Data Processing Agreement - Subcontractor

This Data Processing Agreement along with all exhibits attached (the “Agreement” or the “Data Processing Agreement”), is between the processor, Traction Sales And Marketing Inc. (“Traction”) and the sub-processor identified as the Contractor in a Master Contractor Agreement (“Sub-Processor”) (each a “party”, together the “parties”) and is attached and incorporated into that agreement as between the parties (the “Services Agreement”) as of the Effective Date of the Services Agreement.

1. BACKGROUND. Traction and Sub-processor have entered into an agreement (the “Services Agreement”) under which Sub-processor will provide certain products and/or services (collectively, “Services”) to Traction or its Affiliates (collectively, “Traction”). Because the Services may involve Sub-processor accessing and Processing (as defined below) Traction Information (as defined below) as a data processor on behalf of Traction or as a sub-processor where Traction Processes such information on behalf of its customers, the parties agree to the terms and conditions of this Agreement.

2. DEFINITIONS. Capitalized terms used but not defined in this Data Processing Agreement shall have the meanings set forth in the Services Agreement. For the purposes of this Agreement:

a. “Affiliate” means, as to any entity, any other entity that, directly or indirectly, controls, is controlled by or is under common control with such entity.

b. “Applicable Law” means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding legal requirement (including any and all legislative and/or regulatory amendments or successors) to which a party to this Agreement is subject and is which is applicable to such party’s information protection and privacy obligations.

c. “Data Subject” or **“Individual”** means any individual about whom Personal Information may be Processed under this Agreement.

d. “Traction Information” means any Personal Information or information that Traction provides or makes available to Sub-processor or that Sub-processor collects in connection with the Services, in any form, format or media (including paper, electronic and other records) that a reasonable person under the circumstances would understand to be confidential. Traction Information may include Personal Information or other information that Traction Processes as a data processor on behalf of its customers, which Traction may permit Sub-processor to access or Process as a sub-processor.

e. “Personal Information” or **“Personal Data”** means any Traction Information that relates to an identified or identifiable individual; an identifiable individual 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.

f. “Process” or **“Processing”** means any operation that is performed on Personal Information, whether or not by automated means, such as the collection, recording, organization, alteration, use, access (including remote access), disclosure, copying, transfer, storage, deletion, combination, destruction, disposal, or other use of Personal Information.

g. “Special Categories of Data” or **“Sensitive Information”** means any of the following types of Personal Information: (i) social security number, taxpayer identification number, passport number, driver’s license number or other government-issued identification number; or (ii) credit or debit card details or financial account number, with or without any code or password that would permit access to the account, credit history, or (iii) information on race, religion, ethnicity, sex life or practices, medical or health information, genetic or biometric information, biometric templates, political or philosophical beliefs, political party or trade union membership, background check information, judicial data such as criminal records or information on other judicial or administrative proceedings, or any other category of Personal Information identified as special or sensitive under Applicable Law.

3. DATA PROCESSING AND PROTECTION OF TRACTION INFORMATION. Where Sub-processor Processes Traction Information that does not include Personal Information Sub-processor will, and will ensure that any person engaging in Processing such Traction Information on its behalf, will comply with the following requirements:

a. Sub-processor will Process such information only as necessary to deliver the Services;

b. Sub-processor will not disclose such information except: (i) to Sub-processor Personnel who have a need to know such information and are under confidentiality obligations at least as restrictive as those described herein; or (ii) in accordance with Section 4(h) (Disclosure Requests).

c. Sub-processor will employ reasonable measures to safeguard such information from unauthorized access or use.

4. DATA PROCESSING AND PROTECTION OF PERSONAL INFORMATION. With respect to Personal Information Processed by Sub-processor as a data processor on behalf of Traction or as a sub-processor where Traction Processes such Personal Information on behalf of its customers (or both), Sub-processor will, and will ensure that any person engaging in Processing such Personal Information on its behalf, will comply with the following requirements:

a. Limitations on Use. Sub-processor will Process Personal Information only to deliver Services as instructed by Traction in writing (including in electronic form) and will not Process Personal Information for any other purpose, including for its own commercial benefit, unless Traction has provided its prior express written agreement. The scope, classification, purposes and details of Processing are described in the attached Exhibit A (Description of Processing).

b. Limitations on Disclosure. Sub-processor will not disclose or transfer Personal Information to or allow access to Personal Information (**"Disclosure"**) by any third party (including its Affiliates and subcontractors) without the express prior written consent of Traction, except: (i) as provided in Section 4(h) (Disclosure Requests); or (ii) as specifically stated elsewhere in this Agreement. If Traction provides such consent to Sub-processor's Disclosure to a third party, Sub-processor will, prior to any such Disclosure, enter into an agreement with such third party that is at least as protective of Personal Information as this Agreement. Such agreement will limit use of Personal Information to Traction's written instructions and will be provided to Traction promptly upon request and Traction may share such agreement with its customers or regulatory authorities (where applicable). Sub-processor will remain accountable and responsible for all actions by such third parties with respect to any such disclosure.Sub-processor will make available upon request, an overview of any such approved Affiliates and subcontractors involved in Processing Personal Information under or which have access to Personal Information.

c. Confidentiality. Sub-processor will hold Personal Information in strict confidence and adhere to the requirements provided in section 4(d) (below).

d. Information Security Program. Sub-processor will implement, maintain, and monitor a comprehensive written information security program that (i) is designed to protect Personal Information against anticipated threats or hazards to its confidentiality, integrity or availability (e.g. unauthorized access, collection, use, copying, modification, disposal or disclosure, unauthorized, unlawful, or accidental loss, destruction, acquisition, or damage, or any other form of unauthorized Processing); and (ii) contains appropriate administrative, technical, and physical safeguards (**"Information Security Program"**). The safeguards will meet or exceed each applicable third party security assurance standard, such as ISO 27001, SSAE 16 SOC 2, ISAE 3402. The Information Security Program will contain procedures to respond to a Security Incident (defined at section 4(l) below) and will include the measures listed in the attached Exhibit B (" Security Standards"). The Security Standards apply whether or not there is an export of Personal Data from the European Economic Area.

i. Scope. Sub-processor will maintain and enforce its Information Security Program at each location from which Sub-processor provides Services. In addition, Sub-processor will ensure that its Information Security Program covers all devices and media that process, host or store Personal Information, including without limitation networks, systems, servers, computers, notebooks, laptops, tablets, mobile phones, and other. Sub-processor will ensure that its Information Security Program includes industry standard controls, such as password protections, firewalls, anti-virus and malware protections. Sub-processor shall ensure that all third parties with whom it provides access to Traction Information adheres to the Information Secruity Program.

ii. Risk Assessments. In connection with maintaining its Information Security Program, Sub-processor will: (i) conduct periodic risk assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Personal Information; and (ii) evaluate and improve, where necessary, the effectiveness of its information security controls. Such assessments will also consider Sub-processor's compliance with its Information Security Program and Applicable Law;

iii. Review. Sub-processor will review and, as appropriate, revise its Information Security Program at least annually or whenever there is a material change in Sub-processor's business practices that may reasonably affect the security, confidentiality or integrity of Personal Information;

iv. Modifications. During the course of providing Services, Sub-processor may not alter or modify its Information Security Program in such a way that will weaken or compromise the confidentiality, availability or integrity of Personal Information;

v. Primary Security Manager. Sub-processor will notify Traction of its designated primary security manager. The security manager will be responsible for managing and coordinating the performance of Sub-processor's obligations set forth in its Information Security Program and in this Agreement;

vi. Encryption. Sub-processor will encrypt, using best-in-class industry standard encryption tools, any and all Sensitive Information that Sub-processor (i) transmits or sends wirelessly or across public networks; (ii) stores or uses on computers or storage media (i.e. data at rest, and data in use), and (iii) stores on portable devices, where technically feasible. Sub-processor will safeguard the integrity and confidentiality of all encryption keys associated with encrypted Sensitive Information.

vii. Sub-processor Personnel. Prior to providing access to Personal Information to any Sub-processor officer, director, employee, contractor, subcontractor or agent ("Sub-processor Personnel"), Sub-processor will require Sub-processor Personnel to comply with its Information Security Program and protect all Personal Information in accordance with the requirements of this Agreement (including during the term of their employment or engagement and thereafter), and will provide appropriate training regarding information security and protection of Personal Information to the Sub-processor Personnel. Sub-processor will maintain appropriate access controls including, but not limited to, limiting access to Personal Information to the minimum number of Sub-processor Personnel who require such access in order to provide Services to Traction, and will maintain an audit trail to document when and by whom Personal Information has been accessed. Sub-processor will ensure that any non-compliance of Sub-processor Personnel with this Agreement will result in disciplinary sanctions up to and including termination of the employment or other engagement, in compliance with Applicable Law.

viii. Sub-contracting. Sub-processor shall not subcontract the Services to any other parties without the prior express written consent of Traction. A signed SOW or written approval from an authorized officer of Traction shall constitute Traction's consent and approval of Sub-processor's use of such subcontractors. In any event, Sub-processor is liable for any actions or omissions of

any of its subcontractors ("Sub-subprocessors") and shall ensure that they enter into data processing agreements with Sub-subprocessor that are at least as protective of Traction Information as this Data Processing Agreement.

ix. Systems Inventory. Sub-processor will maintain readily available information regarding: (A) the structure and functioning of all systems and processes that Process Personal Information under this Agreement (e.g., inventory of system and processes); (B) categories of Processing it is engaged in; (C) details regarding any data exports; and (D) names and contact information of Sub-processor Personnel that Process Traction Information.

e. Data Integrity. Sub-processor will ensure that all Personal Information created by Sub-processor on behalf of Traction is accurate and, where appropriate, kept up to date, and ensure that any Personal Information which is inaccurate or incomplete is erased or rectified in accordance with Traction's instructions.

f. Correction and Deletion. Upon Traction's request and within a reasonable time, Sub-processor will correct, delete, and/or block Personal Information from further Processing and/or use and confirm to Traction that Sub-processor has done so.

g. Access Requests. Sub-processor will promptly notify Traction in writing, and in any case within two days of receipt, unless specifically prohibited by Applicable Law if Sub-processor receives: (i) a request from an Individual with respect to Personal Information Processed, including but not limited to opt-out requests, requests for access and/or rectification, blocking, and all similar requests, and will not respond to any such requests unless expressly authorized to do so by Traction, or (ii) a complaint relating to the Processing of Personal Information, including allegations that the Processing infringes on a Data Subject's rights. To the extent permitted by Applicable Law, Sub-processor will cooperate with Traction and act only upon Traction's instructions with respect to any action taken relating to such request or complaint.

h. Disclosure Requests. If Sub-processor receives any order, demand, warrant, or any other document requesting or purporting to compel the production of Personal Information or Traction Information (including, for example, by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands or other similar processes, or requests (a "Disclosure Request") from law enforcement, state security body, or other governmental authority ("Governmental Authorities"), Sub-processor will immediately notify Traction (except to the extent otherwise required by Applicable Law) and will not disclose Information to the third party without providing Traction at least forty-eight (48) hours, following such notice, so that Traction may, at its own expense, exercise such rights as it may have under Applicable Law to prevent or limit such disclosure. To the extent permitted by Applicable Law, Sub-processor will act only upon Traction's instructions with respect to such a Disclosure Request. Sub-processor will assess each Disclosure Request to establish whether it is legally valid and binding on Sub-processor. Any request that is not legally valid or binding on Sub-processor will be resisted by Sub-processor in accordance with Applicable Law. With respect to Disclosure Requests from Governmental Authorities, Sub-processor will request the Governmental Authority to place the Disclosure Request on hold for a reasonable delay in order to enable Traction and its customers (as applicable) to contact the relevant data protection

authority ("DPA") for an opinion on the validity of the Disclosure Request. If the suspension and/or notification of the Disclosure Request is prohibited, such as in the case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, Sub-processor will ask the Governmental Authority to waive this prohibition and will document that it has made this request. In any event, Sub-processor will on an annual basis provide to Traction general information on the number and types of Disclosure Requests received in the preceding 12-month period, and Traction may share this information with customers and applicable DPA as it deems necessary.

i. Internal Compliance Auditing. Sub-processor will regularly audit business processes and procedures that involve the Processing of Personal Information under this Agreement for compliance with this Agreement. Sub-processor will provide a copy of the audit results to Traction upon request. Sub-processor agrees that Traction may share audit results with a customer or the appropriate DPA, if Traction deems such sharing to be necessary. Sub-processor will take adequate steps to remedy any established noncompliance with this Agreement, in the absence of which Traction will have the right to temporarily suspend the relevant Processing under the Agreement until such time that the Processing is adjusted in such a manner that the noncompliance is remedied. To the extent such adjustment is not possible, Traction will have the right to terminate the Services Agreement, without liability to Traction.

j. Audit. Sub-processor agrees that Traction and Traction's customers may perform on-site security audits of Sub-processor's facilities and systems that it uses for the Processing of Personal Information under this Agreement, in order to confirm Sub-processor's compliance with the terms of this Agreement, the Services Agreement, and Applicable Law. Sub-processor will also ensure that Traction, Traction's customers or the DPAs have direct access and rights to audit any of Sub-processor's subcontractors upon reasonable notice in order to confirm compliance with their obligations. Sub-processor will ensure that adequate steps are taken to address breaches of this Agreement identified during such an audit, and will have the right to temporarily suspend the relevant Processing under this Agreement until such time as the Processing is adjusted in such a manner that the noncompliance is remedied. To the extent such adjustment is not possible, Traction will have the right to terminate the Agreement, without liability to Sub-processor.

k. Regulatory Investigations. Upon notice to Sub-processor, Sub-processor (and its subcontractors) will assist and support Traction in the event of an investigation by any Governmental Authorities, including a DPA or similar authority, if and to the extent that such investigation relates to Personal Information Processed by Sub-processor in accordance with this Agreement. Such assistance will be at Traction's sole expense, except where investigation was required due to Sub-processor's acts or omissions, in which case such assistance will be at Sub-processor's sole expense. Sub-processor (and its subcontractors) will also abide by any binding DPA decisions issued to Traction or its customers that may affect Processing of Personal Information under this Agreement.

l. Security Incident. Sub-processor will notify Traction in writing immediately (and in any event within no more than twenty-four (24) hours) whenever Sub-processor reasonably believes that there has been any unauthorized access or disclosure, unauthorized, unlawful or accidental loss,

misuse, destruction, acquisition of, or damage to Traction Information, or any other unauthorized Processing of Traction Information ("Security Incident"). After providing notice, Sub-processor will investigate the Security Incident, take all necessary steps to eliminate or contain the exposure of Traction Information, and keep Traction advised of the status of the Security Incident and all related matters. Sub-processor further agrees to provide reasonable assistance and cooperation requested by Traction and/or Traction's designated representatives, in the furtherance of any correction, remediation, or investigation of any Security Incident and/or the mitigation of any damage, including any notification that Traction may determine appropriate to send to affected Individuals, regulators or third parties, and/or the provision of any credit reporting service that Traction deems appropriate to provide to affected Individuals. Further, if Sub-processor's acts or omissions (including, but not limited to, Sub-processor's breach of this Agreement) have caused the Security Incident, Sub-processor shall bear the cost of the assistance and cooperation requested by Traction under this paragraph. Unless required by Applicable Law, Sub-processor will not notify any Individual or any third party other than law enforcement of any potential Security Incident involving Traction Information, in any manner that would identify, or is reasonably likely to identify or reveal the identity of, Traction, without first consulting with, and obtaining written permission of, Traction. In addition, within thirty (30) days of identifying or being informed of any Security Incident arising from any act or omission by Sub-processor, Sub-processor will develop and execute a plan, subject to Traction's approval, that reduces the likelihood of a recurrence of a Security Incident.

m. Cardholder Information. For purposes of this Agreement, "Cardholder Data" means any Traction Information that includes: (a) with respect to a payment card, the account holder's name, account number, service code, card validation code/value, PIN or PIN block, valid to and from dates and magnetic stripe data; and (b) information relating to a payment card transaction that is identifiable with a specific account. If Sub-processor has access to Cardholder Data, Sub-processor must comply at all times with the security standards for the protection of Cardholder Information, with which payment card companies require merchant to comply, including, but not limited to, the Payment Card Industry Data Security Standards currently in effect and as such standards may be updated from time to time ("PCI Standards"). Where Sub-processor has access to any Cardholder Data, Sub-processor will promptly provide, at Traction's request, a current copy of Sub-processor's PCI Attestation of Compliance demonstrating compliance with the PCI Standards, per the PCI-DSS and SAQ reporting guidelines. Where Sub-processor has access to any Cardholder Data, if during the term of a relevant agreement, Sub-processor undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI Standards, Sub-processor will promptly notify Traction of such circumstances. Sub-processor will not take any actions that will compromise Traction's ability to comply with the PCI Standards.

n. Return or Disposal. Sub-processor will, as appropriate and as directed by Traction, regularly dispose of Personal Information that is maintained by Sub-processor, but that is no longer necessary to provide Services. Upon termination or expiration of this Data Processing Agreement for any reason or upon Traction's request, Sub-processor will immediately cease handling Personal Information and will return in a manner and format reasonably requested by Traction, or, if specifically directed by Traction, will destroy and make unrecoverable, any or all Personal Information in Sub-processor's possession, power or control. If Sub-processor disposes of any

paper, electronic or other record containing Traction Information, Sub-processor will do so by taking all reasonable steps (based on the sensitivity of Traction Information) to destroy Traction Information by: (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying Traction Information in such records to make it unreadable, unreconstructable and indecipherable. Upon request, Sub-processor will provide a written certification that Traction Information has been returned or securely destroyed in accordance with this Agreement.

o. Adverse Changes. Sub-processor will notify Traction promptly if Sub-processor:

i. Has reason to believe that it is unable to comply with any of its obligations under this Agreement and it cannot cure this inability to comply; or

ii. Becomes aware of any circumstances or change in Applicable Law that is likely to prevent it from fulfilling its obligations under this Agreement.

In the event Sub-processor provides such notice, Traction will have the right to temporarily suspend the relevant Processing under this Agreement until such time that the Processing is adjusted in such a manner that the noncompliance is remedied. To the extent such adjustment is not possible, Traction will have the right to terminate this Agreement and the Services Agreement, without liability to Traction.

p. On Premise Requirements. Where Sub-processor or Sub-processor Personnel will perform on premise services (e.g. in a Traction facility), Sub-processor Personnel shall familiarize themselves with and comply with applicable Traction policies, standards and procedures.

q. Other.

i. Sub-processor will provide relevant information and take other steps reasonably requested by Traction and/or its customers to address inquiries and comply with any obligations applicable to Traction and/or its customers under Applicable Laws, including to assist them in meeting their registration and notification obligations under data protection laws.

ii. Traction may share this Data Protection Agreement and other information provided by Sub-processor to demonstrate compliance with this Data Protection Agreement with Traction's customers and DPAs or other regulators.

iii. In the event that this Data Protection Agreement, or any actions to be taken or contemplated to be taken in performance of this Data Protection Agreement, do not or would not satisfy either party's obligations under Applicable Law, the parties will negotiate in good faith upon an appropriate amendment to this Data Protection Agreement.

iv. Upon Traction's request, Sub-processor will execute a HIPAA business associate agreement, where the Services involve access or Processing of Personal Information covered by HIPAA.

5. DATA TRANSFERS

To the extent that the Processing of Personal Data by Sub-processor involves the export of such Personal Data to a third party in a country or territory outside the EEA, such export shall be:

a. to a country or territory ensuring an adequate level of protection for the rights and freedoms of Data Subjects as determined by the European Commission;

b. to a third party that is a member of a compliance scheme recognized as offering adequate protection for the rights and freedoms of Data Subjects as determined by the European Commission, such as, but not limited to the Privacy Shield; or

c. governed by the Standard Contractual Clauses.

6. THIRD-PARTY BENEFICIARIES. The parties agree that Traction's Affiliates are intended third-party beneficiaries of this Agreement and that this Agreement is intended to inure to the benefit of such Affiliates. Without limiting the foregoing, Traction Affiliates will be entitled to enforce the terms of this Agreement as if each was a signatory to this Agreement. Traction also may enforce the privacy and data security provisions on behalf of Traction Affiliates (instead of Traction Affiliate(s) separately bringing a cause of action against Sub-processor). Sub-processor will be entitled to rely solely on Traction's instructions relating to Traction Information.

7. DATA SUBJECT RIGHTS. Sub-processor acknowledges on behalf of itself and any of Sub-processor's subcontractors that Individuals can enforce this Agreement against Sub-processor as third-party beneficiaries in the event Sub-processor (or its subcontractors) fails to fulfill its obligations under this Agreement and an Individual has a claim against Traction or its customer with respect to such violation but is unable to enforce the claim against Traction or its customer if Traction and its customer have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed their entire legal obligations by contract or by operation of law. In such case, the Individual may, at his/her choice, submit a claim against Sub-processor to the DPA or courts in the country of origin of the data transfer, or to the DPA or courts in Ireland. The parties agree that any Individual who has suffered damage as a result of any breach of the obligations of Sub-processor (or Sub-processor's subcontractors or Sub-processor Personnel) under this Agreement shall be entitled to receive compensation for the actual direct damage suffered, to the extent provided by applicable EEA law.

8. AMENDMENTS. The parties agree that this Agreement, except for any Standard Contractual Clauses, may be amended only by written agreement between the parties. The parties agree to negotiate amendments to this Agreement in good faith to address changes in Applicable Law.

9. TERM AND TERMINATION. This Agreement will remain in effect for so long as Sub-processor maintains or has access to Personal Information. Upon termination of the Services Agreement, Sub-processor will promptly cease all Processing of Personal Information, but will continue to safeguard or securely dispose of other Traction Information. Termination will not affect the

accrued rights or liabilities of either party under this Agreement. The obligations of Sub-processor under this Agreement will continue for so long as Sub-processor continues to have access to, is in possession of, or acquires Traction Information, even if all agreements between Sub-processor and Traction have expired or have been terminated.

10. GENERAL. This Agreement may not be assigned by Sub-processor without prior written consent of Traction. This Agreement will not be effective until signed by both parties. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and merges all prior and contemporaneous communications. In the event of a conflict between this Agreement and the Services Agreement, this Agreement shall control. The construction and validity and performance of this Agreement shall be governed by the laws of the province of British Columbia.

Attachments:

Exhibit A – Description of Processing

Exhibit B – Security Standards

Exhibit A
DESCRIPTION OF PROCESSING

This Exhibit A forms part of the Data Processing Agreement between Traction and Sub-processor.

Data Processor

The data processor is:

Traction, as defined above, a user of Sub-processor's Services, as described in more detail in the Services Agreement.

Data Sub-Processor

The data sub-processor is:

Sub-processor, as defined above, providing the Services to Traction.

Data subjects

The Personal Information processed concerns the following categories of data subjects:

Traction's customers and Traction's customers' customers.

Categories of data

The Personal Information transferred concerns the following categories of data:

Any categories of data that Traction's customers include in their salesforce.com instance.

Special categories of data (if applicable)

The Personal Information transferred concern the following special categories of data (please specify):

Any special categories of data that Traction's customers provide to Traction.

Processing operations

The data processing will involve any such processing that is necessary for the purposes set out in the Service Agreement, the Data Processing Agreement, or as agreed upon between the parties in writing.

Duration of processing

The Personal Information will be processed for the term of the Service Agreement, or as otherwise required by law or agreed between the parties in writing.

Exhibit B
Security Standards

This Exhibit B forms part of the Data Processing Agreement between Traction and Sub-processor.

1. Sub-processor has agreed to employ appropriate technical and organizational measures to protect against unauthorized or unlawful processing of Personal Information (as defined in the Data Processing Agreement) ("Security Measures") and against accidental loss or destruction of, or damage to, Personal Information.

2. Sub-processor's Information Security Program shall include specific security requirements for its personnel and all subcontractors, sub-processors, or agents who have access to Traction Information ("Data Personnel"). Sub-processor's security requirements shall include the following requirements:

A. Information Security Policies and Standards

i. Sub-processor will maintain appropriate information security policies, standards and procedures. These policies, standards and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Traction Information. These policies, standards and procedures are designed to:

a. prevent unauthorized persons from gaining physical access to Personal Data processing systems (e.g. physical access controls);

b. prevent Personal Data processing systems being used without authorization (e.g. logical access control);

c. ensure that Data Personnel gain access only to such Personal Data as they are entitled to access (e.g. in accordance with their access rights) and that, in the course of Processing or use and after storage, Traction Information cannot be read, copied, modified or deleted without authorization (e.g. data access controls);

d. ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the recipients of any transfer of Traction Information by means of data transmission facilities can be established and verified (e.g. data transfer controls);

e. ensure the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing (e.g. entry controls);

f. ensure that Personal Data are Processed solely in accordance with Traction's Instructions (e.g. control of instructions);

g. ensure that Traction Information are protected against accidental destruction or loss (e.g. availability controls);

h. ensure that Personal Data collected for different purposes can be processed separately (e.g. separation controls);

i. ensure that Personal Data maintained or processed for different customers is processed in logically separate locations (e.g. data segregation).

j. ensure that all systems that Process Traction Information are subject to a secure software developmental lifecycle.

k. ensure that all systems that Process Traction Information are the subject of vulnerability management program, that includes without limitation internal and external vulnerability scanning with risk rating findings and formal remediation plans to address any identified vulnerabilities.

B. Physical Security

i. General. Sub-processor will maintain commercially reasonable security systems at all Sub-processor sites at which an information system that uses or stores Traction Information is located ("Processing Locations"). Sub-processor will reasonably restrict access to Processing Locations.

ii. Data Centers. Data centers are a type of Processing Location. Physical access controls have been implemented for all data centers. Unauthorized access is prevented through 24x7 onsite staff, biometric scanning and security camera monitoring. Sub-processor audits the physical security of its data center(s) using an independent firm.

C. Organizational Security

i. Sub-processor will maintain information security policies and procedures addressing:

a. Data Disposal. When media are to be disposed of or reused, procedures have been implemented to prevent any subsequent retrieval of any Traction Information stored on them before they are withdrawn from the inventory.

b. Data Minimization. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures have been implemented to prevent undue retrieval of Personal Data stored on them.

c. Data Classification. Sub-processor implements security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for all employees.

d. Incident Response. All Personal Data security incidents are managed in accordance with appropriate incident response procedures.

e. Encryption. All Traction Information is stored and transmitted using industry standard encryption mechanisms and strong cipher suites (AES 265-bit is recommended).

D. Network Security

i. Sub-processor maintains information security policies and procedures appropriately addressing network security.

ii. Sub-processor secures its networks employing a defense in depth approach that utilizes commercially available equipment and industry standard techniques, including without limitation firewalls, intrusion detection systems, access control lists and routing protocols.

E. Access Control (Governance)

i. Sub-processor governs access to information systems that Process Traction Information.

ii. Only authorized staff can grant, modify or revoke access to an information system that Processes Traction Information.

iii. User administration procedures are used to: (i) define user roles and their privileges; (ii) govern how access is granted, changed and terminated; (iii) address appropriate segregation of duties; and (iv) define the requirements and mechanisms for logging/monitoring.

iv. All Data Personnel are assigned unique User IDs.

v. Access rights are implemented adhering to the “least privilege” approach.

vi. Sub-processor implements commercially reasonable physical and technical safeguards to create and protect passwords.

F. Virus and Malware Controls

i. Sub-processor protects Traction Information from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Traction Information

G. Personnel

i. Sub-processor has a security awareness program to train all employees about their security obligations. This program includes training about data classification obligations; physical security controls; security practices and security incident reporting.

ii. Sub-processor has clearly defined roles and responsibilities for employees.

iii. Prospective employees are screened, including background checks for Data Personnel or individuals supporting Traction's technical environment or infrastructure, before employment and the terms and conditions of employment are applied appropriately.

iv. Data Personnel strictly follow established security policies and procedures. Disciplinary process is applied if Data Personnel fail to adhere to relevant policies and procedures.

H. Business Continuity

i. Sub-processor implements disaster recovery and business resumption plans. Business continuity plans are tested and updated regularly to ensure that they are up to date and effective.