AI Terms

These AI Terms ("AI Terms") apply to artificial intelligence provided with the SaaS ("AI Technology(ies)"). Any third-party terms applicable to third party components shall apply and take precedence over these AI Terms as it relates to such third-party components.

1. Output

1.1. "**Output**" means any results generated while operating the AI Technologies or any content generated by AI Technologies based on the data and other source content provided including without limitation Customer Data, and the data used to train the AI Technologies.

1.2. It is acknowledged and agreed that:

(a) Output is provided for assistance and information purposes only and does not entail or constitute legal, financial, operational or professional advice;

(b) Output is created based on a statistical analysis of the source content, without any understanding of the source content as such;

(c) all Output depends on the quality of the input data or other source content on which the Output is based, and IFS cannot have and does not accept any liability of any kind for any inaccurate or incomplete data or source content; and

(d) given the nature of AI functionality, its use may result in incorrect, incomplete, biased, unfair, unexpected or inaccurate Output, or which is otherwise unfaithful to the provided source content.

(e) Customer is solely responsible for:

(i) The accuracy and quality of Customer Data and for any Output

(ii) Having all rights, licenses and permissions needed to input Customer Data into the AI Technologies; and;

(ii) Implementing appropriate controls and human oversight for verification and validation of bias within any source content and Output (which may require obtaining professional advice as appropriate), and the reliance on, and any decision, action or omitted action based on, any Output (including deciding whether any Output is suitable for the specific purpose to which it is put).

1.3. Without prejudice to Customer's rights in Customer Data:

(a) Output may not qualify for intellectual property protection;

(b) Similar or the same Output may be produced by the SaaS in response to similar requests from different customers;

(c) Customer's rights in any Output may not be enforceable against other users of the AI Technologies; and in any event, Customer's ownership in the Output is subject to IFS and/or its licensor's ownership rights in AI Technologies, Documentation, and data used to train the AI Technologies, or any derivatives thereof ("IFS Materials"). Customer is granted a license to use, and may only use, the IFS Materials in the Output to the same extent as Customer is permitted to use the SaaS; and

(d) Subject to the foregoing, solely as between the Parties, Customer retains all ownership of Customer Data contained in the Output. IFS does not claim any ownership in the Output which Customer may own, subject at all times to IFS' retaining all rights in IFS Materials.

1.4. IFS's indemnification obligations, to the extent provided in the Agreement, shall apply to the AI Technologies, but not to the Output. IFS disclaims all liability arising from Output that infringes third party IP rights.

2. Model Training

2.1. Customer agrees that IFS may use data, including Customer Data, to train, enhance, and maintain the performance of its models and services ("**Model Training**",) subject to the provisions of these AI Terms.

2.2. If requested by the Customer, the Parties will coordinate, on the scope and nature of Customer Data used for Model Training. Customer may, with notice to IFS and subject to the exclusions within these AI Terms, opt out of the use of some / all Customer Data for model training, which opt-out may limit access to, or performance of, certain features or improvements derived from trained services.

2.3. Customer acknowledges that opt-out is not available in respect of:
(a) data used by IFS to manage its business relationship with Customer, including but not limited to for account administration and support communications (“Administrative Data”), or
(b) data generated by the SaaS or supporting infrastructure in connection with the operation, performance or security of the SaaS, including but not limited to system logs, telemetry, diagnostic data, service metadata, aggregated usage metrics, and anonymized data used to monitor, analyze, and improve the Service (“Operational Data”).

2.4. All data processing for Model Training will be conducted in compliance with applicable data protection laws and IFS’s data governance and security standards.

3. Legal Framework

Customer acknowledges that the legal framework applicable to and the interpretation of competent courts and authorities regarding the use of certain AI Technologies is evolving and may be subject to future changes. If a change in law or the interpretation of a competent court or authority results in restrictions in the use of certain technology in the SaaS, Customer accepts that the scope of use may need to be reduced or the impacted technology be amended, replaced or discontinued to address such restrictions.

4. Acceptable Use

4.1. Customer will use the AI Technologies responsibly, in a legally compliant manner and for internal business purposes only.

4.2. Customer will not:
(a) Use the AI Technologies or the Output to develop, train, or improve other AI functionality, services or AI models, unless explicitly permitted by IFS,
(b) Use web scraping, web harvesting, or web data extraction methods to extract data from the AI Technologies or Output
(c) Represent that Output was human-generated, or
(d) Input any sensitive data (being (a) special category data under the GDPR (or equivalent sensitive personal data under applicable law), (b) protected health information (including under HIPAA), (c) biometric identifiers used for the purpose of uniquely identifying an individual, (d) payment card data subject to PCI DSS, (e) government-issued identification numbers, and (f) any other data that applicable law or the Documentation designate as requiring heightened protection or restriction), personal data or images of individuals into the AI Technologies. unless expressly permitted by the Documentation and Customer has all rights, permissions and a lawful basis to do so

4.3. Customer will not circumvent measures made available by IFS or a third-party, including but not limited to those intended to help prevent copyright infringement, data breaches, or security incidents.

4.4. Customer will not process any (a) special category data under the GDPR (or equivalent sensitive personal data under applicable law), (b) biometric identifiers used for the purpose of uniquely identifying an individual, (c) payment card data subject to PCI DSS, (d) government-issued identification numbers, (e) any other data that applicable law or the Documentation designate as requiring heightened protection or restriction) or (f) health information protected by regulations that control the use of medical data by AI functionality including without limitation, the GDPR, AI Act and the Health Insurance Portability and Accountability Act (including any implementing regulations and as amended from time to time).

4.5. Certain features of the Application Software may use artificial intelligence and machine learning technologies (“AI Features”). Except as pertaining to any AI Features designed with artificial intelligence as a foundational component driving and inseparable from core functionality (“AI-Native Feature”), as so designated by IFS from time to time, use of AI Features by Customer is discretionary. Some AI Features, but not any AI-Native Feature, may be enabled or disabled by Customer within the configuration options of the Application Software.

4.6. IFS will configure the Application Software so that Outputs generated by AI Features are identified as AI-generated as legally required and, as an integral component of the AI-Native Features, will provide

visibility into the basis or reasoning underlying AI-generated recommendations. Such explanatory information is provided to support user understanding and review only and does not constitute legal, regulatory, financial or professional advice, attestation.

4.7. AI-Native Features operate within predefined functional scopes and authorization boundaries and do not independently take actions outside the permission context of the initiating user or system configuration. Any future expansion of AI-Native functionality will continue to operate subject to these constraints.

5. Data Protection and Isolation

5.1. When Customer uses AI Features, IFS will protect Customer Data processed by such AI Features using appropriate layers of technical and organizational security measures consistent with IFS's information security program and information security management system (ISMS), and, where evidenced by applicable assurance reports or certifications, aligned with applicable industry standards. Such measures may evolve over time in response to emerging threats, changes in technology, or legal and regulatory requirements.

5.2. Customer Data processed in connection with the AI Features will be logically segregated (through technical and organizational controls designed to prevent customers from accessing each other's data in a multi-tenant environment (for example, identity and access controls and tenant-level isolation), and does not necessarily imply dedicated physical infrastructure) from data of other customers. IFS will implement controls designed to prevent unauthorized cross-customer access, inference or correlation through AI Features.

6. Data Handling and Retention for AI Features

6.1. IFS will configure AI Features such that Customer Data provided to or generated by the AI Features is not stored by the AI service components beyond what is necessary to deliver, maintain and provide support for the applicable functionality and is retained only as needed for the provision of the AI Features, including (as applicable) transient processing, caching, and security and diagnostic logging in accordance with IFS's information security program and documented retention practices. For the avoidance of doubt, the persistent knowledge graph structure that constitutes the core data model of the Application Software, including all graph notes, edges, and encoded business rules maintained within Customer's private environment is part of the Application Software purchased by Customer, is deemed necessary to deliver the applicable functionality and is not subject to the retention limits in this clause.

7. Third-party services and Use of Data for Training AI Features

7.1. To the extent IFS utilizes any third-party or external AI services as part of the AI Features, IFS will implement appropriate measures designed to maintain logical segregation of Customer Data and will use commercially reasonable efforts to contractually require such third parties not to use Customer Data to train or improve their generally available models for the benefit of other customers unless otherwise specifically agreed by Customer in advance of such use.

7.2. When using third party services, temporary copies or intermediate data used for the relevant processing session will be handled in accordance with the applicable third-party service terms and IFS's information security program and will be deleted or returned (as applicable) after completion of the relevant processing session, subject to reasonable technical constraints, any legal retention requirements and third-party data retention policy. IFS may replace or modify third-party AI services where reasonably necessary to maintain security, compliance, availability or functionality of the AI Features.

7.3. Notwithstanding Section 2 (Model Training), IFS will not use Customer Data processed through the AI Features to train, retrain or otherwise improve any shared or generally available AI models, outside Customer's logically segregated, customer-specific environment, in order to benefit third parties, unless otherwise specifically stated in applicable terms or Documentation or agreed by Customer in advance of such use. For clarity, IFS may, continuously or periodically use Customer Data processed through the AI Features to train, retrain or otherwise improve the Application Software purchased by Customer, inside Customer's private environment, for Customer's benefit only, as defined and described in the relevant Documentation.

8. Access Controls and Content Filtering

8.1. IFS will maintain and enforce role-based access controls, authentication mechanisms and other technical and organizational measures designed to limit access to Customer Data processed through the AI Features to authorized personnel, systems and users. Access by IFS personnel for support, operations, maintenance and security purposes is permitted where necessary to provide the Services, subject to confidentiality obligations and access control policies consistent with IFS's information security program.

8.2. IFS will implement content filtering and other commercially reasonable safeguards designed to reduce the risk of unauthorized disclosure, leakage or misuse of Customer Data through the AI Features. Such content filtering shall be calibrated against the role-based access controls established above and is intended not to suppress or restrict outputs that are authorized by the requesting user's access permissions, including evidence chain outputs generated as part of the AI-Native Features; provided that IFS may apply filtering or other safeguards to block or limit outputs where IFS reasonably determines there is suspected abuse, prompt injection, data exfiltration patterns, policy violations, or where required to comply with law or to protect the security, availability, or integrity of the Services.

9. Monitoring, Governance and Compliance

9.1. IFS will subject the AI Features and underlying systems to regular monitoring as part of IFS's information security program and risk management processes. Monitoring activities and safeguards may be adapted over time to address new threats, legal obligations or changes in system architecture.

9.2. IFS will maintain an internal governance framework for its AI Features, including oversight by appropriate management or advisory functions, and policies and procedures designed to support responsible use of AI. IFS's information security management system is certified to ISO/IEC 27001 and IFS maintains a SOC 2 Type II report covering relevant controls, in each case as maintained and updated from time to time.