Blattner Technologies Security Data Sheet

V05082024

1. **Definitions.** All capitalized terms not defined herein have the meaning set forth in the Agreement.
   1.1. "**Affiliate**" means an entity controlling, controlled by or under common control of a Party.
   1.2. "**Anti-Virus Signatures**" means a catalog of data that describes the current Malicious Software threats (e.g., virus, worms, spyware) and how Anti-Virus Software is to detect and remove the threat from the given system, message or file.
   1.3. "**Anti-Virus Software**" means an industry-standard software specifically written to prevent the introduction or intrusion of Malicious Software through a set of Anti-Virus Signatures.
   1.4. "**Blattner Tech Systems**" means the equipment, software and communications systems and components used, supplied and/or developed by Blattner Tech or any of its Affiliates or Subcontractors for the provision of the Services or Software Services, including, without limitation any payment card gateways or card processors.
   1.5. "**Collection**" means making a forensic copy of the data and storing such data in a secure location.
   1.6. "**Customer Data**" means all Customer Personal Data, data, information, visual or graphic representations and other similar materials in any medium or format electronic, tangible or otherwise and which are provided to or accessed by Consultant or any of its Affiliates or Subcontractors by or at the direction of Customer or any of its Affiliates or which Consultant and its Affiliates and Subcontractors create, collect, process, store, generate or transmit in connection with the provision of the Services, Software Services, or the performance of Consultant's obligations under the Agreement. Customer Data shall be considered and treated as Confidential Information.
   1.7. "**Customer Personal Data**" means data and/or information that Consultant may obtain or have access to, Process or transmit in connection with the Agreement or any SOW which consists of information or data naming or identifying a natural Person such as: (a) personally identifying information that is explicitly defined as a regulated category of data under any Data Privacy Laws applicable to Customer; (b) non-public information, such as a national identification number, passport number, social security number, driver's license number; (c) health or medical information, such as insurance information, medical prognosis, diagnosis information or genetic information; (d) financial information, such as a policy number, Payment Information, and/or bank account number; and/or (e) sensitive personal data, such as mother's maiden name, race, marital status, gender or sexuality or Internet protocol addresses relating to use of websites or assigned to a person. Customer Personal Data shall be considered and treated as Confidential Information.
   1.8. "**Customer Systems**" means the networks, equipment, software and communications systems and components and elements thereof owned, used or operated by Customer.
   1.9. "**Data Privacy Laws**" means laws relating to data privacy, trans-border data flow or data protection, such as the Gramm- Leach-Bliley Act of 1999 Pub. L. No. 106-102, 12 U.S.C. 1843(k)(1), European Union Directive on the Protection of Personal Data, Council Directive 95/46/EC, 1995 O.J. (L281) and implementing member state legislation and, when effective, the successor EU General Data Protection Regulation 2016/67 and more specific rules or laws by member state laws (such as in the case of employee data, as applicable), the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada, and the fair information principles published by the United States Federal Trade Commission, and any and all successor or supplemebntal laws relating thereto, and any additional laws or regulations that may be promulgated in the future including, without limitation, those of the United Kingdom.

1.10. "**End User(s)**" means any individual Customer permits to use the Software Services, which may include, without limitation, employees, agents, contractors, consultants, outsourcers, supplies or other individuals (including third parties).

1.11. "**Governmental Authority**" means each federal, state and municipal government, authority and agency and its respective agencies, departments, authorities and commissions.

1.12. "**Information Security Incident**" means: (a) the actual unauthorized acquisition, access, use, Processing, loss or disclosure of Confidential Information; (b) the suspicion or reasonable belief that there has been an unauthorized acquisition, access, use, Processing, loss, or disclosure of Confidential Information; or (c) the unauthorized use of any Consultant Systems to gain access to any Customer System or the system of any Affiliate of Customer.

1.13. "**Malicious Software**" means any type of software or program which is designed to: (a) cause unauthorized access to or intrusion upon; or (b) otherwise disrupt and/or damage, computer equipment, software, and/or data (commonly referred to as a virus, worm, Trojan horse, or spyware).

1.14. "**PA DSS Requirements**" means the Payment Application Data Security Standard maintained by the PCI which applies to Persons that process payment card transactions with participating major payment card networks.

1.15. "**Payment Information**" means the payment card (credit, debit or gift card) information collected from a Person, including the cardholder's name and billing address, the payment card number and the expiration date and the external verification (e.g., CVV2) code for the payment card.

1.16. "**PCI**" means the Payment Card Industry Security Standards Council and its successors.

1.17. "**PCI DSS Requirements**" means the Payment Card Industry Data Security Standard maintained by the PCI which applies to Persons that process payment card transactions with the participating major payment card networks.

1.18. "**Person**" means any natural person, corporation, partnership, limited liability company, trust, association, firm, entity or Governmental Authority.

1.19. "**Personnel**" means any Person employed, hired or otherwise compensated for performing work for a Party including, but not limited to, employees, contractors, Subcontractors, consultants, or advisors.

1.20. "**Process**" or "**Processing**" means any operation or set of operations performed or to be performed with respect to or in connection with Customer Personal Data, whether or not by automatic means, such as creating, capturing, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, transmitting, transferring, disclosing, or destroying Customer Personal Data.

1.21. "**Software Service(s)**" means the proprietary Consultant software provided to Customer on a hosted or software as a service basis. For the avoidance of doubt, Software Services are a type of Service, as such term is defined in the Agreement.

1.22. "**Subcontractor**" means any subcontractor of Consultant providing services as permitted under the Agreement or an applicable Statement of Work.

1.23. "**Workstation(s)**" means all laptop, notebook, desktop and any other computer used by Consultant in providing the Services or otherwise Processing Customer Personal Data.

2. **Application and Technological Advances**. The Parties understand and agree that technologies and practices evolve over time, and that the administrative, physical, technical and organizational measures and controls set forth in this Security Datasheet may be subject to progress and development. In that regard, Blattner Tech, Affiliates of Blattner Tech, and Blattner Tech Personnel may, in some cases and upon the prior written approval of Customer, implement alternative but equivalent (or functionally superior) measures to those set forth in this Security Datasheet; provided, however, that the implementation of such alternatives do not result in any degradation or reduction of the effectiveness of the associated measures and controls; and further provided,

Customer's approval of the same shall not be deemed a waiver of any of Blattner Tech's obligations under this Security Datasheet. Blattner Tech will be liable and indemnify Customer for any failure of Affiliates of Blattner Tech and Blattner Tech Personnel to comply with the terms and conditions of this Security Datasheet to the same extent as if such failure was attributable to Blattner Tech itself. Customer may request, and Blattner Tech shall not unreasonably refuse to enter into, a written undertaking to protect Customer's confidentiality and systems security in case of physical or on-line access to Customer's premises and/or Customer Systems or the premises and/or systems of any Affiliates of Customer.

3. **Safeguards**. Blattner Tech will develop, maintain, and implement a comprehensive written information security program that complies with applicable Data Privacy Laws, including mandatory annual training to Blattner Tech Personnel who have access to Customer Confidential Information regarding the privacy, confidentiality and information security requirements set forth in the Agreement and this Security Datasheet. Blattner Tech's information security program and the information security programs of its Affiliates and all Subcontractors will include appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to: (a) ensure the security and confidentiality of Customer Confidential Information; (b) protect against any anticipated threats or hazards to the security and integrity of Customer Confidential Information; and (c) protect against any Information Security Incident.
4. **Security Standards**. Blattner Tech will, and, as applicable, will cause Blattner Tech's Affiliates and Subcontractors to at all times maintain: (a) a SSAE 16 Service Organization Control 2 Type II ("**SOC 2**") or a SSAE 16 Service Organization Control 3 Type II ("**SOC3**") report (or any successor reports) for security, availability, confidentiality, and privacy-related controls of the information processing and management systems (including procedures, people, software, data, and infrastructure) used by Blattner Tech, Affiliates of Blattner Tech, or Subcontractors in processing Customer Confidential Information; or (b) an ISO 27001/27002/27018 certification or industry-standard successor report. Blattner Tech will, and will cause Affiliates of Blattner Tech and Subcontractors to promptly provide a copy of the SOC 2 or SOC 3 report or ISO certification report to Customer upon execution of this Amendment and in no event later than thirty (30) days of receipt from the independent auditor for each annual period in which Blattner Tech, Affiliate of Blattner Tech, or Subcontractor receives the same. Blattner Tech will promptly notify Customer of any deficiencies identified in any reports. Blattner Tech will promptly address and resolve any such deficiencies to the extent necessary to comply with Blattner Tech's obligations under the Agreement and the Security Datasheet, and notify Customer when any such deficiency is resolved. If any deficiency is not promptly resolved, it will be deemed a material breach of the Agreement by Blattner Tech.
5. **Penetration Testing**. Blattner Tech will engage, at its own costs, an independent third party to conduct penetration testing on a yearly basis, including human manual testing, to evaluate the security controls of the application, host and network layers used to provide the Software Service following industry standard methodologies (e.g. OWASP and OSSTMM). Blattner Tech shall provide Customer with copies of its report at the time they are available and in no event later than thirty (30) days after receipt for each annual period. Blattner Tech will promptly notify Customer of any deficiencies identified as well as corrective actions necessary for all vulnerabilities to be corrected. Should any critical weakness be identified, Blattner Tech will, and will cause its Affiliates and Subcontractors (as applicable) to undertake corrective actions within seven (7) calendar days of receipt of the report. Should any high weakness be identified, corrective actions shall be undertaken by Blattner Tech, its Affiliates, or Subcontractors (as applicable) within thirty (30) calendar days of receipt of the report.
6. **Credentials and User Authentication**. Blattner Tech will ensure that each End User is assigned a unique user ID and password, token, or biometric identifier ("**Credentials**"), and will allow End Users to access the Software Services only after authentication with valid Credentials. Credentials will be stored at rest using a one-way hashing algorithm (SHA-256, or the equivalent), and will be encrypted whenever transmitted over the Internet or any untrusted network, using Secure Sockets Layer ("**SSL**") protocol during transmission. Upon authentication, the

Software Services will provide the ability to track each End User's activity through the use of a unique session identifier associated with the Credentials and each login session.

7. **Passwords**. All passwords, whether manually created by the user or automatically generated must comply with minimum complexity requirements including, without limitation, a requirement that all passwords have a minimum of twelve (12) alpha numeric characters and include letters, special characters, and numbers. The Blattner Tech Systems and all Workstations will: (a) contain password history controls to prohibit use of the three (3) most recently used passwords; (b) require a verification question before resetting password; (c) not log passwords under any circumstances; and (d) have controls in place to force a password to expire after a defined period of time (all of the foregoing, the "**Password Security Requirements**"). In no instance will Blattner Tech Personnel manually select and assign a password to an End User of any Software Services. Any automatically generated passwords for the Software Services will be: (i) automatically generated in a manner which produces a random value; (ii) delivered automatically via email to the requesting End User; and (iii) valid only for one successful login, requiring the receiving End User to manually select a replacement password upon login with the automatically generated password.
8. **ID and Access Management**. The Software Services shall have the ability to use identity and access management standards such as: (a) SCIM and/or make API integration available for the creation, modification, and deletion of user accounts and access permissions, and the exchange of identity data; and (b) identity and access management standards such as SAML, OAuth, OpenID Connect in order to make authentication and authorization decisions.
9. **Application Security**. The Software Services and the Blattner Tech Systems will provide, where applicable, configurable security controls including, at a minimum: (a) the ability to revoke access to the Blattner Tech Systems and Software Services after a defined number of consecutive failed login attempts ("**Lockout**"); (b) the ability to specify the Lockout time period; (c) the ability to specify the number of invalid login requests before initiating the Lockout; (d) comply with the Password Security Requirements; (d) controls to terminate an End User session after a defined period of inactivity; (e) the ability to accept logins to the Blattner Tech Systems and Software Services from only certain IP address ranges; (f) the ability to restrict logins to the Blattner Tech Systems and Software Services to specific time periods; (g) the ability to delegate End User authentication or federate authentication via SAML; and (h) up-to-date, via automation or a centrally controlled process, application and operating system patches and services packs.
10. **Physical Security and Workstations**. Any facilities containing the Blattner Tech Systems will, at a minimum: (a) be structurally designed to withstand adverse weather and other reasonably predictable natural conditions; (b) implement appropriate physical environmental safeguards to protect systems from damage related to smoke, heat, water, fire, humidity, or fluctuations in electrical power; (c) be supported by uninterruptible power supplies and on-site backup power generating systems; (d) implement appropriate controls to ensure that only authorized personnel are allowed physical access to the facility; (e) use industry standard processes to dispose of physical components containing Customer Confidential Information; and (f) utilize, at minimum, WPA2 for all wireless network security. Any Workstations that Blattner Tech uses to access Customer's Confidential Information will: (i) be documented and tracked in a formal asset management system; (ii) utilize encrypted hard drives; (iii) have an installed and functional software-based firewall; (iv) ensure operating system and applications have all critical patches installed within two (2) weeks; (v) accept only passwords that comply with the Password Security Requirements; and (vi) have a screen saver that activates after no more than fifteen (15) minutes of inactivity.
11. **Production System Reliability**. Blattner Tech will ensure, and will cause Affiliates of Blattner Tech and Subcontractors to ensure, as applicable, that all networking components, SSL accelerators, load balancers, web servers, application servers, database servers, and storage devices used to provide the Services, including the Software Services are configured using accepted industry-standard redundant design methodology, including, at a minimum: (a) web and database server clustering and load balancing; (b) file system and database mirroring, replication, or other equivalent technologies; and (c) carrier-class disk storage using RAID disks and multiple data paths.

12. **Backup and Data Recovery Procedures**. Blattner Tech will: (a) ensure that Customer Confidential Information is backed up, encrypted, and stored in a location and format available for retrieval as needed up to the last committed transaction; (b) store copies of Customer Confidential Information and data recovery procedures in a different place from where the primary computer equipment processing the Customer Confidential Information is located; (c) have specific procedures in place governing creation of and access to copies of Customer Confidential Information; (d) review data recovery procedures applicable to Customer Confidential Information at least every six (6) months; and (e) with respect to Customer Confidential Information, maintain a log of all restoration efforts, the description of the restored data, the Person responsible for restoration, and which data (if any) required manual input during the data recovery process.
13. **Disaster Recovery and Business Continuity**. Blattner Tech currently has and will maintain at all times an appropriate disaster recovery, business continuity and contingency plan and related policies and procedures (collectively, the "**DR Plan**") agreed upon by Blattner Tech and Customer in writing and will furnish a summary of its DR Plan to Customer in writing upon execution of this Security Datasheet. The DR Plan will provide for continued operation in the event of a catastrophic event affecting Blattner Tech's business operations and will be in accordance with internationally accepted business continuity, contingency and disaster recovery planning standards, procedures and practices, including, but not limited or restricted to the following minimum requirements: (a) a disaster recovery facility that is geographically remote from its primary data center, along with all required hardware, software, and Internet connectivity sufficient to provide the Software Services without substantial reduction or degradation of functionality or availability, in the event the primary data center were to be rendered unavailable; (b) secure backup copies of the Customer Confidential Information that is not stored on a Customer System; (c) restoration of the Software Services within twelve (12) hours after Blattner Tech's declaration of a disaster; and (d) maximum data loss of four (4) hours. Blattner Tech will notify Customer as soon as possible after it deems a service outage to be a disaster and will address any such outage in accordance with the terms of its DR Plan. Blattner Tech will test all features of its DR Plan at least once per calendar year and will provide the results of such tests to Customer upon request.
14. **Logging**. The Blattner Tech Systems and Workstations used in performing the Services and the Software Services will provide, where applicable, the following minimum logging capabilities and/or features: (a) enabled, active, and configured firewalls, routers, network switches and operating systems with logging capabilities to record both successful and unsuccessful authentications or event records in sufficient detail to the respective default logging destination or to a centralized syslog server (for network systems) for diagnostic and analytical purposes in the event of an Information Security Incident; (b) recorded access log entries containing, at a minimum, the date, time, user ID, URL requested or entity ID operated on, operation performed (viewed, edited, etc.) and source and destination IP address; and (c) the ability to track certain administrative changes to the Blattner Tech Systems and Workstations used in performing the Services and the Software Services (such as password changes and adding custom fields) in a "Setup Audit Log" (all of the foregoing, the "**Log Records**"). All Log Records must be made available for viewing, download, and local storage by Customer and maintained for a minimum of one hundred twenty (120) days in a physically and virtually secured location. Blattner Tech will, and will cause Affiliates of Blattner Tech and Blattner Tech Personnel to, upon request, provide to Customer copies of any Log Records.
15. **Intrusion Detection/Prevention**. Blattner Tech will monitor the Software Services and the Blattner Tech Systems for unauthorized access, interception, or interruption using accepted industry-standard network-based intrusion detection or prevention mechanisms.
16. **Malicious Software; Virus Protection**. Blattner Tech and, as applicable, Affiliates of Blattner Tech and Subcontractors will install and maintain on all Workstations and Blattner Tech Systems ICSA Labs certified Anti-Virus Software which use real time protection features which are maintained in accordance with the Anti-Virus Software vendor's recommended practices. In addition, Blattner Tech will ensure and, as applicable, cause Affiliates of Blattner Tech and Subcontractors to ensure that: (a) the Anti-Virus Software checks for new Anti-Virus Signatures at least daily; and (b) the Anti-Virus Signatures are current. Blattner Tech will and, as applicable,

cause Affiliates of Blattner Tech and Blattner Tech Personnel to immediately remove any Malicious Software discovered or which may be present in the Blattner Tech Systems, Workstations or within the Software Services. All Software Services will perform real-time scanning on files and other data uploaded into the Software Services to identify and eliminate any files or other data containing Malicious Software.

17. **No Disabling Devices**. Neither the Software Services nor the Blattner Tech Systems will utilize or otherwise introduce or permit any software routines or element capable of causing or enabling unauthorized access to, disabling, deactivating, deleting or otherwise damaging or interfering with any Customer Systems or the Systems of any Customer Affiliate.
18. **Data Encryption**. Blattner Tech will, and as applicable, cause Affiliates of Blattner Tech and Subcontractors to implement and utilize industry standard best practices that incorporate at a minimum, 256-bit VeriSign SSL Certification and minimum 2048-bit RSA public keys to protect Customer Confidential Information, including during transmissions between Customer's network and the Blattner Tech Systems. Customer Confidential Information and any backups of Customer Confidential Information at rest will be encrypted according to industry standard best practices that incorporate, at minimum Advanced Encryption Standard (AES) disk encryption with a minimum key length of 128 bits.
19. **System Audits**. At any time after the first anniversary of the Effective Date, Customer may elect to conduct a data security audit to benchmark Blattner Tech's then-current data security practices against the best practices of leading providers of services that are the same as or similar to Services provided by Blattner Tech. If any such audit reveals that the data security practices and processes then utilized by Blattner Tech are not consistent with industry best practice, then Customer and Blattner Tech will promptly establish and implement a plan to implement identified best practices into the Services.
20. **Right to Monitor**. Customer will have the right to monitor Blattner Tech's compliance with the terms of the Amendment and this Security Datasheet. During normal business hours, and with thirty (30) days notice, Customer, an Affiliate of Customer or their respective authorized representatives may inspect Blattner Tech's facilities and equipment, and any information or materials in Blattner Tech's possession, custody or control, relating in any way to Blattner Tech's obligations under the Agreement or this Security Datasheet. An inspection performed pursuant to this Security Datasheet will not unreasonably interfere with the normal conduct of Blattner Tech's business. Blattner Tech will cooperate fully with any such inspection initiated by Customer. Blattner Tech will deal promptly and appropriately with any inquiries from Customer relating to the Processing of Customer Personal Data.
21. **Subcontractors**. Blattner Tech will perform sufficient due diligence prior to the retention of any Subcontractor to ensure that such Subcontractor will not, in any way, compromise the security, confidentiality, availability or integrity of any Customer Confidential Information. Further, Blattner Tech will ensure that the terms of its subcontract with any Subcontractor are consistent with the responsibilities and obligations of the Agreement and this Security Datasheet. Blattner Tech will take appropriate action to cause its Affiliates and Blattner Tech Personnel to be advised of and comply with the applicable terms and conditions of the Agreement and the Security Datasheet, and will ensure that Blattner Tech Personnel are trained regarding their handling of Customer Confidential Information and the associated obligations under the Agreement and Security Datasheet.
22. **Access to Confidential Information**. Blattner Tech will ensure, by applying appropriate means, that any Blattner Tech Personnel that has access to Customer Confidential Information will have access based on a least privilege approach/need to know principle. Blattner Tech will also maintain policies that limit Blattner Tech, Blattner Tech Affiliates, or Blattner Tech Personnel from using personally-owned Workstations for the processing of Customer Confidential Information. Blattner Tech will not remove Customer Confidential Information from its location or otherwise copy Customer Confidential Information unless that removal or retention is reasonably necessary to perform the Services. Customer Confidential Information must always be anonymized/obfuscated before transfer to non-live environments.

23. **Customer Data**. Customer Data is and will at all times remain the property of Customer. Blattner Tech will ensure that all Customer Data will be kept strictly separated from Blattner Tech's data and data of any other client by appropriate technical means. Without limiting the generality of any obligations under the Agreement or this Security Datasheet, Blattner Tech shall not use or permit use of the Customer Data to market or solicit any business for any of Blattner Tech's, or its Affiliates', products or services or those of any Blattner Tech Personnel. Unless expressly agreed to by Customer in writing, neither Blattner Tech, nor its Affiliates or Blattner Tech Personnel shall have the right to aggregate Customer Data.
24. **Vulnerability Management**. If providing Software Services, Blattner Tech shall have in place a comprehensive vulnerability management program for the regular (minimum monthly) identification, categorization and timely remediation of technical and process vulnerabilities at the infrastructure and application layers of the Blattner Tech System(s) provided. Software patches to correct vulnerabilities must be installed and activated within the following timeframes:

Vulnerability Severity	Timeline
Critical	24 hours
High	48 hours
Medium	72 hours

25. **PCI Compliance**.

25.1. PCI Compliance Documentation. If Blattner Tech is providing payment processing services or the Software Services include payment processing functionality, Blattner Tech represents and warrants that Blattner Tech: (a) is presently compliant with all applicable PCI DSS Requirements and PA DSS Requirements; (b) has registered as a service provider with all required entities (e.g., Visa, MasterCard, etc.); (c) to the extent required by the PCI DSS Requirements and/or the PA DSS Requirements (i.e., after reaching appropriate transaction thresholds) Blattner Tech has undergone an assessment against PCI DSS Requirements and PA DSS Requirements performed by an independent Qualified Security Assessor (a "**QSA**") within the last twelve (12) months; (d) maintains a current, compliant Attestation of Compliance certificate, a report of validation, a report on compliance and any exceptions noted therein (collectively, the "**Compliance Documentation**"), under PCI DSS Requirements; and (e) will make the Compliance Documentation available for Customer's review upon request.

25.2. PCI Non-Compliance Event. Blattner Tech covenants and agrees to be and remain in compliance with all applicable PCI DSS Requirements and PA DSS Requirements and to perform the necessary steps to validate its compliance with PCI DSS Requirements and PA DSS Requirements and shall notify Customer immediately in the event of any of the following (individually, a "**Non-Compliance Event**"): (a) Blattner Tech learns or has reason to believe that it is no longer in compliance with PCI DSS Requirements and/or PA DSS Requirements; or (b) Blattner Tech undergoes an adverse change in its certification or compliance status with respect to PCI DSS Requirements and/or PA DSS Requirements. Upon the occurrence of a Non-Compliance Event, Blattner Tech will immediately provide Customer with a detailed plan to remediate such Non-Compliance Event. In the event Blattner Tech cannot provide, after reasonable prior notice from Customer, validation of its compliance with PCI DSS Requirements and/or PA DSS Requirements and the necessary Compliance Documentation as required under this Agreement, Customer shall have the right to engage a QSA to conduct an audit of Blattner Tech to determine Blattner Tech's compliance with PCI DSS Requirements and PA DSS Requirements, and Blattner Tech shall pay all costs of such an audit. Any such audit shall be conducted by a QSA on behalf of Customer and shall be conducted so as to reasonably minimize any disruption to Blattner Tech's operations. Blattner Tech shall reasonably cooperate with such QSA, including providing reasonable access to its facilities and applicable personnel necessary to audit and test compliance. Blattner Tech shall implement any remediation measures recommended by such QSA as soon as

reasonably possible in order either to remain certified as compliant with PCI DSS Requirements and PA DSS Requirements or to re- obtain certification under PCI DSS Requirements or PA DSS Requirements and shall provide a detailed plan with respect to any recommended remediation measures. Blattner Tech acknowledges that it is solely responsible at all times for the security of any Payment Information or cardholder data in transit, at rest or in its possession. A failure of Blattner Tech to maintain certification of its compliance with PCI DSS Requirements and/or PA DSS Requirements shall be considered a material breach of the Agreement by Blattner Tech.

25.3. Investigation of PCI Information Security Incident. In the event of an Information Security Incident and in addition to other obligations arising from such Information Security Event, Blattner Tech shall provide full access to PCI members and/or PCI- approved entities so that such Information Security Incident may be thoroughly investigated without restriction. Blattner Tech shall maintain the security of any Payment Information provided to Blattner Tech for the duration of the Agreement and for the life of the Payment Information after the expiration or earlier termination of the Agreement. Blattner Tech agrees to incorporate best practices security in its software to prevent the interception of transaction data, including Payment Information.

26. **Compliance with Data Privacy Laws and Regulatory Compliance and Changes**. Blattner Tech will comply, and will cause all Affiliates of Blattner Tech and Blattner Tech Personnel to comply with: (a) all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality or security of Customer Data including, without limitation, the Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation), the European Union Directives governing security of network and information systems (Directive 2016/1148), privacy and electronic commerce and communications (Directive 2002/58/EC), and data retention (Directive 2006/24/EC); the Canadian Customer Personal Data Protection and Electronic Documents Act (PIPEDA) and relevant provincial laws; the Gramm-Leach-Bliley Act ("**GLBA**"), 15 U.S.C. § § 6801-6827, and all regulations implementing GLBA; the Fair Credit Reporting Act ("**FCRA**"), 15 U.S.C. § 1681 et seq., as amended by the Fair and Accurate Credit Transactions Act ("**FACTA**"), and all regulations implementing the FCRA and FACTA; the Controlling the Assault of Non- Solicited Pornography and Marketing Act (CAN-SPAM); information security breach notification laws (such as Cal. Civ. Code §§ 1798.29, 1798.82 - 1798.84 and Tenn. Code Ann. §47-18-2107); laws imposing minimum information security requirements (such as Cal. Civ. Code § 1798.81.5 and 201 Mass. Code Reg. 17.00); laws requiring the secure disposal of records containing certain Customer Data (such as, but not limited to, N.Y. Gen. Bus. Law § 399-H), and all similar international, federal, provincial, state and local requirements; (b) all applicable industry standards concerning privacy, data protection, confidentiality or information security; and (c) applicable provisions of Customer's written requirements or the written requirements of any Affiliate of Customer currently in effect and as they become effective relating in any way to the privacy, confidentiality and security of Customer Data or applicable privacy policies, statements or notices that are provided to Blattner Tech in writing.
27. **Authority to Process Customer Personal Data**. Blattner Tech, Affiliates of Blattner Tech, and Blattner Tech Personnel will Process Customer Personal Data only on behalf of and for the benefit of Customer and its Affiliates, for the purposes of Processing Customer Personal Data in connection with the Agreement, and to carry out its obligations pursuant to the Agreement and Customer's written instructions or the written instructions of an Affiliate of Customer. Customer will have the exclusive authority to determine the purposes for and means of Processing Customer Personal Data for itself and on behalf of its Affiliates. Blattner Tech will ensure that its personnel who have access to Confidential Information or Customer Personal Data are informed of the confidential nature of the Confidential Information or Customer Personal Data through appropriate training on their responsibilities to access such types of information.
28. **Cross Border Data**. Blattner Tech will not, and will prevent Affiliates of Blattner Tech and Blattner Tech Personnel from Processing, disseminating, or transferring Customer Personal Data outside the country (or, if it

was originally delivered to a location inside the European Economic Area ("**EEA**") or Switzerland, outside the EEA or Switzerland) to which Customer, Affiliates of Customer or their respective personnel originally delivered it for Processing (a "**Cross-Border Data Transfer**") without the explicit written consent of Customer or the appropriate Affiliate of Customer, which may be withheld in its sole discretion. Blattner Tech shall enter into any written agreements as are necessary (in Customer's reasonable determination) to comply with Data Privacy Laws concerning any cross-border transfer of Customer Personal Data, whether to or from Blattner Tech.

29. **Safe Harbor Privacy Framework; EU-U.S. Privacy Shield Framework; EU Model Clauses; Binding Corporate Rules.** In the event of Customer's approval of Cross Border Data Transfers, then prior to instituting such Cross Border Data Transfer, Blattner Tech will at all times satisfy at least one (1) of the following requirements: (a) provide a valid certification to the United States Department of Commerce regarding Blattner Tech's compliance with the "EU-U.S. Privacy Shield Framework"; (b) execute the EU Model Contractual Clauses relating to personal data transfers; or (c) execute binding corporate rules recognized under Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation) (each of (a)-(c), a "**Compliance Method**"). If at any time Blattner Tech's compliance with this section is based on a Compliance Method which is invalidated, Blattner Tech will either: (i) comply with the successor to such Compliance Method, if available; or (ii) comply with at least one (1) of the remaining valid Compliance Method(s). Further, the Software Services and the Blattner Tech Systems will employ operational controls sufficient to enable Blattner Tech to Process Customer Personal Data in accordance with the privacy standards set forth in the "Safe Harbor Privacy Framework" accepted by Switzerland and Israel (and any other jurisdictions that announce such acceptance during the term of the Agreement) or other industry standard.
30. **Information Security Incident Response**. Blattner Tech shall maintain security incident management policies and procedures, including detailed security incident escalation procedures. In the event of any Information Security Incident, Blattner Tech will, at its sole expense: (a) expeditiously (but in no case later than twenty-four (24) hours after Blattner Tech, an Affiliate of Blattner Tech, or Blattner Tech Personnel learns of an Information Security Incident) report such Information Security Incident to Customer, summarizing in reasonable detail the effect on Customer, Customer's Affiliates, the Customer systems or the business reputation of Customer or any of its Affiliates, if known; (b) investigate (with Customer's participation or the participation of an independent third party forensic investigator if requested by Customer) such Information Security Incident and cooperate with Customer and its designees in respect of any investigation by Customer of or any such Person relating to security or Information Security Incident, including, but not limited to, providing any information or material relevant to such security breach in Blattner Tech's possession or control or in the possession or control of any Blattner Tech Personnel or any subcontractor; (c) perform a risk assessment and develop a corrective action plan and provide a written report to Customer of such risk assessment and action plan taken or to be taken by Blattner Tech; (d) prepare and (following Customer's approval) implement a remediation plan to take all necessary and advisable corrective actions and cooperate fully with Customer and all Affiliates of Customer in all reasonable and lawful efforts to prevent, mitigate, rectify and remediate the effects of the Information Security Incident; (e) ensure that such report contains all information necessary to: (i) conduct an appropriate legal analysis to determine compliance with all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective (including, without limitation, Data Privacy Laws); and (ii) determine the extent to which notification and communication to the Affected Persons (defined below) is advisable or required by any Laws; (f) make all Blattner Tech Personnel available for interview; (g) mitigate, as expeditiously as possible and to the extent practicable, any harmful effect of such Information Security Incident that is known to Blattner Tech, Affiliates of Blattner Tech or Blattner Tech Personnel; (h) cooperate with Customer and all Affiliates of Customer and their respective personnel in providing any filings, communications, notices, press releases or reports related to any Information Security Incident; and (i) cooperate with Customer and its designees in respect of implementing new security measures. The content of any filings,

communications, notices, press releases or reports related to any Information Security Incident must be approved by Customer prior to any publication or communication thereof.

31. **Information Security Incident Expenses**. In addition to the indemnification obligations of Blattner Tech set forth in the Agreement, Blattner Tech will defend, indemnify and hold Customer, its Affiliates, and their respective officers, directors, employees and agents, harmless from and against any and all claims, suits, causes of action, liability, loss, costs and damages, including reasonable attorney fees, arising out of or relating to any Information Security Incident including but not limited to: (a) expenses incurred to provide warning or notice to Customer's former and current employees, suppliers, customers, and other Persons whose Customer Personal Data may have been disclosed or compromised as a result of the Information Security Incident (the "**Affected Persons**") and to law-enforcement agencies, regulatory bodies or other third parties as required to comply with law, including Data Privacy Laws, or as otherwise directed by Customer or an Affiliate of Customer; (b) expenses incurred either by Customer, an Affiliate of Customer, or through such Affiliate's retention of a independent third party forensic investigator, legal counsel, or any other third party, to investigate assess or remediate the Information Security Incident and to comply with applicable laws and/or relevant industry standards; (c) expenses related to the reasonably anticipated and commercially recognized consumer data breach mitigation efforts, including, but not limited to costs associated with the offering of credit monitoring for a period of at least twelve (12) months or such longer time as is required by applicable laws or recommended by one or more of Customer's regulators or any other similar protective measures designed to mitigate any damages to the Affected Persons; (d) expenses incurred to retain a call center or to develop any internal or external communication materials in order to respond to inquiries regarding the Information Security Incident for a period of at least one hundred eighty (180) days or such longer time as is required by law; (e) fines, penalties, or interest that Customer or any Affiliate of Customer pays to any governmental or regulatory authority; (f) legal expenses incurred in connection with a Information Security Incident or to address any claims by third parties as a result of the Information Security Incident or investigation by law-enforcement agencies or regulatory bodies; and (g) expenses incurred to the retention of a public relations or crisis management firm in order to manage communications on behalf of Customer and its Affiliates related to any Information Security Incident.
32. **No Violation of Privacy and Information Security Requirements**. Blattner Tech represents and warrants that no applicable law, or legal requirement, or privacy or information security enforcement action, investigation, litigation or claim prohibits Blattner Tech from: (a) fulfilling its obligations under the Agreement and the Security Datasheet; or (b) complying with instructions it receives from Customer or an Affiliate of Customer concerning Customer Confidential Information. Blattner Tech will enter into any further privacy or information security agreement requested by Customer or an Affiliate of Customer.
33. **Lost or Improperly Destroyed Customer Confidential Information**. Blattner Tech will not, and will not permit any Affiliates of Blattner Tech or Blattner Tech Personnel to delete or destroy any Customer Confidential Information or media on which Customer Confidential Information resides without prior authorization from Customer. Customer hereby authorizes Blattner Tech to delete or destroy Customer Confidential Information in accordance with any Customer document retention policies or as otherwise directed by Customer in writing. Blattner Tech will, and will cause its Affiliates and Blattner Tech Personnel to maintain and provide to Customer one or more reports that identify the Customer Confidential Information, including media, that has been destroyed and sanitized as applicable in accordance with the then most current version National Institute of Standards and Technology or ("**NIST**") special publication 800-88 Guidelines for Media Sanitization. In the event any Customer Confidential Information is lost or destroyed due to any act or omission of Blattner Tech, Affiliates of Blattner Tech, or Blattner Tech Personnel, including any Information Security Incident, Blattner Tech will restore or will cause the applicable Blattner Tech Affiliate or Subcontractor to restore such Customer Confidential Information using the most recent available back-up. Blattner Tech will prioritize this effort to minimize any adverse effect upon the business of Customer or its Affiliates or use of the Software Services and the Blattner Tech Systems. Customer agrees to cooperate with Blattner Tech to provide any available information, files, or raw data needed for the regeneration, reconstruction, or replacement of the Customer Confidential Information. If Blattner Tech or

the applicable Blattner Tech Affiliate or Subcontractor fails to fully regenerate, reconstruct and/or replace any lost or destroyed Customer Confidential Information within the time reasonably set by Customer, then Customer may, at Blattner Tech's expense, obtain data reconstruction services from a third party, and Blattner Tech will cooperate, and will cause the applicable Affiliate of Blattner Tech, Subcontractor, or Blattner Tech Personnel to cooperate with such third party as requested by Customer or an Affiliate of Customer. If it is determined that Customer Confidential Information has been lost or destroyed as a result of the willful, intentional, or negligent acts or omissions of Blattner Tech, an Affiliate of Blattner Tech, Subcontractor, or Blattner Tech Personnel, Customer may terminate the Agreement for cause and pursue any civil and criminal actions available to it.

34. **Return or Intentional Destruction of Customer Confidential Information**. Blattner Tech will, and will cause its Affiliates and Blattner Tech Personnel to permanently delete and destroy Customer Confidential Information (or the portion of such Customer Confidential Information specified by Customer or an Affiliate of Customer) and/or will return such Customer Confidential Information to Customer, an Affiliate of Customer or their respective designees, in the format and on the media prescribed by Customer, as follows: (a) within thirty (30) days from the expiration or termination of the Agreement and completion of each Party's obligations hereunder and; (b) at any time Customer or an Affiliate of Customer requests Customer Confidential Information within thirty (30) days from Customer's request. Blattner Tech will deliver to Customer written certification of its compliance with this paragraph and the compliance by its Affiliates and Blattner Tech Personnel signed by an authorized representative of Blattner Tech. Where it is not technically feasible and/or commercially practicable for Blattner Tech or a Blattner Tech Affiliate or Subcontractor to permanently delete or destroy Customer Confidential Information held in electronic form, Blattner Tech will ensure, and will cause its Affiliates and Blattner Tech Personnel to ensure that any residual Customer Confidential Information which is retained under its custody or control is permanently put beyond use and not Processed any further save for the mere retention of such residual information. In no event will Blattner Tech, or any Blattner Tech Affiliate or Subcontractor withhold any Customer Confidential Information as a means of resolving any dispute.
35. **Indemnity**. In addition to any other indemnification obligation contained in the Agreement and in Section 31 above, Blattner Tech shall indemnify, defend and hold Customer, its officers, directors, employees, parent, subsidiaries and Affiliates, harmless from and against any and all claims, demands, losses, liabilities, costs and expenses, including attorneys' fees and in-house counsel fees, arising from a breach of this Security Datasheet by Blattner Tech, its employees, agents, representatives or Blattner Tech Personnel from acts or omissions of Blattner Tech or Blattner Tech Personnel relating to Customer Confidential Information.
36. **Electronic Discovery**. Blattner Tech shall maintain end-to-end electronic discovery capabilities consistent with generally acceptable standards and compliant with all regulations and laws. At a minimum, Blattner Tech shall perform the following functions:
    (a) upon receiving written notice from Customer to preserve and collect electronic data relevant to a matter, Blattner Tech shall take reasonable and immediate steps to preserve and collect all electronic data relevant to a case in a forensically sound manner;
    (b) Blattner Tech shall maintain detailed documentation of all activities related to the preservation and collection of electronic data, including without limitation chain of custody; and (c) at the request of Customer's legal counsel or its designated representative, Blattner Tech shall search collected data and provide the results to Customer or its designated third party.
37. **No Prior Events**. Blattner Tech represents and warrants to Customer that within the six (6) months prior to the effective date of this Agreement, Blattner Tech and its Affiliates and Subcontractors have not suffered an Information Security Incident.
38. **New Products**. Blattner Tech may not provide any new Service, or product in connection with the Service, without first obtaining either: (a) consent from Customer permitting such change; or (b) a fully executed amendment or addendum to this Security Datasheet addressing such change. Neither Customer nor any Affiliate will be liable to Blattner Tech or its Affiliate, and will not incur any payment obligations for products or Services not accepted due

to the lack of both (a) and (b). The acceptance of a new product or Service without (a) or (b) above does not constitute a waiver of any rights or obligations under the Agreement and this Security Datasheet. A breach of this section by Blattner Tech is deemed a material breach of the Agreement.

39. **Notification.** Any notification required from Blattner Tech to Customer pursuant to this Security Datasheet shall be provided to the Customer representative set forth in the Agreement.
40. **Modifications of Terms**. This Security Datasheet, as executed and approved, shall not be modified except by written amendment signed by the Parties expressly stating their intent to modify the terms of this Security Datasheet.
41. **Headings; Interpretations**. The descriptive headings of the sections of this Security Datasheet are inserted for convenience only and shall not control or affect the meaning or construction of any provision hereof. In this Security Datasheet, unless the context otherwise requires: (a) the term “days” means calendar days; and (b) the term “including” shall mean, “including, without limitation.”