DATA PROTECTION ADDENDUM

This DATA PROTECTION ADDENDUM ("Addendum") forms part of the Software as a Service Agreement ("Principal Agreement") between: (i) Credal.AI ("Processor" or "Service Provider" or "Provider"), having its place of business at 66 Rockwell Place, NY, 11217 and (ii) Customer ("Controller" or "Company"), having its place of business at ________________________. This Addendum is entered into and effective as of this _______ day of __________________, 2024.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

RECITALS

(A) The Company and the Provider entered into an Agreement for the provision of the Services as described in the Master Service Agreement, dated _______________ ('**Master Service Agreement**' or '**Agreement**').

(B) In the course of providing the Services to the Company pursuant to the Agreement, the Provider may process Personal Data on behalf of the Company and the parties agree to comply with the following additional terms with respect to any Processing of Personal Data ('**DPA**').

(C) Article 28.3 of the UK GDPR requires an Agreement in writing between the Data Controller and any organization which processes Personal Data on its behalf, governing the processing of that Personal Data.

(D) The Parties have agreed to enter into this Agreement to ensure compliance under the said provisions of the UK GDPR in relation to all processing of Personal Data by the Provider for the Company.

(E) The terms of this Agreement are to apply to all processing of Personal Data carried out for the Data Controller by the Provider and to all Personal Data held by the Provider in relation to all such processing.

1. OPERATIVE PROVISIONS

1.1 Definitions

In this Addendum, the following terms shall have the meanings set out below:

Data Controller	The entity which determines the purposes and means of the Processing of Personal Data as per Art. 4.7 UK GDPR / Section 6 of the Data Protection Act - 2018
Data Processor	The entity which processes Personal Data on behalf of the Controller as per Art. 4.8 UK GDPR.

Data Subject	The identified or identifiable person to whom Personal Data relates as per Art. 4.1 UK GDPR
Subprocessor	Any third party engaged by the Data Processor who has or will have access to or process personal data from a Data Controller.
Personal Data	Any information relating to an identified or identifiable natural person which is Processed by the Provider pursuant to the Agreement, as per Art. 4.1 UK GDPR. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Anonymous Data	Any information which does not relate to. an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable
UK GDPR	The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR)
Data protection Laws and Regulations	All the legislation on privacy and data protection applicable to the Processing of Personal Data under this Agreement, including - but not limited to - the UK GDPR and the data Protection Act of 2018 and all related regulations
Processing, Process, Processes, Processed	Any operation or set of operations which is performed upon Personal Data , whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, as per Art. 4.2 of UK GDPR
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed as per Art. 4.12 UK GDPR
Security Controls	The technical and organizational security measures set out in Schedule 2

Records	The written record kept by the Data Processor of all processing activities carried out on behalf of the Data Controller
Standard Contractual Clauses	The EU Commission Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
Restricted Transfer	The disclosure, grant of access, or other transfer of Personal Data by Controller to Processor, to the extent that: (i) in the context of the European Economic Area ("EEA"), Processor is located in any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission (an "EEA Restricted Transfer"); and (ii) in the context of the United Kingdom ("UK"), Processor is located in any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government (a "UK Restricted Transfer").
Supervisory Authority	An independent public authority which is established by an EU Member State pursuant to the GDPR or any other national Data Protection Legislation
Information Commissioner	The Information Commissioner as per Art. 4.21A UK GDPR / Section 114 of the Data Protection Act 2018
Services	The Services provided by the Provider pursuant to the Agreement
Processor Affiliate	Any entity that owns or controls, is owned or controlled by or is or under common control or ownership with the Processor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 Scope and Application

a) This DPA is incorporated and subject to the terms of the Master Service Agreement. This DPA shall remain in full force and effect so long as the Agreement remains in effect, or the Provider retains any Personal Data in its possession or control. Unless otherwise specified within this DPA, defined terms set forth in the Agreement shall apply to the interpretation of this DPA.

b) In the case of conflict between:

this DPA and the Agreement, the provisions of this DPA shall prevail;

this DPA and the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses shall prevail.

1. **PROCESSING OF PERSONAL DATA**

2.1 Roles of the parties

The parties acknowledge and agree that with regards to the Processing of Personal Data, the Company is the Data Controller and the Provider is the Provider. The Provider shall is only to carry out the Services and only to process the Personal Data as instructed and received from the Company:

a) strictly for the purposes of the Services under the Agreement;
b) to the extent and in such a manner as is necessary for those purpose;
c) strictly in accordance with the expressed written authorization and instructions of the Company.

2.2 Company responsibilities

The Company retains control of the Personal Data at all times and shall, in its use of the Services, Process Personal Data in accordance with the applicable requirements of Data Protection Laws and Regulations, and with respect to the written instructions given to the Provider.

2.3 Details of the Processing

The subject matter of Processing of Personal Data by the Provider is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

3. DATA PROCESSOR OBLIGATIONS

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the provision of the Services in accordance with the Company's written instructions. All instructions given by the Company shall be made in writing and shall at all times be compliant with the applicable Privacy and Data protection Regulations. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Laws and Regulations. The Provider must immediately notify the Company if, in its opinion, a Company's instruction, as varied from time to time, would not comply with the Data Protection

Laws and Regulations. The Provider shall only act under the written instruction given by the Company, unless the Provider is required by the laws to do otherwise as per Art. 29 UK GDPR; in that case the Provider shall immediately inform the Company of the legal requirement in question before processing the Personal Data for that purpose.

3.2 The Provider shall not process the Personal Data in any manner which does not comply with the provisions of this Agreement or with the applicable Data Protection Legislation. The Provider must immediately inform the Company if, in its opinion, any instruction given by the Company does not comply with applicable the Data Protection Legislation.

3.3 The Provider must immediately comply with any Company written request or instruction requiring the Provider to amend, transfer, delete or otherwise Process the Personal Data, or to stop, mitigate or remedy any unauthorized Processing involving Personal Data.

3.4 The Provider will use its best endeavors to assist the Company with meeting its compliance obligations under the applicable Data Protection Laws and Regulations, taking into account the nature of the Provider's Processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments, reporting to and consulting with Supervisory Authorities under the Data Protection Laws and Regulations, Security of Processing, Notification to Supervisory Authorities. The Provider must promptly notify the Company of any changes to Data Protection Laws and Regulations that may adversely affect the Provider's performance of the Agreement.

1.1.

4. CONFIDENTIALITY

4.1 The Provider shall maintain the Personal Data in confidence and shall not disclose the Personal Data to any third party. The Provider shall not process or make any use of the Personal Data supplied by the Company otherwise that as necessary and for the purposes of the provisions of the Services to the Company.

4.2 Nothing in this Agreement shall prevent the Provider from complying with any requirement to disclose or process Personal Data where such disclosure or processing is required by law, court or regulator. In such cases, the Provider shall notify the Company of the disclosure or processing requirements prior to disclosure or processing unless such notification is prohibited by law

4.3 The Provider shall ensure that all employees who can access and/or process any of the Personal Data provided by the Company are informed of its confidential nature and are contractually obliged to keep the Personal Data confidential, have received the appropriate training and have the appropriate skills and qualifications. The Processor shall ensure that such confidentiality obligations indefinitely survive the termination of the personnel engagement.

4.4 The Provider shall not disclose any Personal Data to any Data Subject or to any Third Party except as instructed by the Company or as required by law.

5. PROVIDER PERSONNEL

5.1 Reliability and suitability

The Provider shall take commercially reasonable steps to ensure the reliability and suitability of any Provider personnel engaged in the Processing of Personal Data.

5.2 Limitation of access

The Provider shall ensure that its personnel's access to Personal Data is limited on a need-to-know basis and only to the extent necessary for the purposes of that personnel performing their duties in relation to the Services pursuant to the Agreement.

5.3 Data Protection Officer

The Provider shall appoint a Data Protection Officer (or similar role) in accordance with Art 37 UK GDPR and shall supply the details of the DPO prior to the commencement of the processing of Personal Data provided by the Company.

6. DATA SUBJECTS RIGHTS AND COMPLAINS

6.1 The Provider shall take appropriate technical and organizational measures and provide reasonable assistance to the Company in complying with its obligations under the applicable Data Protection Legislation, regarding:

a) The Rights of the Data Subject under the applicable Data Protection Legislation, including but not limited to: the right of access. the right of rectification, the right of cancellation, the right of portability, the right to object, the right of limitation, right relating to the automated processing;

b) Compliance with notices served on the Company by any supervisory authority under the applicable Data Protection Legislation.

6.2 In the event that the Provider receives any notice, compliant or other communication relating to the Personal Data processing or to the compliance with the Data Protection Legislation, it shall immediately notify the Company.

6.3 The Provider shall promptly, and in any event no later than in 48 hours from receipt, notify the Company if the Provider receives a request from a Data Subject to exercise any of the Data Subject's rights available under Data Protection Laws and Regulations ('**Data Subject Request**'). Taking into account the nature of the Processing, the Provider shall, at no additional cost to the Company, assist the Company by appropriate technical and organizational measures, insofar as this is possible and technically feasible, for the fulfillment of the Company's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

6.4 The Provider shall cooperate with the Company and provide reasonable assistance in responding to any complaint, notice, communication, request, including:

a) providing the Company with full details of the complaint or request;
b) providing the necessary information and assistance in order to comply with a subject access request;
c) providing the Company with any Personal Data it holds in relation to a Data Subject;
d) Providing the Company with any other information requested by the Company.

7. SUB-PROCESSORS

7.1 Appointment of Sub-processors

By entering into the Agreement, the Company gives its specific written authorisation to the Provider to use the Sub-processors listed in Schedule 2.

The Provider may only authorize new Sub-processor(s) to process the Personal Data if:

a) The Company provides prior written consent prior to the appointment of each Sub-processor;

b) The Provider enters into a written contract with each Sub-processor that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organizational data security measures for complying with applicable Data Protection Legislation, and, upon the Company's written request, provides the Company with copies of such contracts;

c) The Provider maintains control over all Personal Data it entrusts to the Sub-processor. The Provider shall deemed to legally control all the Personal Data that may be at any time controlled practically by, or be in the possession of, any sub-processor appointed by it;

d) the Sub-processor complies fully with its obligations under this Agreement and under the applicable Data Protection Legislation;

e) The Sub-processor's contract terminates automatically on termination of this DPA for any reason; and

f) The Provider undertakes a data protection impact assessment when the Processing proposed to be carried out by the Sub-processor is likely to result in a high risk to the rights and freedoms of Data Subjects, and promptly makes available to the Company the results of such data protection impact assessment.

7.2 Audit

On the Company's written request, the Provider will, at no additional cost to the Company, audit a Sub-processor's compliance with its obligations regarding the Company's Personal Data and provide the Company with the audit results.

7.3 Liability

The Provider shall be liable for the acts and omissions of its Sub-processors to the same extent the Provider would be liable if performing the Services of each Sub-processor directly to the Company under the terms of this DPA.

7.4 In the event that a sub processor fails to meet its data protection obligations, the Provider shall remain fully liable to the Company for the subcontractor's compliance with its data protection obligations.

8. SECURITY, RECORD KEEPING AND AUDIT

8.1 Controls

a) The Provider shall maintain appropriate technical and organizational measures for ensuring the protection of Personal Data in its security, including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity. The measures shall be reviewed and approved by the Company and shall include - not limited to - the measures contained within the Security Controls. The Provider will not decrease the overall security of the Security Controls for the term of the Agreement (or, if longer, for the duration of any Processing activity). Also, the Provider shall inform the Company in advance of any changes to such measures.

b) The measures implemented by the Provider shall be appropriate to the nature of the Personal Data, to the harm that may result from an unauthorized or unlawful processing or accidental or unlawful loss, destruction or damage and shall have regard to the state of the technological development and the costs of implementation.

c) The measures implemented by the Provider may include pseudonymization and decryption of the Personal Data; the ability to ensure confidentiality, integrity and availability; the ability to restore availability in a timely manner in the event of an incident; a process for regularly testing, assessing and evaluating the effectiveness of the measures above.

d) The Provider shall, if requested by the Company, supply further details on the technical and organizational measures and of all the safeguards put in place.

e) The Provider shall document all the measures in place in writing and shall review them on a regular quarterly basis - as well as on a need basis - to ensure they remain suitable and up to date.

8.2 Records

a) The Provider will keep detailed, accurate and up-to-date written records regarding any Processing of Personal Data it carries out for the Company, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the Processing purposes, categories of Processing, any transfers of Personal Data to a third country and related safeguards, and details of any technical and organizational security measures ('**Records**').

b) The Provider shall make available to the Company any and all information as is required and necessary to demonstrate the Provider's compliance with the applicable Data Protection Legislation and with this Agreement.

8.3 Audits

The Provider shall make available to the Company all information necessary to demonstrate compliance with the obligations laid down in the relevant Data Protection Laws and Regulations and allow for and contribute to audits, including inspections, conducted by the Company or another auditor mandated by the Company, at no additional cost to the Company. The Company shall take all reasonable steps to minimize the disruption to the Provider's business when conducting an audit. The assistance may include, but is not limited to:

a) physical access to, remote electronic access to, and copies of any Records and any other information held at the Provider's premises or on systems storing Personal Data;

b) access to and meetings with any of the Provider's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

c) inspection of, and where applicable, taking copies of, all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data.

d) the right of Audit can be exercised on a quarterly basis and on a need basis. Audit shall be conducted prior notice (one calendar month).

The requirement for the Company to give prior notice shall not apply if the Company has reasons to believe that the Provider is in breach of any of its obligations under this Agreement or under the applicable Data Protection Legislation, or if it has the reason to believe that a Personal Data Breach has taken place or is taking place.

9. DATA INCIDENT MANAGEMENT AND NOTIFICATION

9.1 The Provider shall maintain security incident management policies and procedures and shall notify the Company without undue delay, and in any event within 24 hours after becoming aware of, any actual or potential, accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any Personal Data, which is transmitted, stored or otherwise Processed by the Provider or its Sub-processors of which the Provider becomes aware (a '**Data Incident**'). The Provider shall take all steps necessary to identify the cause of such Data Incident and remediate the cause of such a Data Incident.

9.2 The Provider shall, without undue delay and, where possible, within 24 hours after becoming aware of any Data Incident, provide the Company with the following information:

a) description of the nature of the Data Incident, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

b) the likely consequences of the Data Incident;

c) description of the measures taken, or proposed to be taken to address the Data Incident including measures to mitigate its possible adverse effects.

9.3 The Provider shall, at no additional cost to the Company, cooperate with the Company and take such reasonable steps as directed by the Company to assist in the investigation, mitigation and remediation of each Data Incident. The Provider shall not inform any third party of any Data Incident without first obtaining the Company's prior written consent, except where required to do so by law.

9.4 The Provider shall use all reasonable endeavors to restore any Personal Data lost, destroyed, damaged, corrupted and otherwise rendered unusable in the Data Incident as soon as possible after becoming aware of the data Incident.

9.5 The Company shall have the sole right to determine whether or not to notify affected Data Subjects, the Supervisory Authority of reference, law enforcement agencies, or other regulators as required by the applicable legislation, including the form of such notification.

9.6 The Company shall have the sole right to determine whether or not to offer any remedy to the involved Data Subjects, including the form and amount of such remedy.

10. RETURN AND DELETION OF PERSONAL DATA

10.1 At the Company's request, and upon termination of this DPA, the Provider shall return or securely destroy (as instructed by the Company) the Personal Data to the Company in accordance with the procedures and timeframes specified in the Security Controls (if applicable), unless otherwise required by law, within a reasonable time after:

a) the end of the provision of the Services, or;

b) the termination of the Services Agreement, or;

c) the processing of that Personal Data by the Provider is no longer required for the performance of the Provider’s obligations under this Agreement.

10.2 The Provider shall not retain all or any part of the Personal Data after deleting or returning it.

10.3 If the Provider is required to retain copies of all or any part of the Personal Data provided by the Company by law, regulation, government or other regulatory body, it shall inform the Company of such requirement in writing, including the precise details of the Personal Data that it is required to retain, the legal basis for the retention, duration of the retention, and when the retained Personal Data will be deleted once it is no longer required to retain it.

10.4 Upon the deletion or disposal of Personal Data, the Provider shall certify the completion of the same in writing to the Company.

10.5 When deleting Personal Data provided by the Company, the Provider shall:

a) physically destroy every hard-copy format when it is no longer needed; this may include shredding or disposal by an appropriate waste paper destruction Services;

b) destroy and dispose portable media and devices in a manner which ensures that any stored information is rendered unrecoverable.

11. TRANSFERS OUTSIDE THE EEA

11.1 The Provider shall not transfer or otherwise Process Personal Data outside the European Economic Area (EEA) without obtaining the Company's prior written consent.

11.2 Subcontractors appointed by the Provider shall not process or transfer Personal Data provided by the Company outside of the EEA without the Company's prior written consent.

11.3 Where such consent is granted, the Provider may only Process, or permit the Processing, of Personal Data outside the EEA if one or more of the following conditions are satisfied:

a) The Provider and, where applicable, the Sub-processor, is Processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Laws and Regulations that the territory provides adequate protection for the privacy rights of individuals; or

b) The Provider and, where applicable, the Sub-processor, participates in a valid cross-border transfer mechanism under the Data Protection Laws and Regulations, so that the Provider (and, where appropriate, the Company) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General Data Protection Regulation ((EU) 2016/679). The transfer mechanism that enables the parties to comply with these cross-border data transfer provisions is to be further detailed in Schedule 1.

11.4 In the event that any transfer of Personal Data between the Company and the Provider requires the execution of Standard Contractual Clauses (SCC) in order to comply with the Data Protection Legislation, the parties shall complete all relevant details contains in the SCC, execute the same and take any and all other actions required to legitimize the transfer of Personal Data.

11.5 In the event that the Company consents to the Provider appointing of one or more sub processors and those sub processors are located outside of the EEA, the Company hereby authorizes the Data Processo to enter into SCC with the subcontractors in the Company's name and on the Company's behalf. The Provider shall make the sais executed SCC available to the Company upon request.

12. Governing Law and Jurisdiction

12.1. The parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement; and

12.2. This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

IN WITNESS WHEREOF, the parties have executed this Data Protection Addendum as of the date first set forth above.

Credal.AI

By: ______________________________________

Name: Ravin Thambapillai

Title: CEO

Customer

By: ______________________________________

Name:

Title:

SCHEDULE 1

Services and Details of the Processing

1. Services

Credal.AI is committed to provide Customer the following services, as described in detail in Master Service Agreement: secure chat portal, Slackbot, and APIs, that ensure all data used in conjunction with Large Language Models are appropriately redacted, access controlled, and audit logged.

2. Nature and purpose of Processing

The Provider will Process Personal Data as necessary to perform the Services pursuant to the Agreement and as further instructed by the Company in its use of the Services.

3. Duration of Processing

The Provider will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

4. Retention Period

The period for which the Personal Data will be retained by the Provider is 30 days.

5. Personal Data and Data Subjects

Please note the following list in not exhaustive. Further PII might be shared only at the explicit discretion and determination of the Company.

Category of Data Subject	Type of Personal Data	Purpose(s) of processing	Duration of processing and retention period
Employees	Full name Email address	Authentication and authorization checks for the services, sending of updates around product and terms of service changes	data is retained for as long as the account is in active status. Data enters an “expired” state when the account is voluntarily closed. Expired account data will be retained for 30 days. After this period, the account and related data will be removed. Customers that wish to voluntarily close their account should download their data manually or by request to support@credal.ai

			prior to closing their account.

Obligations and rights of the parties

The rights and obligations of the Parties are detailed in the Agreement as supplemented by this DPA.

Transfers outside the EEA

Unless agreed otherwise in writing between the parties, transfers outside of the EEA shall be governed by the Standard Contractual Clauses contained in Schedule 3 and by signing this DPA the parties hereby agree to the execution of the Standard Contractual Clauses. For the purpose of the Standard Contractual Clauses, the data exporter shall be the Company and the data importer shall be the Provider.

SCHEDULE 2

Technical and Organizational Data Protection Measures and Security controls

The following are the Technical and Organizational Data protection measures referred to in this Agreement:

1. The Provider shall ensure that, in respect of all Personal Data it receives from or processes on behalf of the Company, it maintains security measures to a standard appropriate to:
   a) The harm that might result from unlawful or unauthorized processing or accidental loss, damage or destruction of the Personal Data; and
   b) The nature of Personal Data.

The Provider shall operate an information security programme designed to meet the confidentiality, integrity, and availability requirements of the Services. The program shall include at a minimum the following security measures.

Governance

1. **Information Security Policy:** The Provider shall develop, implement, and maintain an information security policy and shall communicate and enforce the policy to all staff and contractors.

2. **Information Security Accountability:** The Provider shall have an information security programme that is overseen by a designated, accountable employee of appropriate seniority.

3. **Risk Assessment & Management:** The Provider shall employ a formal risk assessment process conducted at least annually, to identify security risks that may impact the products or Services being supplied and mitigate risks in a timely manner commensurate with the risk.

Asset Management

4. **Asset Inventory:** The Provider shall maintain an inventory of all hardware and software assets, including asset ownership.

5. **Data Classification:** The Provider shall develop, implement, and maintain a data classification scheme and process designed to ensure that data is protected according to its confidentiality requirements.

Supply Chain Risk Management

6. **Supplier Security Assessments:** The Provider shall engage in appropriate due diligence assessments of potential suppliers that may impact the security of the Services or products being supplied.

7. **Security in Supplier Agreements:** The Provider shall ensure that agreements with suppliers who may impact the security of the Services or products being supplied contain appropriate security requirements.

Human Resource Security

8. **Information Security Awareness:** The Provider shall develop and implement an information security awareness program designed to ensure that all employees and contractors receive security education as relevant to their job function.

9. **Background Checks:** The Provider shall conduct appropriate background checks on all new employees based on the sensitivity of the role that they are being hired for.

Identity Management, Authentication, and Access Control

10. **Authentication:** The Provider shall ensure that all access, by employees or contractors, to its information systems, used to provide Services or supply products, shall require appropriate authentication controls that at a minimum will include:

a) Strong passwords, that adhere to industry standard best practices, eg. NIST

b) Multi-factor authentication for all remote access and internet facing systems

11. **Authorisation:** The Provider shall ensure that all access to its information systems, used to provide Services or supply products, shall be approved by management.

12. **Privileged Account Management:** The Provider shall appropriately manage and control privileged accounts on its information systems.

13. **Access Termination:** The Provider shall develop and maintain a process designed to ensure that user access is revoked upon termination of employment, or contract for contractors.

Data Security

14. **Encryption:** The Provider shall ensure that all laptops, mobile devices, and removable media, including those that are owned by The Provider employees or contractors, that may be used to store, process, or transport organizational data are encrypted at all times, in line with industry best practices using AES-256 or above encryption at rest, utilizing strong key management practices. Likewise, for data-in-transit, TLS v1.2 or above using AES-256 is implemented.

15. **Secure Disposal:** The Provider shall ensure that all media that may be used to store, process, or transport organizational data is disposed of in a secure manner.

System Acquisition, Development, and Maintenance

16. **Security Requirements:** The Provider shall ensure that information security requirements are defined for all new information systems, whether acquired or developed.

17. **Separation of IT Environments:** The Provider shall ensure that development and testing environments are separate from their production environment.

18. **Data Anonymization:** The Provider shall ensure that Customer’s data will not be used in the development or testing of new systems.

19. **Secure Coding:** The Provider shall ensure that all applications are developed with secure coding practices, including the OWASP Secure Coding Practises.

Physical and Environmental Security

20. **Risk Assessment:** The Provider shall use a formal, documented methodology and regularly conducted risk assessment to identify physical and environmental threats and implement controls to minimize the risks.

21. **Physical Controls:** The Provider shall design and implement holistic physical security controls (e.g. electronic access control system and other practical measures) to address internal and external risks to premises and information processing facilities. These controls shall be assessed at least on an annual basis.

22. **Security Perimeter:** The Provider shall define and use security perimeters to protect information processing facilities and locations storing Customer Information.

Information Protection Processes and Procedure

24. **Hardening:** The Provider shall develop and implement security configuration baselines for all information systems such as servers, network devices, laptop, and desktops.

25. **Network Segregation:** The Provider shall segregate its network into zones based on trust levels, and control the flow of traffic between zones.

26. **Anti-Malware:** The Provider shall ensure that all information systems that are susceptible to malware are protected by up-to-date anti-malware software.

27. **Wireless Access Control:** The Provider shall ensure that wireless network access is protected, including at a minimum:

a) All wireless network access should be encrypted

b) Wireless network access for personal devices and guest access should be segregated from the production network

28. **Patching:** The Provider shall evaluate, test, and apply information system patches in a timely fashion according to their risk appetite.

29. **Backup and Recovery:** The Provider shall implement a backup and recovery process designed to ensure that data can be recovered in the event of unexpected loss.

30. **Disaster Recovery and Business Continuity:** The Provider shall ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident. The vendor shall have a documented Disaster Recovery and Business Continuity guideline that has been tested at least annually.

Protective Technology

31. **Logging:** The Provider shall ensure that security event logging requirements have been defined and that all information systems are configured to meet logging requirements.

32. **Intrusion Detection:** The Provider shall deploy intrusion detection systems at the network perimeter.

33. **Intrusion Prevention:** The Provider shall deploy intrusion prevention systems at the network perimeter.

34. **URL Filtering:** The Provider shall deploy tools to limit web browsing activity based on URL categories, and monitor web traffic.

35. **Denial of Services Protection:** The Provider shall deploy controls to detect and mitigate denial of Services and DDoS attacks.

Security Continuous Assessment

36. **Security Monitoring:** The Provider shall deploy automated tools to collect, correlate, and analyze security event logs from multiple sources, and monitor them 24/7 for suspected security incidents.

37. **Vulnerability Assessments:** The Provider shall conduct vulnerability assessments against all internet-facing and internal information systems on a regular basis, no less often than monthly.

38. **Penetration Testing:** The Provider shall perform both network and web application penetration tests, in accordance with standard penetration testing methodologies, on a regular basis, no less often than annually.

Information Security Incident Management

39. **Incident Response:** The Provider shall develop, implement, and maintain an information security incident response process and will test the process on a regular basis, no less often than annually.
Have in place methods for detecting and dealing with breaches of security, including:

a) the ability to identify which individuals have worked with specific Personal Data;
b) having a proper procedure in place for investigating and remedying breaches of the personal protection legislations;
c) notifying the Company as soon as any such security breaches occur.

Adopt such organizational operational and technological processes and procedures as are required to comply with the requirements of ISO/IEC 270001:2013 as appropriate to the Services provided to the Company.

If there aren't any security certifications in place, then one of the following should be done within a reasonable time frame (e.g. 1 year). In case the company already has the certification then we would expect them to maintain it and let us know in case they decide to stop following an information security framework:

- ISO27001
- SOC 1 & 2
- PCI DSS
- NIST

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is Personal Data received from the Importer combined with Personal Data collected by the Exporter?
1						
2	x	yes	yes	Specific	1 calendar month	

3						▨
4				▨	▨	

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name:	Customer
Address:	
Contact person's name, position and contact details:	
Activities relevant to the data transferred under the Clauses:	For the Services as specified in the Principal Agreement.
Signature and date:	
Role (controller/processor)	Controller

Data importer(s):

Name:	Credal.AI Corporation
Address:	66 Rockwell Place, NY, 11217
Contact person's name, position and contact details:	Ravin Thambapillai CEO ravin@credal.ai
Activities relevant to the data transferred under the Clauses:	For the Services as specified in the Principal Agreement.
Signature and date:	
Role (controller/processor)	Processor

B. DESCRIPTION OF THE TRANSFER

As set out in Schedule 1 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

- The UK Information Commissioner's Office