notification, or other contractual or technical controls appropriate to the nature of the services provided. Provider's cloud-security practices may include, as applicable, access controls, encryption, logging and monitoring, patch management, network security, backup and recovery practices, and review of relevant vendor security posture or assurance materials.

Provider remains responsible for its obligations under the Agreement with respect to Customer Data in Provider's possession or control, except to the extent an issue is caused by Customer systems, Customer-selected Third-Party Services, Customer configurations, Customer credentials, Customer Data, Customer instructions, or Customer's failure to comply with the Agreement or applicable third-party terms. For clarity, Provider is not required to disclose proprietary model provider selection, model routing, orchestration, prompts, system instructions, workflow logic, configurations, architecture, source code, model selection criteria, internal evaluations, or other Provider IP.

8. Data Location and Offshore Access.

Customer Data will be hosted in the United States unless otherwise stated in an applicable Order Form or otherwise agreed in writing by the Parties. Notwithstanding the foregoing, Provider may permit access to Customer Data by Provider personnel, subcontractors, and Third-Party Services providers located outside the United States solely as necessary to provide, maintain, secure, support, troubleshoot, and operate the Services, provided that such personnel, subcontractors, and providers are subject to confidentiality, security, data protection, or other obligations designed to protect Customer Data. Provider will implement commercially reasonable administrative, technical, and organizational safeguards for such access and will comply with applicable laws governing cross-border transfers of Customer Data, including use of appropriate transfer mechanisms where required by applicable law. Provider remains responsible for its obligations under the Agreement with respect to such access. Provider will apply commercially reasonable access-control, authentication, confidentiality, logging, or monitoring controls to such access, as appropriate based on Provider's security program and the nature of the access.

9. Personnel Security and Training.

Provider personnel with access to Customer Data are subject to confidentiality obligations or duties. Provider provides security awareness guidance or training to relevant personnel as appropriate based on role and business need. Such guidance or training may address, as applicable, secure handling of confidential information, phishing and social engineering awareness, access-control responsibilities, incident reporting, secure development practices, cloud security, and AI-related data protection practices. Provider may provide additional role-based security guidance or training to personnel with security-sensitive, technical, administrative, or development responsibilities.

10. Vulnerability Management, Patch Management, and Penetration Testing.

Provider maintains commercially reasonable vulnerability management and patch management practices for Provider-controlled systems used to provide the Services. Such practices may include vulnerability scanning, security assessments, monitoring of vendor advisories and vulnerability sources, risk-based prioritization, patch testing, deployment of security updates, remediation tracking, rescanning or validation where appropriate, and use of compensating controls where immediate remediation is not commercially reasonable or operationally feasible.

Remediation is risk-based and may depend on severity, exploitability, likelihood, potential impact, vendor dependencies, operational feasibility, availability of patches, testing requirements, and the need to avoid material disruption to the Services. Provider conducts at least annual penetration testing or independent security testing of material Provider-controlled production systems used to provide the Services by a qualified independent third party. Provider will use commercially reasonable efforts to remediate critical and high-severity findings within thirty (30) days after discovery or receipt of the applicable test results, unless remediation reasonably requires a longer period due to technical complexity, vendor dependency, operational risk, testing requirements, or the need to avoid material disruption to the Services.

Provider may make a reasonable summary of penetration testing results or remediation status available to Customer upon reasonable request under NDA, subject to Provider's security, confidentiality, legal,

operational, and third-party restrictions. Provider is not required to disclose vulnerability details, exploit information, security architecture, source code, model configurations, prompts, orchestration logic, or other sensitive technical or proprietary information.

11. Logging and Monitoring.

Provider maintains commercially reasonable logging, monitoring, and alerting practices designed to support the security, operation, troubleshooting, reliability, and integrity of the Services. Such practices may include logging of authentication and authorization events, administrative actions, access-right changes, configuration changes, security events, system events, application events, file upload/download events, credential lifecycle events, and other security-relevant activity at an appropriate operational level.

Provider uses commercially reasonable measures designed to protect security logs from unauthorized access, modification, or deletion. Provider may use automated monitoring, alerting, log correlation, or similar tools to identify suspicious, unusual, or inappropriate activity. Log retention periods may vary based on system, event type, cost, legal, operational, privacy, and security needs.

12. Malicious File Upload and Download Controls.

Where the Services permit file uploads, imports, attachments, exports, reports, or downloads, Provider maintains commercially reasonable file-handling controls designed to reduce the risk that malicious files are uploaded, stored, processed, or redistributed through the Services. Such controls may include file type and size restrictions, content-type validation, pre-release anti-malware scanning, restricted staging, quarantine or blocking of files that are malicious, suspicious, unsupported, or not capable of safe validation, and logging of file-security lifecycle events.

Provider may block, quarantine, reject, remove, or restrict access to files that Provider determines may violate file-handling policy, create security risk, or threaten the Services, Provider systems, Customer Data, or other customers. Provider is not required to disclose sensitive detection details, scanning logic, malware signatures, security tooling, or other information that could reduce the effectiveness of such controls. Customer remains responsible for endpoint security and safe handling of downloaded files within Customer-controlled environments.

13. Incident Response.

Provider maintains an incident response process designed to identify, assess, investigate, contain, mitigate, and remediate confirmed Security Incidents involving Customer Data in Provider's possession or control. Provider's incident response process may include triage, escalation, containment, investigation, mitigation, remediation, preservation of relevant evidence, and post-incident review, as Provider determines appropriate based on the nature and severity of the event. Provider will provide notice of confirmed Security Incidents involving Customer Data in accordance with the Agreement. Provider will take commercially reasonable steps to contain, investigate, mitigate, and remediate the Security Incident and will provide Customer with reasonably available information concerning the nature and scope of the Security Incident, the affected Customer Data, and remediation steps taken or planned, to the extent such

information is reasonably required for Customer to comply with applicable law and does not compromise Provider's security, legal, forensic, confidentiality, or third-party obligations. Provider may provide such information in phases as it becomes available. Provider will cooperate reasonably with Customer in connection with any legally required notifications to affected individuals, regulators, or other legally required recipients arising from a Security Incident involving Customer Data in Provider's possession or control. Provider will not issue any public statement or notice relating to a Security Incident that identifies Customer or Customer Confidential Information without Customer's prior written consent, unless required by applicable law. Provider's notice of, or response to, a Security Incident does not constitute an admission of fault, liability, or breach of the Agreement. Provider has no obligation to notify Customer of unsuccessful security attempts, pings, scans, denial-of-service attacks, attacks on firewalls, malware blocked in the ordinary course, or other events that do not result in a confirmed Security Incident involving Customer Data in Provider's possession or control.

14. Business Continuity and Disaster Recovery.

Provider maintains commercially reasonable business continuity and disaster recovery practices designed to support continuity or restoration of material Provider-controlled systems following material disruptions. Such practices may include risk assessment, identification of critical systems or business functions, backup and recovery practices, redundancy or failover measures where commercially reasonable, incident communications procedures, defined internal recovery responsibilities, periodic review, and testing or tabletop exercises.

Provider's backup, redundancy, and recovery practices may vary by system, data type, environment, hosting provider, customer configuration, and operational risk. Unless expressly stated in an applicable Order Form, Provider does not commit to any specific recovery time objective, recovery point objective, uptime credit, service credit, disaster recovery service level, or uninterrupted availability.

15. Customer Data Handling, Retention, and Disposal.

Provider will process Customer Data in accordance with the Agreement and applicable Order Form. Provider maintains commercially reasonable data handling, retention, and disposal practices designed to retain records only as reasonably necessary for business, legal, security, compliance, audit, operational, backup, archival, and disaster recovery purposes, and to dispose of data no longer required in accordance with Provider's retention and disposal practices.

Following expiration or termination, retention of Customer Data and related records is governed by Section 5.4 of the MSA and any applicable DPA. Retained Customer Data remains subject to the confidentiality and security obligations of the Agreement.

Where Provider disposes of Customer Data from Provider-controlled systems, Provider uses commercially reasonable deletion, sanitization, or disposal methods appropriate to the nature of the data, storage medium, system, and operational context.

16. AI Data Protection and AI Feature Governance.

Provider will not use Customer Data to train or fine-tune models, or permit third-party AI model providers to use Customer Data to train or improve their publicly available, general-purpose models, unless Customer expressly agrees in writing or otherwise provides documented explicit authorization through an agreed administrative enablement workflow, Order Form, statement of work, addendum, or other written instruction from an authorized Customer representative.

For clarity, retrieval, indexing, embeddings, search, retrieval-augmented generation, contextualization, evaluation, prompting, inference, summarization, classification, extraction, recommendation, and generation activities used to provide customer-enabled functionality do not constitute training or fine-tuning to the extent they do not modify model parameters. Provider may process Customer Data, AI Outputs, configurations, interactions, Aggregated Statistics, Usage Data, and related metadata as permitted by the Agreement, including to provide, secure, support, maintain, troubleshoot, configure, improve, and operate the Services for Customer. Provider will not use Customer Data in evaluation datasets for other customers or for public model improvement except as expressly authorized by Customer or permitted under Section 5.3 of the MSA.

Where Customer enables AI Features that operate over Customer Data through retrieval, indexing, search, RAG, or similar contextualization, Provider will use commercially reasonable controls designed to enforce tenant-scoped configuration, access controls, and Customer-approved data scope. Customer is responsible for identifying authorized data sources, ensuring Customer Data is appropriate for the enabled AI Feature, limiting Customer Data to the data reasonably necessary for the applicable use case, and ensuring that Customer has all required rights, permissions, consents, notices, and lawful bases for such use.

Provider will use commercially reasonable measures designed so that AI Features do not provide users access to Customer Data they are not authorized to access through the Services, based on Provider-controlled permissions and configurations applicable to the Services. Provider may maintain records or logs sufficient to support review of AI Feature enablement, data-scope changes, and related operational activity, subject to Provider's confidentiality, security, legal, operational, and third-party restrictions.

17. Human-in-the-Loop and Agent Action Controls.

Where supported by the Services, Provider may make available human-in-the-loop controls, approval workflows, review paths, role-based permissions, audit trails, or other governance controls for Agent-generated outputs or Agent-initiated actions. Such controls are designed to allow Customer to configure, review, approve, reject, override, or monitor certain Agent-prepared actions based on Customer's use case, tenant configuration, user roles, and applicable Order Form.

Where human-in-the-loop controls are enabled or required for a sensitive action, Provider will use commercially reasonable measures designed to require explicit approval through an authenticated user interaction or approved administrative workflow before the applicable Agent action is executed. Sensitive actions may include, where applicable, modifying or deleting records, performing mass updates, transmitting Customer Data externally, generating shareable exports, sending messages externally, or

triggering downstream workflows that materially affect Customer Data, business operations, access rights, security posture, or compliance-relevant records.

Customer is responsible for configuring available Agent controls appropriately, assigning administrative and approval roles, training users and approvers, defining Customer's internal approval rules, and reviewing audit logs or approval records made available through the Services. Provider is not responsible for Customer's approval decisions, Customer's failure to configure available controls, or actions taken by Customer's Authorized Users within the permissions granted by Customer.

18. Independent Security Assessments and Security Documentation.

Provider has completed a SOC 2 Type I examination covering Provider's security controls as of the applicable report date. Provider maintains an information security program and may have such program assessed periodically by an independent third party using a recognized industry-standard framework, including SOC 2 Type I or a substantially equivalent independent security assessment. Upon Customer's reasonable request, Provider may make its then-current SOC 2 Type I report, or a reasonable summary of such report, available to Customer under NDA, subject to Provider's security, confidentiality, legal, operational, and third-party restrictions. Provider is not required to obtain or maintain SOC 2 Type II, ISO 27001 certification, or any other specific certification, attestation, audit report, or third-party assessment unless expressly stated in an applicable Order Form or separate written agreement signed by Provider. Provider may respond to reasonable security questionnaires or information requests, subject to Provider's security, confidentiality, legal, operational, and third-party restrictions. Provider will reasonably cooperate with Customer's security review process by responding to reasonable security questionnaires and providing available security documentation, summaries, certifications, attestations, and policy descriptions, subject to Provider's confidentiality, security, legal, operational, third-party, and Provider IP restrictions. Provider may satisfy security information requests by providing summaries, policy descriptions, certifications, attestations, control narratives, redacted configuration screenshots, redacted audit log samples, security documentation, or other materials determined by Provider to be appropriate. Provider is not required to disclose information that, in Provider's reasonable judgment, would compromise the security, confidentiality, integrity, or availability of the Services, Provider systems, other customers' data, Provider IP, model configurations, prompts, orchestration logic, source code, security architecture, vulnerability information, or other sensitive technical or proprietary information.

19. Customer Security Responsibilities.

Customer is responsible for:

(a) securing Customer systems, networks, accounts, credentials, integrations, browsers, API clients, endpoints, and devices;
(b) administering Customer's Authorized Users, tenant administrators, roles, permissions, access rights, and approval authorities;
(c) promptly deprovisioning Authorized Users who no longer require access to the Services;
(d) ensuring that Customer Data submitted to or made available through the Services is accurate, appropriate, lawful, and limited to data reasonably necessary for the applicable use case;

(e) obtaining and maintaining all required rights, consents, notices, permissions, and lawful bases for Provider to process Customer Data, including in connection with Customer-enabled AI Features, integrations, indexing, retrieval, contextualization, or Agent workflows;
(f) reviewing and approving the Customer Data sources, repositories, datasets, roles, groups, and purposes used for Customer-enabled AI Features, where applicable;
(g) configuring Customer systems, Customer-selected Third-Party Services, Customer-managed integrations, available tenant settings, human-in-the-loop controls, approval workflows, and security features securely and appropriately for Customer's use case;
(h) protecting Customer-managed tokens, API keys, passwords, secrets, integration credentials, and other authentication materials, including by using secure secret-management practices and rotating or revoking credentials as appropriate;
(i) ensuring Customer browsers, API clients, proxies, gateways, and network configurations support applicable security protocols and do not weaken transport-security protections;
(j) maintaining endpoint protection, patching, and safe file-handling practices for Customer-controlled systems and downloaded files;
(k) following Provider's reasonable security instructions; and
(l) not submitting protected health information, payment card data, or other specially regulated data unless expressly authorized in the applicable Order Form and covered by an applicable DPA, business associate agreement, or other legally required protective addendum.

Provider is not responsible for unauthorized access, disclosure, loss, corruption, degradation, or other security issues to the extent caused by Customer's failure to satisfy the responsibilities described in this Section.

20. Customer Security Testing.

Unless expressly stated in an applicable Order Form or separate written agreement signed by Provider, Customer may not conduct penetration testing, vulnerability scanning, security testing, load testing, scraping, automated assessment, or other testing of the Services or Provider systems. Customer also may not attempt to bypass, disable, probe, or circumvent Provider's access controls, tenant isolation controls, file scanning controls, human-in-the-loop controls, model safeguards, rate limits, authentication mechanisms, monitoring controls, or other security features except as expressly authorized in writing by Provider. This Section does not limit compliance-audit rights expressly provided under an applicable DPA, which do not authorize technical testing of Provider systems without Provider's prior written consent.

21. Limitations.

These Security Measures do not expand Provider's liability beyond the limitations, exclusions, and caps established in the Agreement. The Agreement controls in the event of any conflict. Supporting security documentation, policies, questionnaire responses, and similar materials do not create additional contractual obligations unless expressly incorporated into the Agreement.