**Participating Provider Pass-Through Terms for the Apple Access Platform**

These Terms and Conditions ("Terms and Conditions") are in addition to the business partner agreement and Related Services ("Terms of Service"). These additional terms apply if You use Apple Access Technology to securely execute instructions given by Users via Apple Access Technology and for the purpose of enabling Users to securely use Provisioned Credentials to make Transactions (the "Program"). All foregoing terms shall have the meaning set forth below.

**In the event of a conflict between these Terms and Conditions and the Terms of Service, these Terms and Conditions shall govern with respect to Your use of the Apple Access Technology.**

**Definitions.**

"Access Partner" shall mean business partner agreement or an affiliated entity of Kastle System International, LLC.

"Access Partner Data" means any data supplied by Access Partner to Apple or Participating Provider for the purpose of facilitating Participating Provider's provisioning path decision process.

"Access Partner Technology" means Technology owned, controlled or licensable by Access Partner or any of its Affiliates (other than Apple Technology).

"Access Services" means the provisioning of Apple Access Technology to Participating Providers to enable Users to virtually authenticate to and/or to gain access to a physical space or service to utilize such physical space or service controlled or provided by a Participating Provider.

"Account" means any account under which a User may initiate any Access Service through Participating Provider pursuant to a User Agreement.

"Affiliate" means, with respect to a party, any Person that controls, is controlled by, or is under common control with such party. As used in this definition, the term "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of voting securities, by contract, or otherwise. For the avoidance of doubt, but not by way of limitation, the direct and indirect ownership of more than fifty percent (50%) of (i) the voting securities or (ii) an interest in the assets, profits, or earnings of a Person will be deemed to constitute "control" of the Person.

"Apple Access Guidelines" means documentation outlining the minimum program requirements and best practice guidelines that are required to support Access Services and/or the Program. Such Apple Access Guidelines may be updated from time to time will and be provided by Access Partner as a .pdf upon request until a hyperlink becomes available.

"Apple Access Platform" means Apple's platform that utilizes Apple Technology, and may utilize Access Partner Technology pursuant to Apple's agreement with Access Partner, to enable Users to gain access to or authenticate virtually to use a physical space or controlled service using physical, digital or virtual access cards, credentials or account access devices and to access other related services using Apple Products designated by Apple or any of its Affiliates.



KASTLE

"Apple Product" means any Technology, product, or service distributed under an Apple Mark, or used internally and under development for distribution under an Apple Mark or an Apple Affiliate.

"Apple Access Technology" means the Apple Technology that enables Users to gain access to a physical space or controlled service, or authenticate virtually to use (physically, virtually, or otherwise) Participating Provider services, using Apple Products designated by Apple or any of its Affiliates.

"Apple Brand Guidelines" means the guidelines set forth at http://www.apple.com/legal/trademark/guidelinesfor3rdparties.html ("Apple Trademark and Copyright Guidelines") and https://developer.apple.com/apple-pay/marketing ("Apple Pay Marketing Guidelines").

"Apple Marks" means all Marks set forth in Exhibit C (Apple Marks), as may be amended by Apple from time to time. "Apple Technology" means Technology owned, controlled or licensable by Apple or any of its Affiliates.

"Credential" means any digital or virtual card, account access device, or other device capable of accessing an Account issued by Access Partner at the request of Participating Provider for the purposes of initiating an Access Service.

"Effective Date" means the Effective Date of your Terms of Service applicable to Your use of business partner agreement.

"Enabled Device" means any Apple Product that has been enabled to store and/or transmit Provisioned Credentials.

"Governmental Authority" means any domestic or foreign, federal, state, provincial, municipal or local government, any political subdivision thereof and any entity exercising executive, legislative, judicial, regulatory, or administrative functions of or pertaining to government, regardless of form, including any agency, bureau, court, tribunal, or other instrumentality.

"Intellectual Property Rights" means the rights in and to all (i) patents and patent applications in any jurisdiction or under any international convention claiming any inventions or discoveries made, developed, conceived, or reduced to practice, including all divisions, divisionals, substitutions, continuations, continuations-in-part, reissues, re-examinations, renewals and extensions thereof; (ii) copyrights; (iii) confidential information and other proprietary information or data that qualifies for trade secret protection; (iv) semiconductor chip or mask work rights; (v) design patents or industrial designs, and (vi) other similar intellectual or other proprietary rights (excluding all Marks) now known or hereafter recognized in any jurisdiction.

"Law" means any federal, state, local or foreign law (including common law), code, statute, ordinance, rule, regulation, published standard, permit, judgment, writ, injunction, rulings or other legal requirement.

"Marks" means all trademarks, service marks, trade dress, trade names, brand names, product names, business marks, logos, taglines, slogans, and similar designations that distinguish the source of goods or services, whether registered or unregistered, along with all registrations and pending applications for any of the foregoing.

"Non-Apple Access Service" means any software, other than the Apple Pay Technology, that enables the use of a digital or virtual card for the purposes of gaining access to a physical space or authenticating to utilize a controlled service on personal electronic devices.



KASTLE

"Participating Provider" shall mean You as the End Customer.

"Participating Provider Data" means all information related specifically to an Account, Credential, Participating Provider, and/or User that is obtained, generated or created by or on behalf of such Participating Provider in connection with Account establishment, processing and maintenance activities, customer service, and transaction data (as enumerated in the Apple Access Guidelines).

"Participating Provider Properties" means properties owned, leased, or controlled by Participating Provider that are participating in the Program.

"Participating Provider Technology" means Technology owned, controlled or licensable by Participating Provider or any of its Affiliates.

"Person" means any individual, corporation, limited liability company, partnership, firm, joint venture, association, trust, unincorporated organization, Governmental Authority or other entity.

"Provisioned Credential" means a Credential that has been provisioned to an Enabled Device so that the Enabled Device may be used to make Access Services available using such Provisioned Credential.

"Service Provider" means any subcontractor, independent contractor, or third party service provider engaged by a party to provide a service on behalf of such party.

"Technology" means any information, ideas, know-how, designs, drawings, specifications, schematics, software (including source and object codes), manuals and other documentation, data, databases, processes (including technical processes and business processes), or methods (including methods of operation or methods of production).

"Transaction" means using an Enabled Device to gain access to a physical space, or utilize a service controlled or provided by an entity that controls access to physical spaces, in locations agreed to by Access Partner, Participating Provider and Apple.

"User" means a Person that has entered into a User Agreement establishing an Account with a Participating Provider.

"User Agreement" means the agreement between Participating Provider and a User (and any replacement of such agreement), establishing a User Account and governing the use of a Credential, together with any amendments, modifications or supplements that may be made to such User Agreement (and any replacement of such agreement).

**Terms.**

All aspects of the Participating Provider implementation will meet the Apple Access Guidelines.

- Participating Provider will ensure that Provisioned Credentials can be used everywhere physical access credentials can be used in Participating Provider Properties, unless an exception is pre-approved in writing by Access Partner and based on guidelines provided by Apple.
- To support the end-to-end user mobile contactless experience, if Participating Provider Properties are enabled for the hospitality use case, all Participating Provider's payment systems accepting payment cards

(credit/debit) at such properties will accept Apple Pay (including Apple Pay Cash, as described in the Apple Access Guidelines), unless an exception is pre-approved in writing by Apple.

- For provisioning of Credentials, Participating Provider will authorize Access Partner to send data, including Access Partner Data in its possession or control, and any other necessary identifiers for Credentials issued by Participating Provider to Apple necessary to provision credentials.

Participating Provider will support Users by ensuring that the level of service (both in quality and the types of transactions that can be supported) provided for Provisioned Credentials is at least on parity with the level of service provided to physical credentials and credentials offered by Non-Apple Access Services.

Participating Provider will be responsible for the management of the relationship with Users, including being responsible for: (i) the decision to approve or deny provisioning of Credentials to an Enabled Device; (ii) the right to decline the use of a Provisioned Credential to make Transactions (where technically possible to do so); (iii) the on-going management and operation of Accounts, including whether any Provisioned Credential, should be suspended or deactivated; and (iv) providing all access services to Users in connection with Provisioned Credentials.

Apple (on behalf of itself and each of its Affiliates) hereby grants Participating Provider and each of its Affiliates, during the term, a non-exclusive, non-assignable, non-transferable, non-sublicensable, royalty-free, fully paid-up, worldwide right and license to use, reproduce, have reproduced, display, and have displayed any of the Apple Marks solely for the purposes of announcing and promoting the provisioning of Credentials on Enabled Devices at Participating Provider Properties, subject in all cases to Apple's prior written consent. Use of the Apple Marks by Participating Provider, its Affiliates or Service Providers will be pursuant to, and in accordance with, the Apple Brand Guidelines, unless otherwise agreed in writing by Apple and Participating Provider. For the avoidance of doubt, in the event Participating Provider wishes to use any of the Apple Marks in any paid advertising, Participating Provider must first obtain Apple's written consent for such advertising. Apple represents and warrants that, as of the Effective Date, Apple has the right to grant all of the licenses and other rights granted to Participating Provider and each of its Affiliates and Service Providers in these Terms and Conditions. For clarity, the foregoing license shall terminate immediately upon termination of Participating Provider's participation in the Program for any reason.

Participating Provider will ensure that the level of user awareness (both in quality and the types of use cases featured) provided by Participating Provider for Provisioned Credentials is at least on parity with the user awareness provided for physical credentials and/or credentials on Non-Apple Access Services.

Participating Provider will market and describe the Program to potential users in accordance with the Apple Pay Marketing Guidelines unless an exception is pre-approved by in writing Apple.

In no event will Participating Provider promote or advertise the launch of credential services for Non-Apple Access Service using the Apple Access Guidelines or the Apple Pay Marketing Guidelines provided by Apple.

**System Changes**. Absent prior written notice to Access Partner, Participating Provider may not implement changes to its systems, procedures, processes or functionality, which, as the case may be, may have a material impact on: (a) the Apple Access Technology; (b) the manner in which Credentials are provisioned on an Enabled Device, or (c) the manner in which Credentials provisioned to an Enabled Device function or are processed on the Apple Access Technology (such changes to systems, procedures, processes or functionality are referred as to "System Changes"). In addition, and not by way of limitation, Participating Provider will (i) notify Access Partner not less than ninety (90) days prior to any System Change that Participating Provider reasonably believes will disable any core functionality of the Apple Access Technology, or introduce any material additional security exposure to Apple or consumers and (ii) provide support to Access Partner to work in good faith with Apple to address any bona fide concerns of Apple with regard to such proposed System Change. If Apple objects to any System Change, the System Change may not go forward until the objection is resolved.



**Intellectual Property**.

1. Participating Provider and its Affiliates own or have the right to use all Participating Provider Technology (and all Intellectual Property Rights therein or thereto). Apple and its Affiliates own or have the right to use all Apple Technology (and all Intellectual Property Rights therein or thereto).
2. Except as agreed in writing by Apple and Participating Provider, no other rights or licenses to exploit (in whole or in part), in any manner, form or media, any of the Technology, Intellectual Property Rights or Marks of the other party are granted. Nothing contained in these Terms and Conditions will be construed as constituting a transfer or an assignment to a party by the other party of any of the Technology, Intellectual Property Rights or Marks of such other party or any of its Affiliates.

**Governmental Authority.** Participating Provider shall promptly notify Access Partner if it is notified by any domestic or foreign, federal, state, provincial, municipal or local government, any political subdivision thereof or any entity exercising executive, legislative, judicial, regulatory, or administrative functions of or pertaining to government, regardless of form, including any agency, bureau, court, tribunal, or other instrumentality ("Governmental Authority"), or otherwise reasonably believes, upon advice of counsel, that it is not complying with any law applicable to Participating Provider due to the processes used by Apple, Access Partner or Participating Provider, for use and provisioning of Credentials using the Apple Access Platform.

**Confidentiality**. Participating Provider will protect Apple Confidential Information obtained pursuant to these Terms and Conditions from unauthorized dissemination and use with the same degree of care that it uses to protect its own like information. Apple will protect Participating Provider Confidential Information obtained pursuant to the Program from unauthorized dissemination and use with the same degree of care that it uses to protect its own like information. Except as expressly set forth herein, Participating Provider will not use the Apple Confidential Information for purposes other than those necessary to directly further the purposes of these Terms and Conditions. Except as expressly permitted under these Terms and Conditions, Participating Provider will not disclose to third parties the Apple Confidential Information without the prior written consent of Apple, including (i) the public disclosure of any metrics related to the Program and (ii) Participating Provider's planned participation in the Program prior to the public launch of Participating Provider's participation in the Program.

**Termination**. Apple may suspend or terminate Participating Provider's participation in the Program in the event of Participating Provider's breach of any of these terms and such breach is not remedied within thirty (30) days of receiving written notice of such breach by Apple. Participating Provider also acknowledges and agrees that any violation of the requirements set forth in these terms will be grounds for Apple to suspend the provisioning of Credentials to Enabled Devices.

**Data Privacy and Security**.

1. Participating Provider and Apple acknowledge that any information which directly or indirectly identifies individuals ("Personal Data") collected, accessed, processed, maintained, stored, transferred, disclosed, or used in relation to these terms, shall be done for each party's own benefit and not on behalf of the other party, and each party shall be independently and separately responsible for its own relevant activities. Participating Provider and Apple further acknowledge that Apple does not determine the purpose and means of the processing of Personal Data subject to these Terms and Conditions by Participating Provider, which is determined by Participating Provider solely in its own independent capacity. Participating Provider and Apple acknowledge and agree that the Access Partner is processing Personal Data in relation to the Program for the benefit of the Participating Provider as its data processor.
2. Solely in its own independent capacity and commitment to the protection of Personal Data, Participating Provider shall comply with **Exhibit B** ("**Apple Data Privacy and Information Security Terms**") and all applicable data protection laws (altogether, "Data Protection Laws"), including entering into data processing agreements as may be required with Access Partner and, where necessary, ensuring that international data transfers take place only in compliance with the conditions laid down in Data Protection Laws (for example, by executing approved

standard contractual clauses). Participating Provider must also ensure that its Service Providers are bound by the same privacy and security obligations as Participating Provider under these Terms and Conditions and will comply with the Data Protection Laws which shall continue to apply regardless of the location of processing of the data for which Participating Provider acts as data controller. Apple will comply with all Data Protection Laws with respect to the handling and use of Personal Data.

3. Participating Provider will promptly notify Access Partner and Apple if it (i) discovers that any person or entity has breached security measures relating to the Program, or gained unauthorized access to any data related to the Program, including Participating Provider Data, Access Partner Data, or Access Partner Provisioning Data, (in each such case an "Information Security Breach") or (ii) receives a written supervisory communication, written guidance or written direction from a Governmental Authority that requires a modification to or suspension of the provisioning of Credentials on Enabled Devices. Upon discovery of an Information Security Breach for which Participating Provider is responsible, the Participating Provider will, at its cost, (A) appropriately investigate, remediate, and mitigate the effects of the Information Security Breach and (B) provide Access Partner and Apple with assurances reasonably satisfactory to such parties that appropriate measures have been taken to prevent such Information Security Breach from recurring.

**Unauthorized Transactions**. Participating Provider acknowledges and agrees that Apple will not be liable to any party for any Transaction initiated by a person or party who is not authorized to make a Transaction on an Account, including without limitation any fraudulent Transaction.

**Parity with Physical Access Credential and other Access Services**. Participating Provider may not process or decline Transactions, or activate, suspend or cancel Credentials or Accounts, in a manner that discriminates against the Program compared to physical access credentials and Non-Apple Access Services.

**Reporting Data**. Participating Provider agrees to provide Apple (via Access Partner) the data and statistics identified in **Exhibit A (Reporting)** and in accordance with the Apple Access Guidelines (the "Reports"). Apple may use the data and statistics provided by Participating Provider for purposes of (1) performing its obligations and exercising its rights under these Terms and Conditions, or (2) improving the Apple Pay Technology and other Apple Products or technology used internally by Apple in connection with Apple Products.

**Pass Data**. Participating Provider expressly agrees to provide User Personal Data directly to Enabled Devices to support in the creation of representations of Credentials in accordance with Apple Access Guidelines and according to the User's preferences to the extent such provision is allowed under applicable Law.

**Third Party Beneficiaries**. **Apple** shall be entitled to rely upon, shall be an express **third party beneficiary** of, and shall be entitled to enforce, the provisions of these Terms and Conditions. The parties hereto agree that **Apple** shall be an express third-party beneficiary of these Terms and Conditions as provided herein.



KASTLE

**Exhibit A**

## Data to be included in Reports

The following reporting data must be collected by Access Partner (when acting as Credential Manager) and provided to Apple over an STFP that is hosted by such Access Partner. A report must contain aggregated data at the Participating Provider level.

All reporting metrics must be sent on a Daily, Weekly, and Monthly cadence.

**The following will be provided by Access Partner:**

A. Ever Provisioned - Apple Access

1) By Enabled Device type (i.e. iPhone and Apple Watch)

2) By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)

B. Live Credential - Apple Access

1) By Enabled Device type (i.e. iPhone and Apple Watch)

2) By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)

**Access Partner will provide the following data to Apple upon request, on a monthly or quarterly basis:**

A. Transaction - Apple Access

1) By Enabled Device type (i.e. iPhone and Apple Watch)

2) Optional, if available: By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)

3) By Transaction type (i.e. Door Access, Event)

B. Ever Provisioned – Other

1) Other Mobile Wallets

2) Physical/Plastic Cards

C. Live Credential – Other

1) Other Mobile Wallets

2) Physical/Plastic Cards

D. Transaction – Other

1) Other Mobile Wallets

i. By Transaction type (i.e. Door Access, Event,)

ii. By Transaction Status (i.e. Successful/Declines)

2) Physical Cards

i. By Transaction type (i.e. Door Access, Event,)

ii. By Transaction Status (i.e. Successful/Declines)

E. Total Enabled Users

1) By Device type (i.e. iPhone and Apple Watch)

2) By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)

Access Partner will provide the following data to Apple at the time of Participating Provider launch:

A. Total Eligible Users

1) By OS type (i.e. iOS, Android)

**"Live Credentials" means Credentials that have been provisioned and are "live" on a device*

*** "Enabled User" means individuals using an iPhone or Apple watch within a Participating Provider Property*



KASTLE

**Exhibit B**

## Apple Data Privacy and Information Security Terms

Unless otherwise defined, capitalized terms will have the same meaning as such terms in the Terms and Conditions. In the event of a conflict between this Exhibit B and the Terms and Conditions, this Exhibit B will control only with regard to the subject matter addressed in this Exhibit B.

Depending on the location of the use of the Provisioned Credential, "Apple" means Apple Inc., located at One Apple Park Way, Cupertino, California, for users in the United States, including Puerto Rico; Apple Canada Inc., located at 120 Bremner Blvd., Suite 1600, Toronto ON M5J 0A8, Canada for users in Canada; Apple Services LATAM LLC, located at 1 Alhambra Plaza, Ste 700 Coral Gables, Florida, for users in Mexico, Central or South America, or any Caribbean country or territory (excluding Puerto Rico); iTunes K.K., located at Roppongi Hills, 6-10-1 Roppongi, Minato-ku, Tokyo 106-6140, Tokyo for users in Japan; Apple Pty Limited, located at Level 3, 20 Martin Place, Sydney NSW 2000, Australia, for users in Australia or New Zealand, including in any of their territories or affiliated jurisdictions; and Apple Distribution International Ltd., located at Hollyhill Industrial Estate, Hollyhill, Cork, Republic of Ireland, for all other users.

Participating Provider confirms that this Exhibit B sets out its information security commitments regarding the handling of Personal Data by Participating Provider.

1. Protection of Personal Data.

To the extent that the Participating Provider (and Participating Provider's personnel, affiliates, employees, agents, contractors or subcontractors ("Provider Personnel")) may process certain information that identifies, relates to, is linked to or is capable of being linked to individuals ("Personal Data") in relation to the operation of the Terms and Conditions, the Participating Provider, undertakes in its own independent capacity, that such Personal Data will be collected, accessed, processed, maintained, stored, transferred, disclosed or used by it and its Provider Personnel for the Participating Provider's own benefit in connection with the performance of its obligations under the Terms and Conditions and not on behalf of Apple.

Participating Provider undertakes solely in its own independent capacity to (and will procure that all Provider Personnel): (i) comply with all applicable Laws, regulations and international accords or treaties pertaining to Personal Data; and (ii) take all appropriate legal, organizational and technical measures to protect against unlawful and unauthorized processing of Personal Data.

Participating Provider shall be liable for the damage caused to any Data Subject as a result of Participating Provider's or Provider Personnel's handling of Personal Data in connection with the Terms and Conditions, including (without limitation) where Participating Provider or Provider Personnel has not complied with its commitments under this Exhibit B or any applicable Laws, regulations and international accords or treaties pertaining to Personal Data.

2. Data Security Procedures.

Participating Provider undertakes solely in its own independent capacity to (and will procure that all Provider Personnel will) maintain reasonable operating standards and security procedures, and shall use their best efforts to secure Personal Data and Confidential Information (collectively, "Confidential Data") through the use of reasonable and appropriate administrative, physical, and technical safeguards including, but not limited to, appropriate network security and encryption technologies governed by an established set of policies and procedures (an "Information Security Management System"). Participating Provider shall maintain and

regularly update the Information Security Management System based upon a formal change control process that governs how security controls are adjusted over time ensuring at all times that it maintains a comparable or better level of security than that defined in this Exhibit B. Such Information Security Management System shall: (A) ensure the ongoing confidentiality, integrity, availability, and resilience of Participating Provider systems and services processing Confidential Data and those of subcontractors that have been authorized by Apple to process Confidential Data; (B) enable Participating Provider to restore the availability and access to Confidential Data in a timely manner in the event of a physical or technical incident; (C) maintain a process for regularly testing, assessing, and evaluating the effectiveness of all technical and organizational measures for ensuring the security of Confidential Data at all times; and (D) shall also include the following:

(i) Implementation of controls to manage access to Confidential Data, including:

(a) Preventing access to Confidential Data other than by those Provider Personnel that must access Confidential Data to perform Participating Provider's obligations under the Terms and Conditions (hereinafter, the "Services");

(b) Immediately terminating access privileges to Confidential Data for any Provider Personnel that no longer need such access, and conducting regular reviews of access lists in accordance with high industry standards to ensure that access privileges have been appropriately provisioned and terminated;

(c) Requiring Provider Personnel the use of multi-factor authentication to access Confidential Data; and

(d) Providing regular training on data security to all Provider Personnel that may have access to Confidential Data;

(ii) Maintenance of firewalls to segregate Participating Provider's internal networks from the Internet, implementation of reasonable and appropriate network segmentation, and employing appropriate intrusion detection, prevention, monitoring, and logging capabilities to enable detecting and responding to potential security breach attempts as well as data loss resulting from malicious acts;

(iii) Conducting regular vulnerability assessments encompassing every system or network in which Confidential Data is collected, stored, transited, or otherwise processed, or from which it may be accessed;

(iv) To the extent that Participating Provider develops or uses applications in connection with Services, Participating Provider undertakes solely in its own independent capacity to perform security testing in accordance with industry standards for secure software development, including, in the case of web-based applications, to ensure that the application or application code is secure against the vulnerabilities described in (i) the version of the OWASP Top Ten List available as of the Effective Date of the Terms and Conditions and (ii) any changes to the OWASP Top Ten List after the Effective Date of the Terms and Conditions (within a reasonable time after such changes are initially published). The term "OWASP Top Ten List" shall mean the Open Web Application Security Project's Top Ten list (currently available at https://www.owasp.org/www-project-top-ten/);

(v) Application of all manufacturer-recommended security updates to, and the use of manufacturer-supported versions (and, for the avoidance of doubt, no software that is past its "end of life") of all software on, all systems, devices, or applications collecting, storing, processing, or transiting Confidential Data in a timely manner. In the case of security patches or updates that are classified by their manufacturer or otherwise as "critical," or are associated with a vulnerability with a CVSS score of 9.0 or higher in the National Institute of Standards and Technology's National Vulnerability Database, such patches or updates shall be applied as soon as practical, but no later than thirty (30) days after release for systems that are not exposed to the public Internet, or seventy-two (72) hours for systems that are exposed to the public Internet. Provider shall apply

those security patches or updates that are associated with a CVSS score of 7.0 or higher, or that are classified as "high" risk, promptly and no later than ninety (90) days from date of release;

(vi) Maintenance and enforcement of policies and procedures to ensure that all of the following requirements are met:

(a) up-to-date virus protection software shall be installed on all computer systems attached to Participating Provider's networks and/or the networks of any subcontractor Provider Personnel;

(b) access to Participating Provider's computer resources and networks (including wireless networking and remote access) and those of any subcontractor Provider Personnel shall be limited to configurations approved by the Participating Provider utilizing appropriate authentication and authorization methods, including reasonable minimum password requirements, of sufficient length and complexity in accordance with industry standards, which shall be automatically enforced by the operating system used by Participating Provider;

(c) the operating system shall enable a dictionary check to reject commonly used passwords, or Participating Provider shall regularly conduct password audits using tools designed to identify guessable or crackable passwords, and shall lock out the user account after failed authentication attempts, in accordance with industry standards;

(d) Participating Provider shall prevent the use of shared credentials (any credentials that are shared between multiple users) to access Confidential Data except for a limited set of system admin account credentials (the "SysAdmin Accounts") that are regularly changed in accordance with high industry standards and any use of the SysAdmin Accounts to access Confidential Data shall be irrevocably logged with the ability to identify Provider Personnel using any such SysAdmin Account;

(e) Participating Provider shall remain current with industry standards pertaining to digital identity guidelines implementing new measures, as appropriate, from time to time, such as the National Institute of Standards and Technology (NIST) Digital Identity Guidelines (SP 800-63-3), or the successor thereto;

(f) Confidential Data, other than traditional contact information of Apple personnel that is shared with Participating Provider for day-to-day business operations such as name, email address, phone number, and other similar contact information, shall at all times be encrypted in accordance with the Encryption Standards described below, regardless of whether such Confidential Data is at rest or in transit;

(g) all encryption shall be accomplished with strong, modern cryptographic algorithms and ciphers employing robust integrity protection mechanisms and in accordance with industry standards for secure key and protocol negotiation and key management (collectively, the "Encryption Standards");

(h) without limitation to the terms of this Section 2, Participating Provider shall manage in a secure manner in accordance with high industry standards any mobile devices that are used to collect, transmit, store, or otherwise process Confidential Data, including by ensuring that: (i) Confidential Data stored on any such devices can be remotely wiped by Participating Provider; (ii) Confidential Data stored on any such devices is encrypted in accordance with the terms of subsection (g); (iii) the location of each such device can be remotely determined by Participating Provider; and (iv) Participating Provider maintains an up-to-date inventory of all such devices (devices meeting such requirements "Secure Mobile Devices").

(i) Confidential Data shall only be stored on any portable storage device or media, not Secure Mobile Devices, including but not limited to flash drives or other removable media (collectively, "Portable Storage Devices"), solely if authorized by Apple as necessary for the purposes of performing Participating Provider's obligations under the Terms and Conditions, and shall be encrypted at all times in accordance with the terms

of subsection (g) with a record of all such Portable Storage Devices including, to the extent possible, a detailed summary of the Confidential Data on any such Portable Storage Device maintained in an up-to-date inventory subject to regular review in accordance with ISO/IEC 27001:2013 or any successors thereto;

(j) to the extent that Participating Provider provides hosted applications or services to Apple, whether single-tenant or multi-tenant, including software-as-a-service, platform-as-a-service, infrastructure-as-a-service, and similar offerings, (collectively, "Cloud-based Services") to collect, transmit, store, or otherwise process Confidential Data, Participating Provider shall provide Apple the ability: (i) to isolate such Confidential Data logically from the data of Participating Provider's other customers; (ii) to restrict, log, and monitor access to such Confidential Data at any time including access by Provider Personnel; (iii) to create, enable, disable, and delete the uppermost encryption key (the "Customer Managed Key") used to encrypt and decrypt subsequent keys including the lowermost data encryption key; and (iv) to restrict, log, and monitor access to the Customer Managed Key at any time; and at no time shall any subsequent encryption key, an encryption key in a key hierarchy lower than the Customer Managed Key, be stored in the same system as Confidential Data unless encrypted by the Customer Managed Key, also known as being wrapped by the Customer Managed Key;

(k) all documents and electronic media containing Confidential Data shall at all times be protected in accordance with Participating Provider's obligations of confidentiality of the Terms and Conditions, and if disposal is permitted by the Terms and Conditions, shall be disposed of in a secure and final manner in accordance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization (SP 800-88 rev. 1) or ISO/IEC 27040:2015 Information technology — Security techniques — Storage security, or any successors thereto ("Deletion Requirements");

(l) without limitation to Participating Provider's obligation to transmit Confidential Data only in encrypted form, Participating Provider shall ensure that any identities used for electronic communication (e.g. email addresses) are wholly owned by Participating Provider. Participating Provider shall ensure that any domains that it uses to identify itself are adequately protected to prevent impersonation. Provider Personnel shall not use personal email addresses or public email services (e.g. Gmail, Yahoo, Hotmail) to transmit Confidential Data or to communicate with Apple; and

(m) if reasonably requested by Apple at any time during Participating Provider's participation in the Program, Participating Provider shall provide Apple with a copy of the then-current Information Security Management System policies and procedures maintained by Participating Provider.

1. Information Security Breach.

Participating Provider shall promptly (or in any case within 48 hours) notify Apple if Participating Provider knows or has reason to believe there has been any misuse, compromise, loss, or unauthorized disclosure or acquisition of, or access to, Confidential Data (an "Information Security Breach"). Upon any discovery of an Information Security Breach, Participating Provider will investigate, remediate, and mitigate the effects of the Information Security Breach. To the extent the Information Security Breach relates to Apple's Confidential Information, Participating Provider will reasonably cooperate with Apple in connection with each of the foregoing and will comply with any reasonable instructions provided by Apple in connection therewith. Without limitation to the foregoing sentence, in the event that Apple reasonably determines that a third-party security assessment is recommended in connection with an Information Security Breach, Participating Provider will engage a third-party security assessor to conduct such an assessment. Participating Provider shall provide any information related to any such Information Security Breach requested by Apple, including but not limited to, vulnerabilities or flaws, start or end date, date of discovery, and specific actions taken to contain and/or mitigate. If any Information Security Breach occurs as a result of an act or omission of Participating Provider or Participating Provider's Personnel, Participating Provider will, at Participating Provider's sole

expense, undertake remedial measures (including notice, credit monitoring services, fraud insurance and the establishment of a call center to respond to customer inquiries).

4. Assistance.

Participating Provider shall provide Apple with reasonable assistance and support where there is a question in relation to a matter that is the responsibility of Apple in its capacity as a separate party, in (i) responding to an investigation or cooperation request by a data protection regulator or similar authority; (ii) providing notice of an Information Security Breach to any third party where required or requested by Apple; (iii) conducting legally required privacy, security, or data protection impact assessments; and (iv) consulting with the relevant authorities when required in relation to such impact assessments.

5. Return or Destruction of Apple Confidential Information.

Upon termination of Participating Provider's participation in the Program for any reason, Participating Provider shall promptly contact Apple for instructions regarding the return, destruction, or other appropriate action with regard to Apple Confidential Information. Unless otherwise instructed by Apple upon termination Participating Provider's participation in the Program for any reason, or at any time at the request of Apple, Participating Provider: (i) return all Apple Confidential Information to Apple including but not limited to all paper and electronic files, materials, documentation, notes, plans, drawings, and all copies thereof, and ensure that all electronic copies of such Apple Confidential Information are deleted from Participating Provider (and where applicable, its subcontractors') systems; or (ii) if requested by Apple in writing, or remaining on Participating Provider systems following the return of Apple Confidential Information set forth above, promptly destroy all instances of Apple Confidential Information; and for the avoidance of doubt, Apple Confidential Information shall be destroyed in accordance with the Deletion Requirements including Apple Confidential Information on any media used for backup, disaster recovery, and/or business continuity purposes. If requested by Apple, Participating Provider shall provide Apple with written confirmation of its compliance with the requirements of this section.

6. Third Parties including Subcontractors and Provider Personnel.

Participating Provider may only disclose Confidential Data to third parties (including Provider Personnel) who have a need to know that Confidential Data in order to perform the Services and have signed agreements that require them to protect Confidential Data in the same manner as detailed herein. Participating Provider shall not engage any third party to perform any portion of the Services if such party may obtain or otherwise process Apple's Confidential Information, without Apple's prior written consent. Notwithstanding such consent, Participating Provider any shall not be relieved of any obligations under this Exhibit B and shall remain solely liable if any Provider Personnel or other third party fails to fulfil its obligations with respect to Confidential Data.

7. Notification of Non-Compliance.

Without limitation to Participating Provider's obligations under this Exhibit B, and without prejudice to any other rights or remedies available to Apple, if Participating Provider is unable to comply with its commitments stated in this Exhibit B, Participating Provider shall promptly notify Apple, and Apple may immediately terminate Participating Provider's participation in the Program.