SECURITY ADDENDUM

This Security Addendum (this "**Security Addendum**") governs the security controls Pricefx applies to its Services. By (a) executing or otherwise accepting an Order Form, subscription terms governing use of the applicable Services (the "**Subscription Terms**"), a Statement of Work, or any other agreement that references this Security Addendum or (b) using applicable Services, Customer accepts and agrees to this Security Addendum. Upon acceptance, this Addendum is expressly incorporated into the Subscription Terms. If an individual accepts this Security Addendum on behalf of an entity, such individual represents and warrants that they are authorized to bind such entity to this Addendum, and such entity shall be deemed the "Customer" hereunder.

Capitalized terms used but not defined in this Security Addendum shall have the meanings assigned to them in the Subscription Terms. If not defined in the Subscription Terms, the following definitions apply:

"**Pricefx Personnel**" means all individuals involved in the performance of Services as employees, agents, or independent contractors of Pricefx.

"**Pricefx Systems**" means the information technology infrastructure used by or on behalf of Pricefx in performing the Services, including all computers, software, hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by Pricefx or through the use of third-party services.

"**Security Incident**" means any unauthorized access to or use or disclosure of any Customer Data.

Pricefx maintains appropriate technical, physical, and administrative safeguards designed to protect the security and integrity of Customer Data. These safeguards reflect industry best practices and support Pricefx's commitment to maintaining a high standard of data protection across its Services.

1. Data Security Program

Pricefx assigns to an individual or a group of individuals responsibility for developing, implementing, and managing the organization's written information security program (the "**Program**"). Pricefx takes steps to ensure that the Program is at all times sufficient to comply in all material respects with applicable law and regulation.

Relevant Pricefx Personnel are sufficiently trained, qualified, and experienced to be able to fulfill these functions and any other functions that might reasonably be expected to be carried out by Pricefx Personnel responsible for safeguarding Customer Data.

The Program includes reasonable technological, physical, administrative, and procedural safeguards, including without limitation, policies, procedures, guidelines, practices, standards and controls that are designed to:

- ensure the privacy, confidentiality, security, integrity and availability of Customer Data;
- protect against any anticipated threats or hazards to the security and integrity of Customer Data; and
- protect against any Security Incident.

Pricefx regularly tests, monitors and evaluates the sufficiency and effectiveness of the Program, including Security Incident response procedures.

Pricefx has engaged third-party providers to store data across multiple locations. Such providers are responsible for implementing security controls consistent with the Program and that at all times comply with applicable law and regulation. Pricefx's current hosting locations (including backups (DR)) are listed below:

- *EU-West-1 (Ireland) -> data recovery (DR) site is Frankfurt, DE*
- *U-Central-1 (Frankfurt, DE) -> DR site is Ireland*
- *US-East-1 (North Virginia, US) -> DR site is Oregon*
- *US-West-2 (Oregon, US) -> DR site is North Virginia*
- *AP-Southeast-2 (Sydney, AUS) -> DR site is Oregon*

2. Risk Assessment / Audit

Pricefx conducts information security risk assessments at least annually and otherwise whenever there is a material change in the organization's business or technology practices that may impact the privacy, confidentiality, security, integrity, or availability of Customer Data.

Pricefx's risk assessments include:

- identifying and assessing reasonably foreseeable internal and external threats and risks to the privacy, confidentiality, security, integrity, and availability of Customer Data;
- assessing the likelihood of, and potential damage that can be caused by, identified threats and risks;
- assessing the adequacy of Pricefx Personnel training concerning, and compliance with, the Program;
- adjusting and updating the Program to limit and mitigate identified threats and risks and to address material changes in relevant technology, business practices, personal information practices and sensitivity of information that the organization processes; and
- assessing whether the Program is operating in a manner reasonably calculated to prevent and mitigate Security Incidents.

Risk assessment is conducted internally, and all respective risks owners are involved. The sufficiency of the risk management is verified by an independent third party that provides the assurance within regular annual review.

Pricefx remediates vulnerabilities in accordance with its assessments of the applicable risks.

3. Data Collection, Retention, and Disposal

Pricefx collects only as much of Customer Data as needed to accomplish the purpose for which the information is collected and stores that data in encrypted form in a regularly backed up cloud environment.

Pricefx refrains from storing Customer Data on removable media or local hard drives.

Pricefx securely disposes of records containing Customer Data so that the information cannot be read or reconstructed after it is no longer needed to comply with business purposes or legal obligations. Retained Customer Data remains subject at all times to the Program and any binding and enforceable confidentiality and similar obligations.

4. Personnel Training and Education

Pricefx regularly and periodically trains Pricefx Personnel who have access to Customer Data or relevant information systems concerning:

- the Program;
- the importance of the security, confidentiality, and privacy of Customer Data;
- the risks to the organization and its customers associated with Security Incidents.

5. Management and Oversight

Pricefx takes reasonable steps and conducts due diligence to select and retain subcontractors that are capable of maintaining the privacy, confidentiality, security, integrity, and availability of Customer Data consistent with Pricefx's contractual and other legal obligations.
Pricefx contractually requires subcontractors to maintain adequate safeguards for Customer Data that are equivalent to the safeguards that Pricefx must implement pursuant to contractual or legal requirements but in all cases no less than the safeguards that are reasonable and appropriate considering the information processed by the subcontractor and the nature of such subcontractor's services.

6. Segregation of Duties

Duties and areas of responsibility of Pricefx Personnel are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Customer Data or the organization's information systems.

7. Access Controls

Pricefx maintains secure access to Pricefx Systems and the Subscription Services, including the following:

- Pricefx identifies Pricefx Personnel and classes of Pricefx Personnel whose documented business functions and responsibilities require access to Customer Data, relevant Pricefx Systems, and Pricefx's premises and assigns access rights individually.
- Pricefx permits access to Customer Data, relevant Pricefx Systems, and Pricefx's premises only to such authorized Pricefx Personnel.
- Pricefx maintains a current record of Pricefx Personnel who are authorized to access Customer Data, relevant Pricefx Systems, and the organization's premises, and the purposes of such access.
- Pricefx maintains physical access controls, secure user authentication protocols, secure access control methods, and firewall protection or similar compensatory controls and has password parameters in operation.
- Pricefx prevents terminated Pricefx Personnel from accessing Customer Data and Pricefx Systems by immediately terminating their physical and electronic access to Customer Data and relevant information systems.
- Pricefx enforces the above-mentioned criteria through internal company policies.

8. Secure User Authentication

To manage access to Customer Data and relevant Pricefx Systems, Pricefx:

- maintains secure control over user IDs, passwords, and other authentication identifiers;
- maintains a secure method for selecting and assigning passwords and use reasonable authentication technologies;
- assigns unique user identifications and passwords that are not vendor supplied default passwords;
- uses multi-factor authentication;
- avoids reusing or recycling old passwords;
- restricts access to Customer Data and relevant Pricefx Systems to only active users and accounts;
- block user access after multiple unsuccessful attempts to login or otherwise gain access to Customer Data or relevant Pricefx Systems.

9. Incident Detection and Response

Pricefx maintains policies and procedures to detect, monitor, document and respond to actual or reasonably suspected Security Incidents, and encourage the reporting of such incidents, including through:

- training Pricefx Personnel with access to Customer Data to recognize actual or potential Security Incidents and to escalate and notify senior management of such incidents;
- post-Security Incident review of events and actions taken concerning the security of Customer Data; and
- policies governing the reporting of Security Incidents to regulators and law enforcement agencies.

10. Encryption

Pricefx takes reasonable steps to ensure strong encryption of information:

- stored on laptops or mobile devices under the Bring Your Own Device Policy ("**BYOD**");
- stored outside of the organization's physical controls;
- transmitted across any public network (such as the Internet) or wirelessly; and
- in transit outside of the organization's information systems.

11. Malicious Code Detection

Pricefx employees must follow the BYOD requirements to ensure that all devices used in connection with Pricefx's business have software that detects, prevents, removes, and remedies malicious code designed to perform an unauthorized function on, or permit unauthorized access to, any information system, including without limitation, computer viruses, trojan horses, worms, and time or logic bombs.

12. Change Controls

Prior to implementing changes to Pricefx Systems, Pricefx assesses the potential impact of such changes on privacy, confidentiality, security, integrity, and availability of Customer Data, and determines whether such changes are consistent with the Program.

No changes are made to Pricefx Systems or the Program that, in Pricefx's reasonable belief, would increase the risk of a Security Incident or that would cause any non-compliance with Pricefx's contractual or other legal obligations.

13. Physical Security

Pricefx maintains reasonable restrictions on physical access to Customer Data and relevant Pricefx Systems. Notwithstanding the foregoing, Pricefx does not control the physical access controls imposed by third-party hosting providers or other third-party providers of Pricefx Systems.

Pricefx employees lock workstations with access to Customer Data when unattended and are required to follow the BYOD policy.

Pricefx documents repairs and modifications to information security-related physical components of Pricefx Systems.

Office facilities are secured thoroughly with anti-burglary measures and 24/7 porter service, and entrances are equipped with CCTV cameras. Visitors must always be accompanied when on company premises.

14. Contingency Planning

Pricefx maintains policies and procedures for responding to an emergency or other occurrence that can compromise the privacy, confidentiality, integrity, or availability of Customer Data or damage the organization's information systems.