11:11 SYSTEMS

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is entered into by and between Provider and Customer. This DPA amends and forms part of the Master Services Agreement or other written agreement between the parties (the "**Agreement**"). This DPA applies where Provider Processes Customer Personal Information as a Processor on behalf of Customer, the Controller, in connection with providing the Services. This DPA will be effective as of the effective date of the Agreement. This DPA will terminate automatically upon termination of the Agreement or as earlier terminated pursuant to the terms of this DPA.

1. DATA PROCESSING AND PROTECTION

1.1. **Limitations on Use.** Provider will Process Customer Personal Information only: (a) in a manner consistent with Customer's documented instructions as specified under Section 1.2 (Instructions), including with regard to transfers of Customer Personal Information to a third country; and (b) as required by applicable laws, provided that Provider will inform Customer (unless prohibited by law) of the applicable legal requirement before Processing pursuant to such law if such Processing would be inconsistent with Customer's instructions. Provider will not: (x) retain, use, or disclose the Customer Personal Information (i) outside of the direct business relationship between the parties or (ii) for any purpose other than for the specific purpose of performing the Services, including retaining, using, or disclosing the Customer Personal Information for a commercial purpose other than providing the Services; (y) sell or share (as defined by Data Protection Law) the Customer Personal Information; or (z) combine Customer Personal Information with Personal Information Provider receives from other sources, except as permitted by Data Protection Law.

1.2. **Instructions**. Customer instructs Provider to Process Customer Personal Information as necessary to provide the Services and as otherwise authorized or permitted under this DPA and the Agreement, including as specified in Attachment 2 (Scope of Processing). This DPA, the Agreement, and any instructions provided by Customer through configuration tools made available by Provider constitute Customer's documented instructions regarding Provider's Processing of Customer Personal Information. Additional instructions provided by Customer (if any) require prior written agreement by Customer and Provider, including agreement on any additional fees to carry out such instructions. Customer will not instruct Provider to perform any Processing of Customer Personal Information that violates any Data Protection Law. Provider may suspend Processing based upon any Customer instructions that Provider reasonably suspects violate Data Protection Law, provided Provider will promptly inform Customer if, in Provider's opinion, an instruction infringes Data Protection Law.

1.3. **Compliance.** Each party will comply with its obligations under Data Protection Law. Provider shall notify Customer if it determines that it cannot meet its obligations under Data Protection Law. Upon receiving written notice from Customer that Provider has Processed Customer Personal Information without authorization, Provider will take reasonable and appropriate steps to stop and remediate such Processing.

1.4. **Confidentiality.** Provider will ensure that persons authorized by Provider to Process any Customer Personal Information are subject to appropriate confidentiality obligations.

1.5. **Security.** Provider will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Information against Security Incidents

and provide the level of protection required by Data Protection Law as described in Attachment 3 (Data Security Exhibit). Provider may amend the technical and organizational measures, provided such amendments do not reduce the level of security provided by the measures described in Attachment 3 (Data Security Exhibit).

1.6. **Disposal.** At the choice of Customer, Provider will (or will enable Customer via the Services to) delete (and will delete existing copies of) all Customer Personal Information after the end of the provision of Services (unless Data Protection Law requires the storage of such Customer Personal Information by Provider, in which case Provider will only retain and Process such Customer Personal Information for the limited duration and purposes required by such Data Protection Law). The certification of deletion contemplated by Section 8.5 of the SCCs shall be provided on Customers' written request.

2. DATA PROCESSING ASSISTANCE

2.1. **Data Subject Rights Assistance**. Customer shall be responsible for responding to requests from Data Subjects to exercise rights under Data Protection Law relating to Customer Personal Information (each a "**Data Subject Request**"). Provider will, to the extent permitted by Data Protection Law, notify Customer without undue delay if Provider receives a Data Subject Request. To the extent Customer does not have the ability to address the Data Subject Request through the Services, Provider will, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent the response to such Data Subject Request is required under Data Protection Law and Customer has provided the information necessary for Provider to assist.

2.2. **Security Assistance.** Taking into account the nature of Processing and the information available to Provider, Provider will provide commercially reasonable efforts to assist Customer in Customer's efforts to comply with Customer's obligations to secure Customer Personal Information by providing the information and assistance described in Section 3 (Audits).

2.3. **Security Incident Notice and Assistance.** Provider will notify Customer without undue delay after becoming aware of a Security Incident. Provider will take commercially reasonable steps to mitigate the effects and minimize any impact from the Security Incident. Taking into account the nature of Processing and the information available to Provider, Provider will assist Customer in ensuring compliance with Customer's notification obligations imposed under Data Protection Law in connection with any Security Incident.

2.4. **Data Processing Impact Assessment ("DPIA") and Prior Consultation Assistance**. Taking into account the nature of Processing and the information available to Provider, Provider will provide commercially reasonable efforts to assist Customer in ensuring compliance with the obligations related to DPIAs and consulting with regulatory authorities.

3. AUDITS

3.1. **General Assistance.** Subject to Section 3.3 (Customer Audits), Provider will make available to Customer information necessary to demonstrate compliance with its obligations in this DPA. Any such information or results of audits will be deemed the Confidential Information of Provider under the Agreement.

3.2. **Provider Reports**. Provider may procure summaries of independent audits by third parties to assess Provider's adherence to the following standards or requirements: (a) SOC 2 Type II (or reports or other documentation describing the controls implemented by Provider that replace or are substantially equivalent to SOC 2 Type II); (b) ISO 27001 or 27701 (or certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001 or 27701); and/or (c) certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to the foregoing (collectively, "**Reports**"). If Provider obtains such Reports, Provider will provide Customer, subject to the confidentiality obligations set forth in the Agreement, with a copy of Provider's then-current Reports in response to Customer's reasonable request no more than once per year.

3.3. **Customer Audits.** Customer agrees to exercise its audit rights by first requesting the Reports as described in Section 3.2 (Provider Reports). Customer will only request additional information or an on-site audit of Provider to the extent the Reports are not reasonably sufficient to enable Customer to evaluate Provider's compliance with this DPA and/or Data Protection Law. Except in the event of a Security Incident or regulatory investigation, Customer will provide no less than 30 days' advance notice of its request for an on-site audit and will cooperate in good faith with Provider to schedule any such audit on a mutually agreed upon date and time (such agreement not to be unreasonably withheld by either party). Any such on-site audit must (1) occur no more than once per year during Provider's normal business hours, (2) be limited in scope to any deficiencies identified in the Reports or any aspects of Provider's Processing of Customer Personal Data not covered by the Reports, and (3) be conducted by Customer or a nationally recognized independent auditor. In connection with conducting the audit, Customer and/or its auditor must: (a) comply with reasonable and applicable on-site policies and procedures provided by Provider, (b) sign a standard confidentiality agreement with Provider, and (c) not unreasonably interfere with Provider's business activities. Customer will provide a written summary of any audit findings to Provider, and the results of the audit will be the confidential information of Provider.

4. SUBPROCESSORS

4.1. **Appointment of Subprocessors.** Customer authorizes Provider to use subcontractors to Process Customer Personal Information in connection with providing the Services (each, a "**Subprocessor**"). Customer specifically consents to Provider's appointment of the Subprocessors identified at https://1111systems.com/1111-subprocessors/ (the "**Subprocessor List**") which may be updated from time to time at Provider's sole discretion. Unless otherwise required by applicable Data Protection Law, Customer shall be notified of such changes by monitoring the Subprocessor List made available online or upon request.

4.2. **Objection Right for New Subprocessors.**

4.2.1. Where required by applicable data protection laws, Provider will notify Customer of its intent to update the Subprocessor List at least 15 days prior to engaging a new Subprocessor. Customer may object to Provider's use of a new Subprocessor within 10 days of receiving such notice by sending an e-mail to privacy@1111systems.com clearly indicating its desire to object to any such change.

4.2.2. If Customer objects to the change in Subprocessors, Provider and Customer will cooperate in good faith to resolve Customer's objection. If the parties unable to

resolve Customer's objection within 10 days, then either party may terminate the Agreement only with respect to those Services that Provider indicates cannot be provided without the objected-to Subprocessor.

4.3. **Liability.** Provider will impose data protection obligations upon any Subprocessor that are no less protective of Customer Personal Information than those included in this DPA. Provider will remain liable to Customer for any breach of such obligations by its Subprocessors as it would for its own acts and omissions.

5. DATA TRANSFERS

5.1. **Overview.** The transfer of EEA, UK, and Swiss residents' Customer Personal Information to a country not subject to an adequacy decision (a "**Data Transfer**") will be subject to the SCCs, which are incorporated by this reference and deemed executed as of the effective date of this DPA. If an alternative transfer mechanism for legitimizing Data Transfers (an "**Alternative Mechanism**") becomes available during the term of this DPA, and Provider notifies Customer that Data Transfers can be conducted in compliance with Data Protection Law pursuant to the Alternative Mechanism, the parties will rely on the Alternative Mechanism to legitimize Data Transfers instead of the provisions that follow.

5.2. **SCCs.** The parties agree to comply with the general clauses and with Module 2 (Controller to Processor) of the SCCs with Customer as the "data exporter" and Provider as the "data importer." The parties agree to implement the SCCs as follows:

5.2.1. In Clause 7, the optional docking clause will apply.

5.2.2. The audits contemplated by Section 8.9 of the SCCs shall be conducted according to the audit provisions of this DPA.

5.2.3. In Clause 9, Option 2 will apply and the time period for notice of Subprocessor changes will be as set forth in this DPA.

5.2.4. In Clause 11 the optional language will not apply.

5.2.5. In Clause 17, the SCCs shall be governed by the laws of Ireland.

5.2.6. In Clause 18(b), the parties agree to resolve disputes arising from the SCCs in the courts of Ireland.

5.2.7. The information needed to complete the annexes of the SCCs is provided in the attachments to this DPA.

5.3. **Data Transfers Subject to Swiss Data Protection Law.** For Data Transfers subject to the Swiss Federal Act on Data Protection of 19 June 1992 (the "**FADP**"), the parties agree to modify the SCCs as follows: the competent supervisory authority shall be the Federal Data Protection and Information Commissioner; references to a "Member State" and "EU Member State" will not prevent data subjects in Switzerland from suing for their rights in Switzerland; and references to "GDPR" will be understood as references to the FADP.

5.4. **Data Transfers Subject to the UK GDPR.** For Data Transfers subject to the UK GDPR, the UK IDTA, which is incorporated by this reference and deemed executed as of the effective date of this DPA, will supplement the SCCs. Neither party can terminate the UK IDTA

pursuant to Table 4 and Section 19 thereof without the written consent of the other. The information needed to complete the tables to the UK IDTA is provided in the attachments to this DPA.

6. LIMITATION OF LIABILITY

Each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability in the Agreement. Nothing in this Section 6 is intended to restrict the rights of data subjects under Data Protection Law.

7. MISCELLANEOUS

To the extent there is any conflict between the terms of this DPA, and the applicable SCCs or UK IDTA, the SCCs or UK IDTA, as appropriate, will control. Except as specifically amended and modified by this DPA, the terms and provisions of the Agreement remain unchanged and in full force and effect. Except as expressly stated in the SCCs and the UK IDTA, the governing law clause and forum selection clause of the Agreement will apply to any disputes arising out of this DPA. No supplement, modification, or amendment of this DPA will be binding unless executed in writing by each party to this DPA.

Attachment 1: Definitions

For purposes of this DPA, the following terms will have the meaning ascribed below:

"**CCPA**" means the California Consumer Privacy Act of 2018, including (a) as amended by the California Privacy Rights Act of 2020 or otherwise and (b) any regulations promulgated thereunder.

"**Controller**" means "controller" and "business" (and analogous variations of such terms) under Data Protection Law.

"**Customer Personal Information**" means Personal Information described in Attachment 2 that Provider Processes on behalf of Customer in connection with providing the Services.

"**Data Protection Law**" means the GDPR, the UK GDPR, the FADP, the CCPA, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Virginia Consumer Data Protection Act, the Utah Consumer Privacy Act, and any other state, federal, or international data protection or privacy laws that apply to Provider's Processing of Customer Personal Information pursuant to the Agreement.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Personal Information**" means "personal data" and "personal information" (and analogous variations of such terms) under Data Protection Law.

"**Process**" means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated 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, extending further to such operation or operations under Data Protection Law.

"**Processor**" means "processor" and "service provider" (and analogous variations of such terms) under Data Protection Law.

"**SCCs**" means Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914, as may be replaced or superseded by the European Commission.

"**Security Incident**" means "personal data breach" and "security incident" (and analogous variations of such terms) under Data Protection Law.

"**Services**" means the services provided by Provider pursuant to the Agreement.

"**UK GDPR**" means the GDPR as incorporated into United Kingdom law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (each as amended, superseded, or replaced).

“**UK IDTA**” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

Attachment 2 - Scope of Processing

Data exporter

Customer

Data importer

Provider

Subject-Matter and Duration of Processing

Provider Processes Customer Personal Information if and when provided by Customer in the course of providing the Services in accordance with the Agreement and until the Agreement terminates or expires.

Nature and Purpose of Processing

Processing of Customer Personal Information in connection with and for the purpose of Provider providing the Services to Customer pursuant to the Agreement. Specifically, the Customer Personal Information will, if and to the extent Customer provides it, be subject to storage and analysis, among other Processing activities.

Types of Customer Personal Information

Customer may submit Customer Personal Information to the Services, the extent of which is determined and controlled by Customer in its sole discretion. This may include, but is not limited to the following categories of data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data

Categories of Data Subjects

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's users authorized by Customer to use the Provider's services

Special Categories of Data (as applicable)

The Services are not designed for special categories of Personal Information. Provider does not anticipate that Customer will submit special categories to the Services. To the extent that

such data is submitted to the Services, it is determined and controlled by Customer in its sole discretion.

Frequency of Transfers

Provider will import Customer Personal Information on a continuous basis.

Period of Data Retention

Provider will retain the Personal Information until the termination of the Agreement, unless otherwise agreed to by the parties.

Identity of Subprocessors

As described in the Subprocessor List.

Attachment 3 - Data Security Exhibit

The Provider has implemented the following appropriate technical and organizational security measures - this list is not exhaustive:

I. Asset Management

- A. Asset management processes
- B. Equipment and media disposal processes
- C. Service asset and configuration management

II. Availability

- A. 24x7x365 global customer support
- B. 100% uptime guarantee in accordance with Service Level Agreements (SLAs)
- C. Antivirus/firewall systems
- D. Business continuity procedures
- E. Disaster recovery objectives
- F. High availability network with diverse and redundant Tier 1 telecommunications providers
- G. Redundant enterprise class firewalls to provide security from external threats
- H. Redundant power with diverse A+B Uninterruptible Power Supply (UPS) conditioned power with backup generators on every device with N+1 redundancy;
- I. Server farm with multiple virtualization-optimized servers with redundant power and hard drives;

III. Data transfer

- A. Use of encrypted private networks for data transfers
- B. Use of encryption technologies to protect customer data at rest and in transit
- C. Virtual private network (VPN) for remote access

IV. Human Resource Security

- A. Acceptable use policy
- B. Access termination process
- C. Appropriate employee references and background checks
- D. Employee handbooks
- E. Information security training program

F. Required confidentiality agreements with employees and contractors

V. Logical Security

A. Access rights defined according to duties

B. Access to systems subject to approval processes

C. Password controls (including, as appropriate, minimum length, use of special characters, forced change of passwords on a regular basis)

D. Periodic review of access rights

E. Principle of least privilege

F. Provider does not have access to Personal Information stored within Provider's Secure Cloud Environment

G. Secure network design

H. Segregation of duties

I. Two-factor authentication

VI. Logging & Monitoring

A. Audit trails

B. Capacity management

C. Clock synchronization

D. Intrusion detection system (IDS) and intrusion prevention system (IPS) alerts

E. Ongoing monitoring of system and network health and proactive hardware replacement support consistent secure operation of infrastructure components

F. Patch management

G. Penetration testing

H. System logging and monitoring

I. Vulnerability management

VII. Organizational Measures

A. Backup and restoration procedures

B. Change management, i.e., change development, documentation, testing, and approval requirements

C. Communication of status updates

D. Dedicated in-house compliance team

E. Defined information security roles and responsibilities

F. Incident communication and response process
G. Internal audit program
H. Risk management program
I. Timely investigation and response to customer problems based on criticality
J. Vendor evaluation, selection, and assessment due diligence processes

VIII. Physical Security

A. Access control system
B. Alarm system, video/CCTV monitoring system
C. Biometric and key card (color-coded) security
D. Dual authentication entry into building and data halls
E. Information security and physical security policy
F. Logging of facility exits/entries
G. On-site security guards 24x7x365
H. Perimeter fence

The appropriate technical and organizational security measures implemented by the Provider shall be audited by third parties on an annual basis. Such audits shall result in the Provider achieving a SOC2 Type 2 report, an ISO 27001 report, or an industry accepted successor to such reports, and any reports achieved shall be made available to the Customer through either the submission of a request by the Customer to the Provider for such reports or through the Provider's console services.