

ELITE DATA PROCESSING ADDENDUM (DPA)

LAST UPDATED: JULY 1, 2025

This Data Processing Addendum ("DPA") forms part of the Elite Master Terms agreed to by and between Elite and Customer (each as defined in the Elite Master Terms, and as further defined in the Elite Master Terms, the "Agreement") and is subject to the Agreement.

1. Definitions. The following definitions apply in this DPA. In cases where a capitalized word or phrase is not defined in this Section but is defined in the Agreement, the appropriate definitions from the Agreement are hereby incorporated by reference into this DPA.

1.1 **"Applicable Privacy Law"** means all applicable national, federal, state or local laws relating to the protection of Personal Information as amended, updated or replaced from time and time and which apply to Customer or Elite in the processing of Customer Personal Information in the circumstances governed by this DPA, including but not limited to: (a) the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, et seq. as amended by the California Privacy Rights Act ("CPRA") and implementing regulations, (collectively, the "CCPA"); (b) EU Regulation (EU) 2016/679 ("General Data Protection Regulation", "GDPR"); and (c) the United Kingdom GDPR as transposed into national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (UK GDPR) and the Data Protection Act 2018.

1.2 **"Controller"** means the entity that determines the purposes and means of the Processing of Customer Personal Information and also includes "Business" and/or similar terms as used under Applicable Privacy Law.

1.3 **"Data Subject"** means an identified or identifiable natural person, or, where required by Applicable Privacy Law, Household. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as name, an identification number, location data, an online identifier, or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

1.4 **"Customer Personal Information"** means Personal Information of Customer that is processed by Elite on behalf of the Customer to perform the Services under the Agreement.

1.5 **"EU Restricted Transfer"** means a transfer of Customer Personal Information from the European Economic Area ("EEA"), Brazil, Switzerland, or any other country (excluding however a UK Restricted Transfer) in circumstances where such transfer would, in the absence of additional protections, be prohibited by Applicable Privacy Law.

1.6 **"Household"** means a group of people who: (1) cohabit with one another at the same residential address, (2) share use of a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier, or as such term has been otherwise defined by Applicable Privacy Law.

1.7 **"Personal Information"** or **"Personal Data"** means any personal information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, or is linkable, directly or indirectly, with a particular Data Subject.

1.8 **"Process"** or **"Processing"** means any operation or set of operations which is performed on Customer Personal Information, whether or not by automated means, including collecting, recording, organizing, structuring, storing, analyzing, adapting, altering, retrieving,

consulting, using, sharing, disclosing, transmitting, transferring, disseminating, otherwise making available, aligning, combining, restricting, erasing, or destroying that Personal Information.

1.9 **"Processor"** means the entity which Processes Customer Personal Information on behalf of the Controller, including, as applicable, any "service provider" as the term is defined by the Applicable Privacy Law.

1.10 **"Restricted Transfer"** means an EU Restricted Transfer or a UK Restricted Transfer.

1.11 **"Security Controls"** means the technical and organizational measures set out in Exhibit 3.

1.12 **"Security Breach"** means a breach of security leading to actual unauthorized access, loss, disclosure, use, destruction, or alteration of Customer Personal Information without lawful authority where such breach of security results in a significant risk of harm to a Data Subject.

1.13 **"Services"** means the services provided to the Customer by Elite pursuant to the Agreement.

1.14 **"Standard Contractual Clauses" or "SCCs"** are the standard contractual clauses as adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal information to third countries pursuant to Regulation (EU) 2016/679 including their appendices and with the relevant Modules and Options set out under Section 5 of this DPA incorporated, or their successor as adopted by the European Commission and where applicable, as modified by the UK Addendum.

1.15 **"UK Addendum"** means the addendum to the SCCs covering the transfer of Personal Information from the United Kingdom ("**UK**") to third countries as approved by the UK's Information Commissioner's Office and incorporating:

- a. the party details as set out in Part 2 of Exhibit 2 to this DPA, inserted in Table 1 (Parties) of such UK Addendum;
- b. the first option in Table 2 of such UK Addendum to clarify that the UK Addendum incorporates the Standard Contractual Clauses;
- c. the list of parties and the description of the transfer of Personal Information, each as set out in Part 2 of Exhibit 2 to this DPA, inserted in Table 3 (Appendix Information) of such UK Addendum;
- d. the Security Controls and the list of sub-processors as referenced in Section 10 of this DPA inserted in Table 3 (Appendix Information) of such UK Addendum; and
- e. the option "neither party" set out in Table 4 of such UK Addendum.

1.16 **"UK Restricted Transfer"** means a transfer of Customer Personal Information from the United Kingdom in circumstances where such transfer would, in the absence of additional protections, be prohibited by Applicable Privacy Law.

2. Compliance and Roles.

2.1 For the purposes of this DPA, the Customer is the "Controller" of the Customer's Personal Information and Elite is the "Processor" of such data, except when the Customer acts as a processor of the Customer's Personal Data, in which case Elite is a "sub-processor".

2.2 Each Party shall comply with its respective obligations under Applicable Privacy Law when Processing Customer Personal Information.

2.3 Customer warrants that: (i) the Processing of the Customer's Personal Data is based on legal grounds for processing, as may be required by Applicable Data Protection Laws and that it has made and shall maintain throughout the term of the Agreement all necessary rights, permissions, registrations and consents in accordance with and as required by Applicable Privacy Laws with respect to Elite's Processing of the Customer's Personal Data under this DPA and the Principal Agreement; (ii) it is entitled to and has all necessary rights, permissions and consents to transfer the Customer's Personal Data to Elite and otherwise permit Elite to Process the Customer's Personal Data on its behalf, so that Elite may lawfully use, process and transfer the Customer's Personal Data in order to carry out the Services and perform Elite other rights and obligations under this DPA and the Agreement; (iii) it will inform its Data Subjects about its use of Processors in Processing their personal data, to the extent required under Applicable Privacy Laws; and, (iv) it will respond in a reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the Processing of their personal data, and to give appropriate instructions to Elite in a timely manner.

2.4 In addition, Customer will ensure that all Customer Personal Information is accurate, and where appropriate kept up to date; and will notify Elite if it becomes aware that any Customer Personal Information is inaccurate. Except as required under Applicable Privacy Law, Customer acknowledges and agrees that Elite is under no duty to independently collect consent from or provide notice to any Data Subjects or to investigate the completeness, accuracy or sufficiency of any specific Customer instruction or Customer Personal Data.

3. Purpose Limitation and Responsibilities.

3.1 Elite shall Process Customer Personal Information only in accordance with Customer's instructions, including those set forth in this DPA and the Agreement (the "Purpose") unless otherwise required by Applicable Privacy Law. Elite shall not sell or share Customer Personal Information as the terms "sell" and "share" are defined by CCPA or analogous provisions of Applicable Privacy Law. Elite shall only disclose Customer Personal Information to third parties as permitted under this DPA, including Sections 5 (Restricted Transfers), 10 (Sub-processors) and 11 (Audits).

3.2 Each party will (i) inform the other if, in its reasonable opinion, an instruction infringes on its own obligations under Applicable Privacy Law or other laws, and (ii) upon reasonable request, provide assistance required under Applicable Privacy Law with respect to data protection impact assessments, consulting with relevant data protection authorities, and/or making available relevant information necessary to demonstrate compliance with Applicable Privacy Law.

4. International Customer Personal Information and Restricted Transfers.

4.1 Elite will Process Customer Personal Information only in the jurisdictions where Elite or its affiliates operate or as otherwise necessary or required to provide, support and otherwise maintain the Services.

4.2 Elite will not transfer Customer Personal Information (or permit Customer Personal Information to be transferred) from any national jurisdiction to any other national jurisdiction (the EEA constituting a single jurisdiction for this purpose), unless (i) it has first obtained Customer's prior written consent (such consent not to be unreasonably withheld, conditioned or delayed); (ii) it takes any such measures as are necessary to ensure the transfer is in compliance with Applicable Privacy Laws; or (iii) otherwise provided in this DPA in connection with its provision of the Services to the Customer.

4.3 In the event of any EU Restricted Transfer involving Customer Personal Information subject to this DPA, it shall be subject to the Standard Contractual Clauses and the Parties hereby enter into such Standard Contractual Clauses incorporating: (i) the general Clauses (*Clauses 1-6*); (ii) Modules 1 (*Transfer Controller to Controller*), 2 (*Transfer Controller to Processor*) and 4 (*Transfer Processor to Controller*) as applicable in accordance with Part 1 of Exhibit 2 to this DPA; (iii) the relevant Options set out in Part 1 of Exhibit 2 to this DPA; and (iv) with the Annexes populated as set out below:

- a. Annex I of the Standard Contractual Clauses shall be pre-populated with the details set out in Part 2 of [Exhibit 2](#) to this DPA; and
- b. Annex II of the Standard Contractual Clauses shall be pre-populated with the details set out in to this DPA.

4.4 In the event of any UK Restricted Transfer between the Parties, this shall be subject to the UK Addendum incorporating the Standard Contractual Clauses and the Parties hereby enter into such UK Addendum which shall come into effect upon the commencement of any UK Restricted Transfer.

4.5 To the extent that the terms of any of the additional contractual protections referred to in this Section 4 of this DPA (the "**Transfer Contractual Clauses**") conflict with the other terms of this DPA, the Transfer Contractual Clauses shall take precedence.

5. Retention, Deletion and/or Return of Customer Personal Information.

5.1 Unless otherwise permitted by Applicable Laws, Elite shall not retain Customer Personal Information for longer than necessary for the Processing set forth under this DPA.

5.2 Upon Customer's request, Elite shall delete all Customer Personal Information in its possession or control, except to the extent required by Applicable Privacy Law or for Elite's archival purposes, including: (i) to enable Elite to comply with its professional standards requirements and substantiate any applicable work product, or (ii) with respect to backup media for which selective deletion of files is not feasible.

6. Cooperation and Data Subject Rights.

6.1 Elite shall provide legally required notice and cooperation (taking into account the nature of the Processing and insofar as is possible by using appropriate technical and organizational measures) to Customer to enable Customer as a Controller to promptly respond to: (i) a request from a Data Subject to exercise their rights under Applicable Privacy Law such to access, correct, delete or cease processing of data; and (ii) any other inquiry or complaint received from a Data Subject, regulator, governmental agency, law enforcement authority, or other third party requesting Customer Personal Information and/or otherwise in connection with the Processing of Customer Personal Information which Customer is legally required to respond to under Applicable Privacy Law.

7. Privacy Impact Assessment.

7.1 If Elite believes or becomes aware that its Processing of Customer Personal Information is likely to result in a high risk to the data protection rights and freedoms of Data Subjects as prescribed under Applicable Privacy Law, it shall inform Customer. Upon a verifiable Customer request, Elite shall, taking into account the nature of the Processing and the information available, provide Customer with reasonable assistance as legally required in order to conduct a privacy impact assessment and, if necessary, consult with any relevant data protection authority.

Any such assistance shall be solely at Customer's expense to the extent permitted by Applicable Privacy Law.

8. Security.

8.1 General. Elite has implemented, and shall maintain throughout the duration of this DPA, commercially reasonable administrative, technical, organizational, and physical measures as further set out in **EXHIBIT 3**, which include measures intended to protect Elite's customers' Personal Information from (i) unauthorized, accidental or unlawful destruction, (ii) loss, misuse, alteration, unauthorized disclosure of, or access, or (iii) other unlawful Processing of customers' Personal Information. The parties agree that measures outlined on Exhibit A attached hereto are in scope and fulfill the obligations of this section and at a minimum comply with Applicable Privacy Law.

8.2 Security Breach. Elite will notify the Customer without undue delay if Elite becomes aware of a Security Breach affecting Customer Personal Data. Elite will, taking into account the nature of the processing and the information available to Elite, use commercially reasonable efforts to provide Customer with sufficient information to allow the Customer, at its cost, to determine whether data breach notifications are required or otherwise appropriate and to make any such notifications in accordance with the requirements of Applicable Privacy Law. Elite shall not communicate with any third party (including affected Data Subjects) regarding any Security Breach without Customer's prior written approval, unless otherwise required by law, as determined by Elite. Notwithstanding the preceding sentence, Elite is not restricted from providing information (A) to law enforcement, legal counsel, insurers, advisers, regulators, or Elite's forensic or other consultants investigating the incident, (B) to affiliates of Elite for the purpose of managing the Security Breach, and (C) to other customers impacted by the same incident (so long as Customer is not identified to such other customers).

9. Sub-processors and Authorized Individuals.

9.1 Customer hereby gives a general authorization to Elite to appoint sub-processors in accordance with this Section 9 of this DPA. Elite shall ensure that all sub-processors are subject to a written agreement imposing obligations substantially similar to those imposed on Elite under this DPA. Customer also gives specific authorization to Elite to continue to use those sub-processors already engaged at the date of this DPA, as referenced in this Section 9.1. Upon request of the Customer, Elite will provide a list of sub-processors or make available a link to an online list of its sub-processors. Upon receiving such list, Customer may object to Elite's appointment of a third party sub-processor solely on grounds relating to the protection of the Customer Personal Information. If such an objection is raised within 10 days of notice of the appointment or replacement of a sub-processor, in which case and to the extent reasonable, Elite will endeavor to give Customer an opportunity to pay for the Service without use of the objectionable sub-processor or terminate, subject to the terms of the Agreement, the specific Service(s) affected by the sub-processor at issue.

9.2 Notwithstanding anything contained in Section 4.1, Customer acknowledges and confirms that Elite may transfer Customer Personal Information to: (i) its sub-processors (whether affiliates or external third parties) wherever situated for the limited purposes of performing the Services under the Agreement, and (ii) its affiliates and its processors wherever situated for purposes of administration, support and back-up, provided that in relation to such transfers, Elite, in compliance with the provisions of Applicable Privacy Law, has established safeguards to protect Customer Personal Information so transferred, including by way of Transfer Contractual Clauses where necessary.

9.3 Elite will remain primarily liable for any acts or omissions of its sub-processors in the same manner as for its own acts or omissions under the Agreement.

9.4 Elite shall ensure that any personnel that it authorizes to Process Customer Personal Information are (i) subject to a duty of confidentiality (whether a contractual duty or a statutory duty), (ii) Process Customer Personal Information only as permitted by this DPA, and (iii) receive appropriate security and privacy training regarding their duties.

10. Anonymized, De-identified, and Pseudonymized Data.

10.1 Customer acknowledges and agrees that the Services may include pseudonymization, de-identification, and anonymization of data (meaning data that cannot reasonably be used to infer information about, or otherwise be linked to, a particular Data Subject or Household, including de-identified and aggregated Customer Personal Data) for the purpose of aggregate reporting and (trends) research, that such data is not Personal Information under Applicable Privacy Law and that Elite may use pseudonymized, de-identified, and anonymized data for its own business purposes, including, but not limited to, providing the Services, improving its operations, and research and enhancing the features, functions, and performance of the Services and/or data purposes, provided, however, Elite will comply with all Applicable Privacy Laws in respect of such processing, including taking reasonable measures to ensure that such de-identified data cannot be associated with a Data Subject or Household. All analysis and output derived from de-identified data shall be owned by Elite.

10.2 Elite may derive pseudonymous data, meaning data that cannot be attributed to a specific individual without the use of additional information, from personal information provided by Customer or the Services provided to Customer. Elite shall keep the information required for reidentification separate from such pseudonymous data to ensure the pseudonymous data cannot be attributed to a specific Data Subject or Household.

11. Audit.

11.1 Upon Customer's written request and no more than once per year during the term of the Agreement, Elite will allow for and contribute to audits conducted by Customer or an external auditor selected by Customer in the form of providing answers to reasonable questionnaire with respect to Elite's Processing of Customer Personal Information. Audits shall be at Customer's expense, conducted during normal business hours with minimal disruption and performed subject to reasonable security restrictions of Elite, including any confidentiality requirements. To the extent a more extensive audit is granted by Elite, then the parties agree to negotiate, in good faith, a statement of work that outlines the scope and time frames of the audit, consistent with this Section 11.

11.2 If using a third party to conduct the audit, such a third party shall be qualified, independent, and subject to Elite's approval, which shall not be unreasonably withheld, and such third party must sign a non-disclosure agreement. Customer acknowledges and agrees that for purposes of this consent, a third party that is a competitor to Elite will not be considered a reasonable request for purposes of this section.

12. General.

All other terms and conditions of the Agreement remain in full force and effect. In the event of any inconsistencies between this DPA and the Agreement, the DPA shall prevail as it relates to the Processing of Customer Personal Information.

EXHIBIT 1

CUSTOMER PERSONAL INFORMATION

This Exhibit 1 forms part of the DPA and describes the Processing that Elite will perform on behalf of Customer.

(1) Categories of Customer Personal Information, including Sensitive Personal Information, if any.

The following categories may be included as part of Customer Personal Information (special categories of personal information or sensitive personal information shown in **bold**):

- Name, nicknames, or aliases
- Address (business or personal)
- Telephone or fax numbers
- Email address (business or personal)
- Gender, sex life, or sexual identity**
- Date of Birth
- Signature
- Social security, national insurance, social insurance number or equivalent**
- Account name(s)
- Passport number
- Drivers' license or national/state identification card number**
- Insurance policy number
- Bank account number
- Credit/debit card number**
- Account login, financial account, debit, or credit card in combination with any required security or access code, password or credential allowing access**
- Other financial information (please specify)
- Racial/ethnic origin or nationality**
- Political opinions, religious or philosophical beliefs, or trade union membership**
- Immigration or citizenship status**
- Records of personal property, products, or services purchases, obtained, considered
- Other purchasing or consuming histories or tendencies
- Online identifiers such as IP address
- Internet browsing or search history
- Information about a user's interaction with a website, application, or advertisement
- Website session replay information
- Education history including academic or professional qualifications, achievements, or discipline
- Human resources data such as job title, role description, job responsibilities, start and end disciplinary records, performance evaluations, or organizational structure
- Job application materials
- Contents of mail, email, or text messages (unless Elite is the intended recipient of such messages)**
- Photographs, video, audio recordings or other audio, electronic, visual, thermal olfactory, or similar information
- Profiles, predictions, inferences, or conclusions drawn from any of the information identified above to create a profile or predict behavior about a consumer**

- reflecting the consumer's tendencies, preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- Any other unique personal identifier, characteristic, or code (please describe)
 - Any other certificate or license numbers of any kind (please describe)
 - Other – please specify below:

(2) Categories of Data Subjects:

- Customer Employees and/or Contractors
- End users of Customer products and services (e.g., client customers)
- Other (please describe fully below)

(3) Subject Matter, Nature, and Purpose of the Processing of Customer Personal Information

As set forth in the DPA and Agreement.

(4) Data Retention (i.e., duration of Processing):

As set forth in the DPA and Agreement.

(5) Obligations and Rights of the Controller

As set forth in the DPA and Agreement.

EXHIBIT 2

CONTENT OF THE STANDARD CONTRACTUAL CLAUSES

PART 1: Selected modules and options of the SCCs:

For the purposes of Section 5, Customer and Elite agree that the following Modules and Options of the SCCs shall be deemed to be incorporated:

Clause 7 (<i>Docking clause</i>)	Clause 7 shall not be incorporated;
Clause 8 (<i>Data protection safeguards</i>)	Module Two (Controller to Processor) will apply where Elite acts as Customer's data processor and Module Three (Processor to Processor) will apply where Elite acts as Customer's sub-processor;
Clause 9 (<i>Use of sub-processors</i>)	Module Two, Option 2 and the general written authorization shall apply, and the specific time period referred to shall be 30 days;
Clause 10 (<i>Data subject rights</i>)	Modules One, Two and Four;
Clause 11 (<i>Redress</i>)	The option wording in Clause 11(a) on independent resolution bodies is not incorporated;
Clause 13 (<i>Supervision</i>)	For the purposes of Clause 13 (Supervision), Ireland's Data Protection Commission shall act as competent supervisory authority;
Clause 17 (<i>Governing law</i>)	Option 1 of Clause 17(Governing Law) shall apply and the laws of Ireland shall govern the SCCs.
Clause 18 (<i>Choice of forum and jurisdiction</i>)	The courts inserted shall be the courts of Ireland.

PART 2: CONTENT OF ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s):

Name: As set out in the Agreement.

Address: As set out in the Agreement.

Activities relevant to the data transferred under these Clauses: fulfillment of the Agreement

Role (controller/processor): Controller

Data importer(s)

Name: As set out in the Agreement.

Address: As set out in the Agreement.

Activities relevant to the data transferred under these Clauses: fulfillment of the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

See Exhibit 1 of the Data Processing Agreement (DPA).

Categories of personal data transferred:

See Exhibit 1 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Exhibit 1 of the DPA.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

As necessary for the purposes of processing according to the Agreement.

Nature of the processing: for fulfillment of the Agreement.

Purpose(s) of the data transfer and further processing

See Exhibit 1 of the DPA

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Exhibit 1 of the DPA.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing

See Exhibit 1 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

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

The Data Protection Commission (Ireland).

EXHIBIT 3

TECHNICAL AND ORGANIZATIONAL MEASURES

Information Security Program. Elite will maintain an information security program designed to protect the confidentiality, integrity, and availability of Customer Personal Data. The program includes, but is not limited to, the following components:

- 1.1.1. Information security policy framework;
 - 1.1.2. Program documentation;
 - 1.1.3. Auditable controls;
 - 1.1.4. Compliance records;
 - 1.1.5. Appointed security officer and information security personnel.
- 1.2. **Policies, Standards, and Guidelines.** Elite will establish and maintain information security policies, standards, and guidelines designed to protect the confidentiality, integrity, and availability of Customer Personal Data hosted in the Services, which includes the following:
- 1.2.1. Policies to restrict access to Customer Personal Data only to authorized Elite personnel and subcontractors;
 - 1.2.2. Policies requiring the use of unique user ID's and passwords;
 - 1.2.3. Policies requiring secure connections to the internet to have commercially reasonable controls designed to detect and prevent unauthorized activity;
 - 1.2.4. Policies requiring performance of regular vulnerability assessments of Elite's critical application and network components;
 - 1.2.5. Policies for the use of anti-malware and patch management controls designed to protect against virus or malware infection and exploitation of security vulnerabilities;
 - 1.2.6. Policies and standards for the use of auditable controls that record and monitor activity.
- 1.3. **Training.** Elite will train and communicate to its personnel the defined information security principles and information security policies and standards, including that:
- 1.3.1. Elite personnel will be trained in information security practices and the correct use of information processing facilities designed to minimize possible security threats;
 - 1.3.2. Security awareness training attendance reports will be maintained in the Elite personnel's file or other compliance tracking tool;
 - 1.3.3. Elite personnel will be required to report any observed or suspected threats, vulnerabilities, or incidents to the designated point of contact;
 - 1.3.4. Elite information security personnel will be made aware of reported information security threats and concerns, and will be equipped to support the Elite information security policy in the course of their normal work.
- 1.4. **Access Controls.** Elite will manage its personnel access to systems supporting the

Services in a manner that is designed to be granted on a need-to-know basis consistent with assigned job responsibilities.

- 1.5. **Business Continuity.** Elite will develop business continuity plans, in which these plans will be tested and approved by Elite management on a periodic basis.
- 1.6. **Vendor Risk Assessment.** Elite will maintain a program for vendor risk assessment.

2. DATA SECURITY CONTROLS. In the context of the Agreement, Elite will use commercially reasonable efforts to:

1.7. **Application Strategy, Design, and Acquisition.**

- 1.7.1. Inventory applications and network components that support provision of hosted services and assess their business criticality;
- 1.7.2. Perform Elite standard security compliance review for acquired or developed applications;
- 1.7.3. Review critical applications at least annually for compliance with industry and commercially reasonable security standards.

1.8. **Anti-Virus and Anti-Malware.**

- 1.8.1. Implement and configure anti-virus and anti-malware software for regular signature updates;
- 1.8.2. Implement threat management capabilities designed to protect systems holding or processing Customer Personal Data.

1.9. **Network Security.**

- 1.9.1. Configure network devices (including routers and switches) according to approved lockdown standards;
- 1.9.2. Govern and monitor changes to network security controls (including firewalls) using change management standards;
- 1.9.3. Segregate data center networks into separate logical domains with the network security controls approved by Elite security personnel.