THE BOARD OF THE PENSION PROTECTION FUND

ADDENDUM TO TERMS AND CONDITIONS FOR THE SUPPLY OF SERVICES TO THE PPF

INFORMATION SECURITY

Version 1.0, November 2024

This Addendum is intended to be used in conjunction with the PPF's Terms and Conditions for the Supply of Services to the PPF (the "Core Terms") and can be elected from the Order Form used to call off services under those terms.

1. Definitions

1.1. Except to the extent specified otherwise in this Addendum, defined terms will have the meanings given in the Core Terms.

1.2. Capitalised defined terms used in this Addendum have the following meanings:

(a) **HMG Baseline Personnel Security Standard** means the most up-to-date version of the HMG Baseline Personnel Security Standard published by the Cabinet Office (at the Effective Date, version 6.0, dated May 2018), as amended from time-to-time;

(b) **ICT Environment** means the information and communication technology systems used by the PPF and Supplier respectively in connection with the delivery of the Services;

(c) **Malicious Software** means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;

(d) **PPF Software** means software which is owned by or licensed to the PPF, including software which is or will be used by the Supplier for the purposes of providing the Services under the Contract but excluding the Supplier Software; and

(e) **Supplier Software** means software which is proprietary to the Supplier, including software which is or will be used by the Supplier for the purposes of providing the Services under the Contract.

2. Security Requirements

2.1. The Supplier acknowledges that the PPF places great emphasis on confidentiality, integrity and availability of information and consequently on the security of premises and information, communication and technology systems. The Supplier shall ensure that it shall at all times during the Term provide a level of security in compliance with the provisions of this clause 20.

2.2. The Supplier must obtain independent certification from a reputable and independent industry partner, to the satisfaction of the PPF, of the following (or an equivalent approved by the PPF):

(a) ISO 27001 (2013) or (2022) – Information Security Management;

(b) Cyber Essentials Plus; and

(c) Where the Services include cloud-based services, the Cloud Security Alliance Cloud Controls Matrix (CCM) STAR Level 2+.

2.3. The Supplier shall ensure that any data transfer services used in the delivery of the Services are subject to regular annual and independent technical vulnerability assessment from either CREST, TIGER or CHECK scheme assessors (or an equivalent approved by the PPF), or, a Cyber Essentials Certification Body if Cyber Essentials Plus is adopted. Identified vulnerabilities with a CVSS score of 7.0 or greater must be mitigated within 30 (thirty) calendar days of the initial finding at the Supplier's cost. If the Supplier is unable to remediate vulnerabilities within this timescale, it must notify the PPF as soon as reasonably practicable and provide all information requested by the PPF to satisfy its assurance requirements.

2.4. The Supplier shall ensure that all Supplier Personnel with regular access to PPF facilities are vetted in accordance with the HMG Baseline Personnel Security Standard (or an equivalent standard approved by the PPF) and this process must include independent verification of spent criminal convictions.

2.5. The PPF also requires the Supplier to meet the following technical security requirements:

(a) implementation of the NCSC Cloud Security Principles. Depending upon the Supplier's technical solution, exceptions to some inappropriate or irrelevant NCSC Cloud Security Principles control recommendations will be permissible subject to prior agreement with the PPF. More information about the principles can be found at:

https://www.ncsc.gov.uk/collection/cloud-security

(b) the Services must be encrypted end-to-end using x509 digital certificate based strong encryption. Certificates must be obtained from a recognised, public Certificate Authority and must support only strong encryption (as a minimum TLS 1.2, or the standard currently recommended by the National Cyber Security Centre, whichever is greater);

(c) the movement of all data including PPF data relating to the Services and any access must be logged and retained for the duration of the Contract. The Supplier must keep audit logs which are capable of identifying the time, host, user account and source/destination of any data movement or access and shall provide copies of these logs to the PPF within 10 (ten) Business Days of a request by the PPF to view them. The PPF may request the provision by the Supplier of automated or ad-hoc secure transmission of logs to the PPF, in which case the Supplier shall take all reasonable steps to provide such transmission in accordance with the above timescale.

2.6. The Supplier shall, promptly following request from the PPF, complete any security questionnaire requested by the PPF.

2.7. The PPF may appoint a third-party Supplier to conduct penetration testing against a system developed, designed or implemented by the Supplier for managing PPF Data. The Supplier shall provide all reasonable cooperation to any such appointed penetration tester.

2.8. The Supplier shall, upon receipt of reasonable notice from the PPF, permit members of PPF Personnel to undertake a site visit and/or technical security review to inspect records relating to the Supplier's compliance with this Addendum.

2.9. The Supplier shall confirm to the PPF on an annual basis that it continues to meet the information security standards required under this Addendum. Such confirmation may be given to the PPF by email to the address specified in the Order Form.

2.10. The references to standards, guidance and policies set out in this Addendum shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

2.11. In the event of any inconsistency in the standards, guidance and policies referred to in this provision, the Supplier should notify the PPF of such inconsistency as immediately upon becoming aware of the same and the PPF shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

2.12. The Supplier shall promptly notify the PPF of any material cyber-attack or security breach and shall, as soon as practicable, provide such assistance and information as the PPF reasonably requires about the cyber-attack or security breach and the action being taken by the Supplier to remedy it.

3. Malicious Software

3.1. The Supplier shall, as an enduring obligation throughout the Term of this Contract, use the latest versions of anti-virus definitions and Software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software in the ICT Environment (or as otherwise agreed by the Parties).

3.2. Notwithstanding clause 3.1, if Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software on the delivery of the Services, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of PPF Data. The Parties shall also take reasonable steps to assist each other to mitigate any losses and restore the Services to their desired operating efficiency.

3.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of clause 3.2 shall be borne by the Parties as follows:

(a) by the Supplier where the Malicious Software originates from the Supplier Software, any third-party software supplied by the Supplier or the PPF Data (whilst the PPF Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the PPF when provided to the Supplier; and

(b) by the PPF if the Malicious Software originates from the PPF Software or the PPF Data (whilst the PPF Data was under the control of the PPF).