HICO VAULT

END USER LICENSE AGREEMENT
TERMS OF USE

Version 1.0
Effective Date: The date on which the Customer first accepts this Agreement or first accesses or uses the Service ("Effective Date").
This End User License Agreement ("Agreement") constitutes a legally binding contract by and between:

1. HICO Group AG, a company incorporated under the laws of Switzerland, having its registered office at Hauptstrasse 157, 8272 Ermatingen, Switzerland ("HICO", "we", "us", or "our"); and

2. The Customer, an entity or organization and its duly authorized employees, contractors, or representatives who are permitted to access or use the Service (collectively, "Users"),
(each a "Party" and collectively, the "Parties").

This Agreement governs the access, use and licensing of HICO Vault Chat ("Vault Chat" or the "Service"), including all associated software, web interfaces, tools, documentation, updates and any related services provided by HICO.
By accessing, registering for, or using Vault Chat, the Customer and Users acknowledge, agree and warrant that they have:

- Read and understood this Agreement in its entirety;

- The legal authority to bind the Customer to the terms herein; and
- Agreed to be fully bound by all terms, conditions, obligations and disclaimers set forth in this Agreement.

If the Customer or any User does not agree to any provision of this Agreement, they are prohibited from accessing or using the Service.

1. SCOPE OF THE PRODUCT AND SERVICE

1.1 Service Description
Vault Chat is a web-based artificial intelligence-powered communication and assistance platform that enables the Customer and its authorized Users to securely interact with multiple large language models ("LLMs") through a centralized chat interface. The Service is designed exclusively for internal business purposes and may not be used for personal, consumer, or unlawful activities.

The Service includes all associated software, web interfaces, tools, documentation, updates and related services provided by HICO, whether delivered online, via API, or through other mechanisms.

1.2 Operational Role of HICO
HICO provides the technical infrastructure, administrative tools and user interface necessary to access, interact with and manage third-party AI models. HICO does not develop, train, maintain, or operate the LLMs themselves. The Service functions solely as a platform enabling interaction with external AI models under the terms of this Agreement.

HICO is responsible for:

- Ensuring the proper integration of AI models into Vault Chat;

- Maintaining the hosting infrastructure, security and availability of the Service;

- Providing administrative and monitoring tools to manage Users, roles, permissions and token usage.

The Customer acknowledges that HICO's obligations are limited to platform provisioning and do not extend to the internal functioning, outputs, or decision-making of third-party AI models.

1.3 Third-Party AI Model Providers
Vault Chat integrates and provides access to external AI models.
The AI models currently integrated into the VAULT Chat are displayed at https://www.hico-vault.com.

HICO reserves the right to integrate additional or substitute AI providers at its discretion. In the event of significant changes to the list of AI model providers, HICO will notify the Customer in a timely manner.

The Customer acknowledges and agrees that HICO is not responsible for the availability, performance, or outputs of third-party AI model providers.

1.4 Key Features of the Service
The Service provides, among other functionalities:

- A web-based chat interface for interaction with integrated LLMs;

- An administrative panel for managing Users, roles, permissions, token quotas and configuration settings;

- The ability to upload, process and analyze text and PDF documents;

- Access to web search, formatted outputs and file download functionalities;

- A white-label option allowing customization of branding, logos, colors and domain configuration to align with the Customer's corporate identity.

The Customer acknowledges that the availability and performance of certain features may depend on technical constraints or the capabilities of third-party AI providers.

1.5 Hosting and Data Processing Locations
- The Service is primarily hosted on EU-based servers, including Kamatera Germany and Microsoft Azure EU regions (Northern and Western Europe).

- Processing outside the EU may occur only if technically necessary, for instance in response to provider outages, peak loads, or model-specific requirements.

- The Customer acknowledges that while HICO will make reasonable efforts to maintain all processing within the EU, non-EU processing may occasionally be unavoidable.

1.6 Nature and Use of AI-Generated Responses
All outputs generated by Vault Chat are produced by statistical AI models and are:

- Indicative only and may contain errors, omissions, or inaccuracies;

- Non-binding and do not constitute professional, legal, financial, or medical advice;

- To be reviewed, validated and verified by the Customer before use, distribution, publication, or decision-making.

The Customer acknowledges that Vault

Chat is a support tool and that responsibility for the use, interpretation and dissemination of AI-generated content remains solely with the Customer.

2. TRANSPARENCY OF AI FUNCTIONALITY AND DECISION-MAKING

2.1 Disclosure of AI Operations

HICO provides Users with full transparency regarding the operation of Vault Chat and the underlying artificial intelligence models. Specifically, the Customer and Users acknowledge and agree that:

1. Automated Generation of Responses: All outputs produced by Vault Chat are automatically generated by integrated large language models (LLMs), including third-party AI providers, based on statistical algorithms and pattern recognition. These outputs are indicative only and may not be complete, accurate, or suitable for any particular purpose.

2. No Legally Binding Automated Decisions: Vault Chat does not perform automated decisions that carry legal effects, regulatory consequences, or other significant outcomes for the Customer, its Users, or third parties. All decisions based on AI-generated outputs remain the sole responsibility of the Customer and Users.

3. Purpose-Limited Data Processing: Inputs provided by the Customer or Users are processed solely to generate the requested outputs. HICO does not use such inputs or outputs for training, fine-tuning, or improving AI models unless expressly authorized in writing by the Customer.

2.2 Interface Disclaimers and Notices

Vault Chat incorporates clear and prominent interface notices to inform Users about:

- The limitations, capabilities and statistical nature of AI outputs;

- The potential for inaccuracies, inconsistencies, or incomplete results; and

- Relevant operational or technical risks associated with using the Service.

These notices are designed to ensure that all Users are aware of the proper context for interpreting AI-generated content and the inherent limitations of automated responses.

2.3 Customer Responsibility for AI Outputs

The Customer acknowledges and agrees that:

1. The use of Vault Chat is as a support and advisory tool only and HICO does not assume responsibility for any decisions, actions, or consequences arising from the use of AI-generated outputs.

2. The Customer and its Users are solely responsible for:

- Reviewing, validating and interpreting AI-generated outputs;

- Verifying any information before reliance, dissemination, or decision-making; and

- Ensuring that any reliance on outputs complies with applicable laws, internal policies, or regulatory obligations.

3. HICO shall not be liable for any direct, indirect, or consequential damages resulting from the Customer's or Users' use of AI-generated outputs.

3. DATA PROTECTION AND GDPR COMPLIANCE

3.1 EU-Based Processing

HICO ensures that the primary processing of all Customer and User data occurs on servers located within the European Union, specifically including Kamatera Germany and Microsoft Azure EU regions (Northern and Western Europe).

All processing within these locations is conducted in accordance with applicable EU data protection laws, including the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR").

3.2 Cross-Border Processing

In the event that data processing outside the European Union is technically necessary (e.g., provider outages, peak system loads, or model-specific requirements), HICO shall ensure that:

1. Standard Contractual Clauses (SCCs) or equivalent legally recognized safeguards are implemented;

2. Appropriate technical and organizational measures are in place to maintain confidentiality, integrity and security of Customer and User data; and

3. Cross-border processing occurs only to the minimum extent necessary for proper functioning of Vault Chat.

The Customer acknowledges that while HICO will endeavor to minimize cross-border processing, some limited non-EU processing may be unavoidable under operational constraints.

3.3 Data Retention

HICO shall process and retain Customer and User data only for as long as necessary to provide the Service and for operational purposes. Specifically:

- Temporary data: Session logs, temporary uploads and related service data are retained solely for the duration required to execute the requested operations;

- Account or User termination: Upon expiration of a license term, deletion of an account, or when a User leaves the Customer organization, all associated data will be permanently deleted within fourteen (14) calendar days;

- HICO does not retain Customer or User data beyond this period, except as required by law or regulatory obligations.

3.4 Model Training and AI Use

HICO does not use Customer or User data to train, fine-tune, or improve any AI models, whether operated by HICO or third-party providers, unless otherwise expressly authorized in writing by the Customer.

3.5 Customer and User Rights

The Customer and its Users retain all rights granted under GDPR, including but not limited to:

1. Access: Right to obtain confirmation of processing and access to personal data;

2. Rectification: Right to correct inaccurate or incomplete personal data;

3. Erasure: Right to request deletion of personal data processed by Vault Chat;

4. Restriction of Processing: Right to request limitations on the processing of personal data;

5. Feature Deactivation: Right to request deactivation of specific Service functionalities (e.g., web search or external

integrations) to limit data processing;

6. Data Portability and Objection: Where applicable, rights to receive personal data in a structured, machine-readable format and to object to processing.

HICO shall respond to all requests from the Customer or Users in a timely manner consistent with GDPR requirements.

3.6 Incorporation of Privacy Policy
The HICO Privacy Policy, as may be updated from time to time, is incorporated by reference and forms an integral part of this Agreement. By using the Service, the Customer and Users acknowledge that they have read, understood and accepted the Privacy Policy.

4. RESPONSIBILITIES OF THE PARTIES

4.1 HICO's Responsibilities
HICO shall use commercially reasonable efforts to provide Vault Chat in a secure, stable and reliable manner. In particular, HICO shall be responsible for:

1. Service Security and Reliability: Maintaining the Service infrastructure to ensure operational continuity, system availability and protection against unauthorized access, loss, or corruption of data;

2. Third-Party AI Model Integration: Properly integrating all third-party AI models into Vault Chat and ensuring they function as intended within the Service platform;

3. Hosting Infrastructure and Administrative Tools: Managing the hosting environment, administrative dashboards, user management, role assignments and token allocation in accordance with this Agreement;

4. Role-Based Access and Token Management: Implementing and enforcing access controls, role-based permissions and token quotas to ensure fair and secure usage of the Service;

5. System Performance Monitoring: Monitoring Service performance, detecting system anomalies and taking reasonable measures to maintain availability and mitigate downtime;

6.1 Technical Support Services: Provider shall provide support for functional issues and technical malfunctions of the Chatbot Service („Functional Support")

6.2 2 Response Time. Provider shall acknowledge and provide an initial response to any technical support request submitted by the Customer through the official support channels [e.g. support-portal/email] within a maximum of 48 hours from the time the request was received.

This support period applies to the initial technical assessment only. The time required for a final resolution may vary depending on the complexity of the technical issue. Support does not include content-related changes, design adjustments, or third-party infrastructure failures beyond the Provider's control.

6.3 For assistance in how to use the software and manage users, please refer to the product help. Alternatively, you can purchase book a support package via our webshop. Our general support is limited to technical issues, like bugs and connectivity issues.

HICO shall not be responsible for any errors, omissions, or inaccuracies in AI-generated outputs or for decisions made by the Customer or Users based on such outputs.

4.2 Customer Responsibilities
The Customer acknowledges and agrees to:

1. Verification of AI Outputs: Review, validate and verify all AI-generated content prior to use, distribution, or reliance in any business decision;

2. Sensitive Data Restrictions: Avoid inputting unnecessary sensitive or prohibited data, including but not limited to health data, financial data, identity data, special-category data under GDPR and unauthorized third-party data;

3. Credential Security: Maintain strict confidentiality of all credentials, login details and access tokens and ensure they are not shared with unauthorized parties;

4. Access Control: Limit access to Vault Chat strictly to authorized Users within the organization and promptly revoke access for departing personnel;

5. Compliance with Laws and Policies: Ensure all use of the Service complies with applicable local, national and international laws, as well as internal corporate policies and guidelines;

6. Responsible Use: Use Vault Chat in accordance with the terms and limitations of this Agreement, including token limits, acceptable use policies and feature-specific restrictions.

The Customer acknowledges that misuse, improper input of sensitive data, or violation of this Agreement may result in temporary or permanent suspension of access to the Service at HICO's discretion.

4.3 No Assumption of Liability for AI-Generated Content

The Customer and Users acknowledge and agree that:

1. Vault Chat is provided as a tool to assist workflows and decision-making and HICO does not assume responsibility for the accuracy, completeness, reliability, or appropriateness of AI-generated outputs;

2. Any actions, decisions, or outcomes resulting from reliance on AI-generated content are solely the responsibility of the Customer;

3. HICO expressly disclaims liability for any direct, indirect, incidental, or consequential damages arising from the use of AI outputs, including but not limited to business, financial, or reputational losses.

5. PROHIBITED CONTENT AND SENSITIVE DATA

5.1 Restrictions on User Inputs
The Customer acknowledges and agrees that Vault Chat is not intended for the processing of highly sensitive or restricted data unless absolutely necessary for legitimate business purposes. Users must not input or submit any of the following data types.

1. Health or Medical Data: Including diagnoses, clinical findings, therapies, or other health-related personal information;

2. Financial Data: Including bank account numbers, credit card information, investment portfolios, or other confidential financial details;

3. Identity Information: Including government-issued ID numbers, passport numbers, social security numbers, or equivalent personally identifiable information;

4. Special-Category Data under GDPR Article 9: Including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, or biometric data;

5. Third-Party Personal Data: Any data belonging to individuals for whom the Customer does not hold proper authorization to submit.

The Customer shall implement internal policies, training and monitoring to ensure Users comply with these restrictions.

5.2 Risk Allocation and Liability Disclaimer

The Customer and its Users acknowledge and agree that:

1. Assumption of Risk: Any input of prohibited, sensitive, or otherwise restricted data is undertaken at the sole risk of the Customer and Users;

2. Liability Disclaimer: HICO expressly disclaims all liability, including direct, indirect, incidental, or consequential damages, arising from the Customer's or Users' submission of prohibited or sensitive data;

3. Indemnification: The Customer shall indemnify, defend and hold harmless HICO from any claims, losses, damages, or regulatory penalties arising from unauthorized or improper submission of sensitive data to the Service.

6. KNOWN RISKS AND MITIGATION MEASURES

6.1 Acknowledged Risks

The Customer acknowledges that the use of Vault Chat involves certain inherent risks, including but not limited to:

1. Inaccurate or Incomplete Outputs: AI-generated responses may contain errors, omissions, or inaccuracies and are indicative only;

2. Dependency on Third-Party LLM Providers: Vault Chat relies on external AI providers (e.g., Microsoft Azure OpenAI Service, OpenAI GPT-5, xAI Grok 3, Mistral AI) and their availability, performance, or accuracy may be subject to limitations outside the control of HICO;

3. Accidental Submission of Sensitive Data: Users may inadvertently input sensitive, restricted, or third-party data contrary to Section 5;

4. Exceeding Token Limits or Usage Quotas: Users may unintentionally exceed allocated token limits, potentially affecting service performance or triggering usage restrictions.

The Customer acknowledges that these risks are inherent to AI services and that HICO cannot guarantee the absolute accuracy, completeness, or uninterrupted availability of the Service.

6.2 Mitigation Measures Implemented by HICO

HICO has implemented technical, organizational and administrative safeguards to mitigate known risks and enhance the security, reliability and compliance of Vault Chat, including:

1. Certified EU-Based Hosting: Use of hosting infrastructure located within the European Union, operated by certified providers (e.g., Kamatera Germany, Microsoft Azure EU) to ensure data protection compliance;

2. Encryption and Security: End-to-end TLS encryption, secure authentication and advanced cybersecurity measures

to protect data in transit and at rest;

3. Role-Based Access Control and Token Management: Enforcement of user roles, permissions and token quotas to prevent unauthorized access and ensure fair and secure use of the Service;

4. Interface Notices for AI Limitations: Prominent, in-application notices alerting Users to the statistical nature of AI outputs, limitations and potential inaccuracies;

5. Limited Retention in Shared Instances: In shared or test environments, temporary data is retained only as necessary for system operation, in accordance with Section 3;

6. Continuous Monitoring and Maintenance: Active monitoring of APIs, system performance, uptime and connectivity to detect anomalies, mitigate potential disruptions and maintain stable service availability.

The Customer acknowledges that while HICO employs these mitigation measures, no technical or administrative safeguard can entirely eliminate all risks and use of the Service remains subject to the limitations and responsibilities described in this Agreement.

7. USAGE LIMITS AND ABUSE PREVENTION

7.1 Token-Based Usage Model

Vault Chat operates on a token-based usage system, with limits established for:

1. Per-Request Tokens: Maximum number of tokens that may be consumed per individual request;

2. Daily Token Quotas: Maximum number of tokens allocated per User per day. The specific token limitsare defined by HICO and are set to enable the customer to use Vault Chat in way that is common and reasonable for chatbots in a daily use. . The Customer acknowledges that exceeding these limits may trigger temporary restrictions or suspension of the Service to maintain fair usage and system stability.

7.2 Abuse Prevention and Enforcement Measures

HICO reserves the right, at its sole discretion, to limit, suspend, or terminate access to Vault Chat in order to prevent abuse, unauthorized activity, or disproportionate resource consumption. Such actions may be taken in response to, but are not limited to:

1. Automated or Mass Requests: Submission of excessive or automated requests that significantly exceed normal business operations;

2. Excessive Token Consumption: Use of tokens beyond reasonable operational limits, whether accidental or deliberate;

3. Unauthorized Data Harvesting: Activities such as web scraping, extraction of data for external AI training, or other unauthorized aggregation of outputs;

4. Circumvention of Controls: Attempts to bypass or override technical, security, or usage restrictions implemented within Vault Chat;

5. Excessive System Load or Costs: Behavior that results in disproportionate server load, degraded performance, or unusually high operational costs.

HICO shall exercise reasonable judgment in enforcing these limits and, where feasible, provide notice to the

Customer regarding corrective measures before suspension. The Customer acknowledges and agrees that such enforcement is necessary to ensure stability, fairness and security of the Service for all Users.

8. WHITE-LABEL BRANDING AND INTELLECTUAL PROPERTY

8.1 White-Label Customization Rights

HICO grants the Customer a limited, non-exclusive, non-transferable right to customize the Vault Chat interface under the Customer's subscription plan. Customization may include:

1. Branding Elements: Modification of logos and color schemes, within the Vault Chat interface;

2. Domain Configuration: Use of Customer-specific domains or subdomains, subject to technical feasibility and compliance with HICO's configuration standards;

3. User Experience Adjustments: Layout and stylistic adjustments that enhance the integration of Vault Chat into the Customer's corporate environment.

All customizations must comply with this Agreement, applicable law and HICO's technical guidelines.

8.2 Restrictions on Branding and Use

The Customer acknowledges and agrees that:

1. No Misrepresentation: Vault Chat shall not be represented or marketed as developed, owned, or operated by the Customer;

2. Respect for Third-Party Rights: Customizations must not infringe or violate the intellectual property rights, moral rights, or other legal rights of any third party;

3. Transparency of Service Origin: Users must not be misled regarding the origin, ownership, or operational control of Vault Chat.

HICO reserves the right to review and request modifications to Customer branding to ensure compliance with these restrictions.

8.3 Intellectual Property Ownership

1. Ownership: All rights, title and interest in and to Vault Chat, including the underlying software, AI integrations, platform architecture, algorithms, documentation, trademarks and all associated intellectual property, remain exclusively owned by HICO or its licensors.

2. No Transfer of Rights: Except for the limited customization rights expressly granted herein, the Customer acquires no rights, licenses, or interests in HICO's intellectual property.

3. Protection: The Customer shall not attempt to reverse-engineer, decompile, copy, or otherwise exploit Vault Chat in a manner inconsistent with HICO's proprietary rights.

9. SYSTEM AVAILABILITY, SUPPORT AND MAINTENANCE

9.1 System Availability

HICO shall use commercially reasonable efforts to ensure that Vault Chat is available and operational on a consistent basis. The Customer acknowledges and agrees that:

1. No Guarantee of Uninterrupted Access: Vault Chat availability may be impacted by factors outside HICO's control, including but not limited to:

- Scheduled maintenance, updates, or upgrades of the Service;

- Outages or performance issues with third-party AI model providers integrated with Vault Chat (e.g., Microsoft Azure OpenAI Service, OpenAI GPT-5, xAI Grok 3, Mistral AI);

- Network, internet, or hosting infrastructure disruptions;

- Force majeure events, including natural disasters, strikes, governmental actions, or other extraordinary circumstances beyond HICO's reasonable control.

2. Temporary Disruptions: HICO may, from time to time, suspend or restrict access to Vault Chat to perform necessary maintenance or updates and shall endeavor to provide advance notice where feasible.

The Customer accepts that such limitations are inherent to cloud-based AI services and shall not constitute a breach of this Agreement.

9.2 Support Services

HICO shall provide technical support to the Customer in accordance with the Customer's subscription plan, which generally includes:

1. Standard Business Hours: Support availability during regular business hours as defined by HICO, unless otherwise agreed in writing;

2. Scope of Support: Assistance regarding access, configuration, troubleshooting and operational issues within the Vault Chat platform;

3. Limitations: Support does not extend to verification of AI-generated content, compliance with Customer internal policies, or use of Vault Chat outputs for external or regulatory purposes.

HICO reserves the right to prioritize support requests based on severity and impact on system performance or Customer operations.

10. SECURITY AND BREACH NOTIFICATION

10.1 Security Measures

HICO shall implement and maintain appropriate technical and organizational measures to ensure the confidentiality, integrity and availability of Customer data processed via Vault Chat, in accordance with applicable data protection laws, including GDPR. Such measures shall include, without limitation:

1. Access Controls: Role-based permissions and secure authentication mechanisms to prevent unauthorized access;
2. Encryption: Data encryption in transit and at rest using industry-standard protocols (e.g., TLS/SSL);

3. System Monitoring: Continuous monitoring of system operations, network activity and potential vulnerabilities;

4. Physical and Logical Security: Secure hosting environments and protection against unauthorized physical or logical access;

5. Incident Management: Internal procedures to detect, respond to and mitigate security incidents. While HICO applies these safeguards, the Customer acknowledges that no system can be entirely immune to security breaches and residual risk remains.

10.2 Breach Notification and Cooperation

In the event of a confirmed or suspected security breach affecting Customer data, HICO shall:

1. Prompt Notification: Notify the Customer without undue delay upon becoming aware of a breach that may materially affect Customer data;

2. Investigation and Mitigation: Cooperate with the Customer to investigate the incident, assess its impact and implement reasonable measures to mitigate further exposure;

3. Regulatory Support: Provide reasonable assistance to enable the Customer to comply with GDPR or other applicable breach notification obligations, including communication with supervisory authorities or affected individuals, as required;

4. Documentation: Maintain internal records of the breach and HICO's response actions for compliance and audit purposes.

HICO shall not be liable for breaches caused by: (i) Customer or User negligence, (ii) unauthorized actions by third parties beyond HICO's control, or (iii) failure to follow HICO's security instructions and best practices.

11. AUDIT AND COMPLIANCE RIGHTS

11.1 Customer Audit Rights

The Customer may, subject to the terms below, request an audit of HICO's processing, hosting and administrative practices to verify compliance with applicable laws and regulations, including but not limited to:

1. General Data Protection Regulation (GDPR): Verification of data protection measures, retention policies and lawful processing of Customer data;
2. AI Act Compliance: Verification of adherence to transparency, risk management and accountability requirements applicable to the AI services provided under Vault Chat. Such audits are intended to provide reasonable assurance of HICO's compliance without disrupting the normal operation of the Service.

11.2 Audit Procedures and Limitations

Any audit requested by the Customer shall be conducted under the following conditions:

1. Scope and Frequency: Audits shall be limited to areas reasonably necessary to verify compliance and may be conducted no more than once per calendar year, unless otherwise agreed in writing;

2. Confidentiality Obligations: The Customer and its representatives conducting the audit shall maintain strict confidentiality regarding all proprietary, technical and operational information of HICO and its third-party providers;

3. Advance Notice: HICO shall be provided with reasonable advance notice of any audit request, including the intended scope, objectives and personnel involved;

4. Operational Impact: Audits shall be conducted in a manner that minimizes disruption to Vault Chat operations and Users;

5. Cost Allocation: Unless otherwise agreed, the Customer shall bear all costs associated with conducting the audit, including any fees for HICO personnel required to facilitate the audit.

HICO reserves the right to deny audit requests that are excessive, duplicative, or beyond the agreed scope to protect

operational integrity, security and the rights of third-party providers.

12. AI ETHICS AND EXPLAINABILITY

12.1 Commitment to Responsible AI

HICO commits to the ethical and responsible use of AI in the provision of Vault Chat, in accordance with applicable laws and regulations, including the European Union AI Act. This commitment encompasses:

1. Transparency: Providing clear information regarding the functionality, limitations and intended use of AI models integrated into Vault Chat;

2. Risk Management: Implementing safeguards to mitigate potential risks associated with AI outputs, including errors, biases, or misuse;

3. Accountability: Ensuring HICO personnel adhere to defined procedures for AI integration, monitoring and oversight, consistent with legal and regulatory obligations.

HICO endeavors to ensure that the Service is aligned with ethical AI principles, including fairness, reliability and safety, but does not guarantee the elimination of all risks or biases inherent in statistical AI models.

12.2 Explainability and User Guidance

HICO provides Customers and Users with accessible information and guidance to promote safe, responsible and informed use of AI within Vault Chat, including:

1. Generation of AI Responses: Clear explanation that outputs are automatically generated by integrated large language models (LLMs) and are statistical in nature;

2. Known Limitations and Potential Biases: Disclosure of potential inaccuracies, model limitations, or biases inherent to AI outputs;

3. Safe Usage Instructions: Guidelines for avoiding input of sensitive or restricted data, verification of outputs before operational use and responsible integration of AI responses into business workflows.

The Customer acknowledges that AI outputs are advisory in nature and HICO does not assume responsibility for decisions or actions taken based on such outputs.

13. INDEMNIFICATION

13.1 Customer Indemnification Obligations

The Customer agrees to indemnify, defend and hold harmless HICO, its affiliates, officers, directors, employees and agents (collectively, the “Indemnified Parties”) from and against any and all claims, losses, liabilities, damages, costs and expenses (including reasonable legal fees) arising out of or relating to:

1. Misuse of Vault Chat: Any unauthorized, improper, or prohibited use of the Service by the Customer or its Users;

2. Entry of Prohibited or Sensitive Data: Submission or processing of data that violates this Agreement, applicable law, or the restrictions set out in Section 5, including highly sensitive or third-party data without proper authorization;

3. Reliance on AI-Generated Outputs: Decisions or actions taken based on outputs generated by Vault Chat, including any consequences from inaccuracies, errors, or omissions in AI res-

ponses;
4. Violation of Laws or Regulations: Any breach of applicable laws, regulations, or internal corporate policies by the Customer or its Users in connection with the use of Vault Chat.

13.2 Indemnification Procedures
The indemnification obligations set forth herein shall be subject to the following procedures:

1. Prompt Notice: HICO shall provide written notice to the Customer of any claim, demand, or action for which indemnification is sought;

2. Control of Defense: The Customer shall have the right, at its own expense, to assume control of the defense and settlement of such claim, provided that HICO shall have the right to participate in such defense at its own expense;

3. Cooperation: HICO shall provide reasonable cooperation to the Customer in the defense of any claim, including providing relevant documentation and access to personnel, at the Customer's reasonable cost;

4. Settlement: The Customer shall not settle any claim in a manner that imposes any obligation or liability on HICO without HICO's prior written consent, such consent not to be unreasonably withheld.

14. FORCE MAJEURE

14.1 Definition and Scope
Neither HICO nor the Customer shall be held liable for any failure, delay, or inability to perform its obligations under this Agreement if such failure or delay is caused by events or circumstances beyond the reasonable control of the affected party ("Force Majeure Events"). Such events include, without limitation:
1. Natural and Environmental Events: Earthquakes, floods, fires, storms, or other acts of God;

2. Human-Caused Events: War, acts of terrorism, riots, strikes, labor disputes, or civil unrest;

3. Third-Party Provider Failures: Outages or disruptions caused by integrated third-party AI model providers, hosting services, or cloud infrastructure;

4. Infrastructure and Utility Failures: Internet connectivity issues, power outages, telecommunication disruptions, or other technical infrastructure failures.

14.2 Effect on Obligations
1. Suspension of Performance: The obligations of the affected party shall be suspended for the duration of the Force Majeure Event and the affected party shall use commercially reasonable efforts to resume performance as soon as reasonably practicable;

2. Notification: The affected party shall promptly notify the other party of the occurrence of a Force Majeure Event, describing the nature, expected duration and impact on performance;

3. Mitigation: Both parties shall use commercially reasonable efforts to mitigate the effects of the Force Majeure Event and resume normal performance;

4. Termination Option: If a Force Majeure Event continues for more than 60 consecutive days, either party may terminate the Agreement without liability by providing written notice to the other party.

15. MODIFICATION OF TERMS

15.1 Right to Update

HICO reserves the right, at its sole discretion, to update, modify, or enhance Vault Chat and/or this Agreement from time to time to reflect changes in the Service, legal requirements, technological improvements, or operational needs. Such updates may include, without limitation:

1. Changes to Service features, functionality, or user interface;

2. Updates required to comply with applicable laws or regulations, including data protection and AI legislation;

3. Modifications to operational, technical, or security requirements.

15.2 Communication and Acceptance

1. Notification of Material Changes: HICO shall provide prior notice of any material changes to this Agreement via email, in-service notifications, or other reasonable communication channels. Material changes include modifications that significantly affect:

- Customer rights or obligations;

- User access, features, or limitations of Vault Chat;

- Data processing, privacy, or security provisions.

2. Customer Response: Upon notification of material changes, the Customer may:

- Accept the changes and continue using Vault Chat under the updated terms; or

- Reject the changes, in which case the Customer may terminate the Agreement without penalty within the notice period specified.

3. Non-Material Changes: Updates that do not materially affect the Customer's rights or obligations shall be effective immediately upon posting or notification and continued use of the Service constitutes acceptance of such changes.

16. TERMINATION FOR CONVENIENCE

16.1 Right to Terminate

Either HICO or the Customer may terminate this Agreement for convenience, without cause, by providing prior written notice to the other party. The required notice period shall be 90 days, unless otherwise agreed in writing. For agreements concluded via the online shop where a notice period of three (3) months is explicitly stated, a deviating notice period of fourteen (14) days to the end of the respective contractual term shall apply.

16.2 Effects of Termination

1. Access Revocation: Upon the effective date of termination, HICO shall revoke the Customer's and Users' access to Vault Chat and all associated administrative and technical functionalities;

2. Data Deletion: HICO shall permanently delete all Customer data, including uploads, session data and logs, within 14 days of termination, except as required to comply with applicable law or regulatory obligations;

3. Outstanding Obligations: Termination shall not release either party from obligations accrued prior to termination, including payment obligations, indemnification and confidentiality commitments;

4. Survival of Clauses: Provisions of this Agreement which by their nature survive termination (including but not limited to Sections 3, 6, 10, 11, 13, 14 and 18) shall remain in full force and effect.

17. SUBPROCESSORS

17.1 Engagement of Subprocessors

HICO may, from time to time, engage third-party subprocessors to perform certain services necessary for the operation, hosting, support, maintenance, analytics, or enhancement of Vault Chat.

Such subprocessors may include, without limitation, cloud hosting providers, AI model providers, technical support vendors and analytics services.

17.2 Customer Consent and Oversight

1. Consent: By entering into this Agreement, the Customer consents to the engagement of subprocessors for the purposes described herein.

2. Responsibility: HICO shall remain fully responsible for the acts or omissions of its subprocessors as if they were HICO's own, including ensuring compliance with all obligations under this Agreement, applicable data protection laws (including GDPR) and security requirements.

3. Notification of Changes: HICO shall provide the Customer with prior notice of any material changes to subprocessors, including the addition or replacement of subprocessors and an opportunity to review relevant compliance information.

4. Due Diligence: HICO shall conduct appropriate due diligence and implement contractual obligations with subprocessors to ensure adherence to the security, confidentiality and data protection obligations imposed by this Agreement.

18. CONFIDENTIALITY

18.1 Obligation of Confidentiality

Each party (the "Receiving Party") agrees to maintain the confidentiality of all non-public information disclosed by the other party (the "Disclosing Party") in connection with this Agreement ("Confidential Information"). Confidential Information includes, without limitation, technical, operational, financial, commercial, strategic, or proprietary information, including data, documentation, trade secrets, business plans, AI models, system architecture and user-related information.

The Receiving Party shall:

1. Use Confidential Information solely for the purposes of performing or enjoying the benefits of this Agreement;

2. Restrict disclosure of Confidential Information to its employees, contractors, or agents on a need-to-know basis who are bound by confidentiality obligations at least as restrictive as those herein;

3. Implement appropriate technical, administrative and organizational measures to protect Confidential Information against unauthorized access, disclosure, or use.

18.2 Permitted Disclosures

Confidential Information may be disclosed only to the extent that the Receiving Party can demonstrate that such disclosure:

1. Is already in the public domain at the time of disclosure through no fault of the Receiving Party;

2. Was independently developed by the Receiving Party without reference to the Disclosing Party's Confidential Information;

3. Is required to be disclosed by applicable law, regulation, or court order, provided that the Receiving Party gives prompt written notice to the Disclosing Party to enable the Disclosing Party to seek protective measures.

18.3 Duration of Confidentiality
All confidentiality obligations shall survive termination or expiration of this Agreement for a period of five (5) years, except for trade secrets or information protected under applicable law, which shall remain confidential for as long as legally permissible.

19. LIMITATION OF LIABILITY

19.1 No Warranties
Vault Chat outputs are automatically generated by statistical AI models and may contain inaccuracies, errors, or omissions. HICO makes no representations or warranties, whether express, implied, statutory, or otherwise, including without limitation any warranties of:

1. Accuracy, completeness, or reliability of AI-generated content;

2. Merchantability, fitness for a particular purpose, or non-infringement;

3. Uninterrupted or error-free operation of Vault Chat.

19.2 Exclusion of Liability
To the maximum extent permitted by applicable law, HICO shall not be liable for any claims, losses, or damages arising from or relating to:

1. Customer or User reliance on AI-generated outputs;

2. Loss, corruption, or unauthorized access to Customer data;

3. Service interruptions, downtime, or system failures;

4. Indirect, incidental, consequential, punitive, or special damages, including loss of profits, revenue, or business opportunities;
5. Failures or interruptions caused by third-party AI model providers, hosting services, or other subprocessors;

6. Misuse, abnormal, or abusive usage of Vault Chat by Users, including exceeding token limits or circumventing technical restrictions.

19.3 Cap on Liability
Except for liability arising from gross negligence, willful misconduct, or breach of confidentiality obligations under this Agreement, HICO's total aggregate liability to the Customer for any claim, whether in contract, tort, or otherwise, shall not exceed the total fees paid by the Customer to HICO under this Agreement during the twelve (12) months immediately preceding the event giving rise to the claim.

20. TERM AND TERMINATION

20.1 Standard Term
Unless otherwise agreed in writing, this Agreement shall have an initial term of twelve (12) months (the "Initial Term"), commencing on the Effective Date. The Agreement shall automatically renew for successive twelve (12) month periods (each a "Renewal Term") unless either party provides written notice of non-renewal at least three (3) months prior to the expiration of the then-current term.

20.2 Starter Package Term
For Customers subscribing to the Starter Package, the initial term shall be three (3) months, automatically renewing for a subsequent three (3) month period unless either party provides written notice of termination at least two (2) weeks prior to the end of the initial term.

20.3 Effects of Termination
Upon the expiration or earlier termina-

tion of this Agreement, for any reason:
1. Revocation of Access: HICO shall immediately revoke the Customer's and Users' access to Vault Chat and all associated administrative functions;

2. Data Deletion: All Customer data, including uploaded files, session logs and AI-generated content, shall be permanently deleted within fourteen (14) days unless otherwise required by law or regulatory obligations;

3. No Data Recovery Obligation: HICO shall have no obligation to retain, restore, or recover deleted data after the applicable deletion period;

4. Survival of Provisions: Obligations under Sections 3 (Data Protection), 6 (Known Risks), 10 (Security), 11 (Audit), 13 (Indemnification), 18 (Confidentiality) and 19 (Limitation of Liability) and any other clauses that by their nature survive termination, shall continue in full force and effect.

21. GOVERNING LAW AND JURISDICTION

21.1 Governing Law
This Agreement, including all matters relating to its validity, interpretation, performance and enforcement, shall be governed by and construed in accordance with the laws of Switzerland, without regard to any conflict of laws principles that would result in the application of the laws of another jurisdiction.

21.2 Jurisdiction
The parties agree that any disputes, claims, or proceedings arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts of Thurgau, Switzerland. Each party hereby irrevocably submits to the jurisdiction of such courts and waives any objections to venue or inconvenient forum.

21.3 Alternative Dispute Resolution
For operational flexibility, the parties may include an optional mediation or arbitration clause, for example:

Prior to initiating litigation, the parties shall attempt in good faith to resolve any dispute through mediation administered by a mutually agreed mediator in Switzerland. If mediation fails, the parties may pursue claims exclusively before the competent courts of Thurgau, Switzerland.

22. FINAL PROVISIONS

22.1 Severability
If any provision of this Agreement is held to be invalid, illegal, or unenforceable by a court of competent jurisdiction, such provision shall be severed from the Agreement and shall not affect the validity, legality, or enforceability of the remaining provisions, which shall continue in full force and effect.

22.2 Entire Agreement
This Agreement constitutes the entire understanding and agreement between the parties with respect to Vault Chat and supersedes all prior or contemporaneous agreements, understandings, communications, or representations, whether written or oral, relating to the subject matter herein.

22.3 Amendments and Updates
HICO may, from time to time, update or modify the terms of this Agreement, including the functionality or features of Vault Chat. Material updates will be communicated to the Customer in writing. Continued use of Vault Chat after receipt of notice constitutes acceptance of the updated terms. Customers who do not accept material changes may

terminate the Agreement in accordance with Section 16 (Termination for Convenience) or other applicable termination provisions.

22.4 No Waiver
Failure or delay by either party to enforce any right or provision under this Agreement shall not constitute a waiver of such right or provision, nor affect the validity of the Agreement.

10. Feb. 2026, Zurich

Executed by:

HICO Group AG

Name:
_____

Title:
_____

Date:
_____

Customer / Company

Name:
_____

Title:
_____

Date:
_____