SecurePCI® Services Additional Terms and Conditions

The following additional terms and conditions shall apply to all SecurePCI and Hardware Add-On Services ordered by Client from Viking Cloud (including its affiliates) and provided by Viking Cloud or any of Viking Cloud's affiliates. Capitalized terms used herein but not specifically defined shall have the same meanings ascribed to them in either the Master Agreement, Ordering Agreement (whether a Subscription Services Agreement, Participation Agreement, Order Form or other similar document), or the Additional Terms for Managed Security, Business Continuity, Compliance and Voice Add-On Services.

1.1 **Services description**.

1.1.1 Viking Cloud shall provide, on a subscription basis, the Services ordered by Client for its Sites, which:

1.1.1.1 include certain SecurePCI Services which may include, if ordered, Business Protection Services, Continuous Compliance Management, Continuous Compliance Management – Core, Advanced Scanning, PCI Tools, IT Security Blueprint Management and Device Care;

1.1.1.2 include, if ordered, Hardware Add-On Services, and;

1.1.1.3 include, if ordered, Viking Cloud Endpoint Services.

1.1.2 As the Services are managed services provided by Viking Cloud to many Clients, Viking Cloud, at its sole discretion may, from time to time, make changes to the Services, and any such changes may result in additional charges to Client, for which Client will be notified in advance.

1.1.3 Viking Cloud may provision the Services through its affiliates, agents, suppliers or subcontractors.

1.1.4 The Services may include services related to compliance with the Payment Card Industry Data Security Standard (PCI-DSS) ("PCI Compliance Services") and notwithstanding the provision of any PCI Compliance Services or any provisions to the contrary in this Agreement, Client is solely responsible for (a) its compliance with all applicable PCI requirements; (b) any fees or fines payable to the Payment Card Industry Security Standards Council ("PCI SSC") or card brands related to its operations or to the Services; and (c) notification of any suspected breach of its systems or unauthorized access to any personal information.

1.1.5 The fees and charges are based on the Services facilitating the management of compliance with the Payment Card Industry Data Security Standard (the "PCI DSS"), Version 4.0.1 December 2024. In the event of changes to the PCI DSS, VikingCloud may change the fees and charges upon written notice to Customer.

1.2 **Business Protection Services**. "Business Protection Services" collectively refers to the "HIPAA Data Breach Protection Services," the "PCI Data Breach Protection Services," and the "Personally Identifiable Information ("PII") Data Breach Protection Services". The Business Protection Services shall only apply to Data Security Events which are reported in writing to Viking Cloud, by a Merchant: (i) during the policy period of the insurance policy which backs Viking Cloud's provision of the Business Protection Services, and; (ii) no more than sixty (60) days after discovery of the Data Security Event by the Merchant. Final determination of all Business Protection Services claims, and amounts paid, if any, shall be made by the insurer underwriting the Business Protection Services insurance policy to Viking Cloud.

1.2.1 HIPAA Data Breach Protection Services.

1.2.1.1 The HIPAA Data Breach Protection Services (the "HIPAA-DBP-Services") include reimbursement of the following HIPAA Expenses subject to the maximum reimbursement amounts set forth in Section 1.2.1.4 below, in connection with a HIPAA Security Event:

1.2.1.1.1 HIPAA Civil Penalties;

1.2.1.1.2 HIPAA Legal Expenses; and,

1.2.1.1.3 HIPAA Notification Expenses.

1.2.1.2 The HIPAA-DBP-Services shall: (i) be in effect for all Sites for which it was ordered as of the date Client completes all of the Viking Cloud required installation and provisioning of the Services so that the Services are functioning as designed and intended by Viking Cloud, and; (ii) apply to claims for breaches of which Client receives written notice after the Portal Start Date, and; (iii) not apply to claims for breaches which (a) Client knew, or should have known, had occurred prior to the Portal

Start Date, or (b) are not reported in accordance with Section 1.2 above; provided, however, in the event that Client does not pay the applicable fees and charges when due, the HIPAA-DBP-Services shall be void as of the Portal Start Date, and shall not apply to any claims for breaches. Upon such failure to pay being remedied by Client (the "Pay Remedy Date"), the HIPAA-DBP-Services shall: (i) be in effect from and after the Pay Remedy Date; (ii) apply to claims for breaches of which a Client receives written notice after the Pay Remedy Date, and; (iii) not apply to claims for breaches which (a) Client knew, or should have known, had occurred prior to the Pay Remedy Date, and (b) are not reported in accordance with Section 1.2 above.

1.2.1.3 In order to file a HIPAA-DBP-Services claim, Client shall follow Viking Cloud's then current claim filing procedures.

1.2.1.4 The maximum reimbursement of HIPAA Expenses is limited to $100,000 per HIPAA Security Event, regardless of the number of Covered Entities affected, and is further limited to:

1.2.1.4.1 $25,000 of HIPAA Legal Expenses per HIPAA Security Event, which limit is included within, and not in addition to, the limit set forth in Section 1.2.1.4 above, and;

1.2.1.4.2 $25,000 of HIPAA Notification Expenses per HIPAA Security Event, which limit is included within, and not in addition to, the limit set forth in Section 1.2.1.4 above.

1.2.1.5 The Client shall cooperate with Viking Cloud and its respective contractors in: (i) enforcing any legal right to contest any HIPAA Civil Penalty and/or HIPAA Notification Expense, and; (ii) enforcing any right of contribution or indemnity against any party other than the Covered Entity who may be liable for the HIPAA Security Event.

1.2.1.6 The HIPAA-DPB-Services shall not apply to:

1.2.1.6.1 any HIPAA Security Event known prior to or discovered outside the coverage period of the HIPAA-DBP-Services;

1.2.1.6.2 a Business Associate, unless the Covered Entity has been made legally liable for such HIPAA Civil Penalty, HIPAA Legal Expense, or HIPAA Notification Expense, or;

1.2.1.6.3 any fraudulent, illegal, dishonest or criminal act committed by, at the direction of, or with the knowledge of any director, officer or owner of the Covered Entity.

1.2.2 PCI-PII Data Breach Protection Services.

1.2.2.1 The PCI Data Breach Protection Services (the "PCI-DBP-Services") and Personally Identifiable Information Data Breach Protection Services (the "PII-DBP-Services) (collectively the PCI-PII-DBP-Services); shall include reimbursement of the following combined PCI and PII Expenses ("PCI-PII Expenses") subject to the maximum reimbursement amounts set forth in Section 1.2.6 below:

1.2.2.1.1 Forensic Audit Expenses;

1.2.2.1.2 Card Replacement Expenses;

1.2.2.1.3 Card Association Assessments;

1.2.2.1.4 Post PCI Security Event Expenses;

1.2.2.1.5 Loss Mitigation Expenses, and;

1.2.2.1.6 Crisis Management and Fraud Prevention Expenses.

1.2.2.2 "Personally Identifiable Information ("PII") shall include:

1.2.2.2.1 social security number;

1.2.2.2.2 medical service or healthcare data;

1.2.2.2.3 driver's license or state identification number;

1.2.2.2.4 account, credit card, or debit card number, alone or in combination with any information that permits access to an individual's financial information, including, but not limited to, security or access code or password, and;

1.2.2.2.5 other-non-public information to the extent prescribed under Privacy Regulations. For the avoidance of doubt, PII does not include publicly available information that is lawfully in the public domain or information available to the general public from government records.

1.2.2.3 The PCI-PII-DBP-Services shall: (i) be in effect for all Sites for which it was ordered as of the date Client completes all of the Viking Cloud required installation and provisioning of the Services so that the Services are functioning as designed and intended by Viking Cloud, and; (ii) apply to claims for breaches of which Client receives written notice after the Portal Start Date, and; (iii) not apply to claims for breaches which (a) Client knew, or should have known, had occurred prior to the Portal Start Date, or (b) are not reported in accordance with Section 1.2 above; provided, however, in the event that Client does not pay the applicable fees and charges when due, the PCI-PII-DBP-Services shall be void as of the Portal Start Date, and shall not apply to any claims for breaches. Upon such failure to pay being remedied by Client (the "Pay Remedy Date"), the PCI-PII-DBP-Services shall: (i) be in effect from and after the Pay Remedy Date; (ii) apply to claims for breaches of which a Client receives written notice after the Pay Remedy Date, and; (iii) not apply to claims for breaches which (a) Client knew, or should have known, had occurred prior to the Pay Remedy Date, and (b) are not reported in accordance with Section 1.2 above.

1.2.3 Client is not required to be PCI DSS compliant to be eligible for the PCI-PII-DBP-Services; provided, however, if Client (or any Client Affiliate) has had a previous breach at any time, or incurs a breach while eligible, Client shall not be eligible (or re-eligible) for the PCI-PII-DBP-Services until Client's then current PCI DSS compliance is verified or re-verified, as applicable.

1.2.4 Only Level 2, 3, and 4 merchants (as such levels are defined by the PCI DSS) are eligible for the PCI-PII-DBP-Services. Ineligible merchants include those that process greater than six (6) million payment card transactions annually with a card brand or are deemed a Level 1 merchant by a card brand.

1.2.5 In order to file a PCI-PII-DBP-Services claim, Client shall follow Viking Cloud's then current claim filing procedures.

1.2.6 Maximum reimbursement of PCI-PII Expenses.

1.2.6.1 Per Merchant PCI-PII-DBP-Services. For a Client with only one (1) MID, the maximum reimbursement of PCI-PII Expenses is limited to: (i) $100,000 per Merchant annually; (ii) a per occurrence maximum of $100,000, and; (iii) an annual aggregate maximum of $100,000.

1.2.6.2 Per MID PCI-PII-DBP-Services. For a Client with multiple MIDs, the maximum reimbursement of PCI-PII Expenses is limited to: (i) $100,000 per MID per year, and; (ii) a per occurrence maximum reimbursement of $500,000, and an aggregate annual maximum reimbursement of $500,000.

1.2.7 The PCI-PII DPB-Services shall not apply to:

1.2.7.1 any Level 1 merchant as defined under the PCI DSS;

1.2.7.2 any Data Security Event that arises out of a Merchant allowing any party other than its employees to hold or access cardholder information, or;

1.2.7.3 any Data Security Event that arises outside of the direct care, control and custody of the Client or Client's Service Contractor.

1.2.8 Mitigation. Client agrees to take reasonable steps to prevent the occurrence of Data Security Events and to mitigate losses arising out of such events, including, without limitation, following the procedures required by Card Associations and the Regulator, as applicable, in the event of a Data Security Event. In the event of a Data Security Event, Client agrees not to take any potentially harmful action or fail to take any potentially remedial or mitigating action, assume any financial obligation, pay any money or incur any expense in connection with the Data Security Event that prejudices the rights of Viking Cloud under this Agreement without first obtaining Viking Cloud's prior written consent. If Client fails to meet any of the preceding mitigation duties or obligations, some portions or the entirety of Client's claim may not be covered by the Data Breach Protection Services.

1.3 **PCI Tools**. PCI Tools may include the following:

1.3.1 Viking Cloud Portal. Each of Client's Sites will be implemented in the basic version of the Viking Cloud Portal. Client agrees that if Client is a franchisee, data about franchisee's Client Sites related to compliance, network security, LTE usage, or WiFi connectivity and use that is contained in the Viking Cloud Portal may be shared with Client's franchisor.

1.3.2 Initial IT Security Blueprint. If ordered, Viking Cloud will develop a network and security blueprint for launching the initial compliance solution to be deployed at Client's Sites. The Initial IT Security Blueprint is a one-time effort and does not cover ongoing updates to the blueprint as may be required when Client makes changes to internal systems or processes (e.g. POS update, changes to POS security zone, new application deployment, etc.). All firewall rules, configurations and network blueprints are the property of Viking Cloud and will only be provided to a Client for an additional fee, with such fee to be determined at the time of request.

1.3.3 Basic Merchant SIEM. If ordered, PCI-required log management and 365-day log retention for one (1) firewall and one (1) software agent per Site.

1.3.3.1 Basic Merchant SIEM may include centralized log collection from merchant's firewall and Host systems, including security logs, and firewall security notifications.

1.3.3.2 Security and network logs and events are the property of Viking Cloud and will only be provided to a Client for an additional fee, with such fee to be determined at the time of request.

1.3.3.3 Additional agents, if needed, are purchased per Site.

1.3.3.4 In the event that Viking Cloud determines that a Client is producing excessive logs and/or notifications, Viking Cloud will work with the Client in an effort to reduce the number of logs and/or notifications produced. If this effort is unsuccessful, Viking Cloud may suspend log collection and/or notification services until such time as the issue is remedied.

1.3.4 ASV External Vulnerability Scanning. If ordered, Viking Cloud will provide a web-based tool for Client to initiate and scan one (1) IP address per Site. Client is responsible for all scanning and remediation activities. ASV Scanning is ONLY available for Level 4 Merchant Sites.

1.3.5 PCI eLearning Courses. If ordered, Client's Sites shall have access to PCI eLearning Courses via the Viking Cloud Portal. Each Site shall receive ten (10) unique Users to the Cashier's PCI Training and one (1) unique User to the Risk Owner Training. Additional Users per Site may be purchased.

1.3.6 PCI Portal. If ordered, Client's Sites shall have access to a PCI Portal, providing a Self-Assessment Questionnaire ("SAQ") wizard, Security Policy Templates, and Pre-Populated SAQ.

1.3.7 Configuration Management. If Viking Cloud is managing a firewall, Secure Cloud Gateway ("SCG"), Wireless Access Point ("WAP"), Switch or other device for Client (collectively referred to as "Devices"), standard PCI-required configuration management will be provided for up to one (1) firewall or SCG Device per Site that is at or below the level of an SCG 4500. If Client purchases the Financial Institutions Services Bundle, standard PCI-required configuration management will be provided for up to one (1) firewall or SCG Device per Site that is at or above the level of an SCG 8000. Other configuration management services are optional Add-On Services. In all cases, Client shall:

1.3.7.1 Provide Viking Cloud with the ability to create VPN Tunnels between Viking Cloud's data center and firewalls or SCG devices at Client's Sites;

1.3.7.2 Provide Viking Cloud with access to Client's firewall management system if Viking Cloud is to manage a Client-supplied firewall, and;

1.3.7.3 Enable ICMP on all hardware devices (firewall, WAPs, switches) such that Viking Cloud may transmit ping messages to devices.

1.3.7.4 Client agrees to configure, or allow Viking Cloud to configure, all devices and device management systems (e.g. FortiManager) such that Viking Cloud's designated SIEM will receive a copy of PCI-required logs and SNMP traps from Client's devices. Viking Cloud shall provide a list of all required logs and traps to Client.

1.3.7.5 Provide Viking Cloud with information about Client's firewall, including, but not limited to, make, model, serial number, MAC address, VLANs and IP addresses.

1.4 **Continuous Compliance Management**. Continuous Compliance Management" ("CCM") is limited for use only by Level 4 Merchant Sites. Client is solely responsible for its compliance with all applicable PCI requirements, any fees or fines payable to the Payment Card Industry Security Standards Council ("PCI SSC") or card brands related to its operations or to the

Services, and notification of any suspected breach of its systems or unauthorized access to any personal information. CCM includes the following:

1.4.1 Managed PCI eLearning. Bulk upload of Users and assignment of training and policy on a monthly basis. A Viking Cloud account manager will work with Client on User changes and assignment of training courses and policies.

1.4.2 Managed Security Policy. Provides templates for PCI Security Policy by SAQ type. Policy will be adjusted to the Client's environment and published on the applicable learning management system. A Viking Cloud account manager will work with Client to update the policy on a quarterly basis to incorporate changes to the Client's environment.

1.4.3 Managed PCI Self-Assessment Questionnaire. A Viking Cloud account manager will work with Client to: (i) determine the SAQ which is applicable to Client's Bank Card processing, and; (ii) provide annual guided SAQ completion assistance.

1.4.4 Managed Penetration Testing Guidance. Annual penetration testing guidance for Clients that have multiple corporate-owned Sites. A Viking Cloud account manager will work with Client to determine the types of Penetration testing required by Client. Penetration testing guidance does not include the performance of penetration tests by Viking Cloud. If penetration tests are desired by Client, Viking Cloud will provide a quotation for those additional services.

1.4.5 Advanced Threat Visibility. Viking Cloud will analyze Intrusion Detection System ("IDS") and Intrusion Protection System ("IPS") events for Client's Sites, categorize critical events, and provide Client visibility into critical events via the Viking Cloud Portal.

1.5 **Continuous Compliance Management – Core.** Continuous Compliance Management – Core ("CCM Core") is limited for use only by Level 4 Merchant Sites, and includes the following:

1.5.1 Managed PCI Self-Assessment Questionnaire. A Viking Cloud account manager will work with Client to: (i) determine the SAQ which is applicable to Client's Bank Card processing, and; (ii) provide annual guided SAQ completion assistance.

1.5.2 Managed ASV External Vulnerability Scanning and Remediation Assistance. A Viking Cloud account manager will work with Client on a quarterly basis to: (i) determine IP type (i.e. Static or Dynamic), and; (ii) review ASV scans and provide remediation guidance based on scanning results.

1.6 **Advanced Scanning**. Advanced Scanning requires that Continuous Compliance Management be purchased at each Site (which means Advanced Scanning is ONLY available for use by Level 4 Merchant Sites) and includes the following:

1.6.1 Managed ASV External Vulnerability Scanning and Remediation Assistance. A Viking Cloud account manager will work with Client on a quarterly basis to: (i) determine IP type (i.e. Static or Dynamic), and; (ii) review ASV scans and provide remediation guidance based on scanning results.

1.6.2 Internal Scanning. Viking Cloud will provide a web-based internal scanning tool for Client to scan internal hosts. Scanning may be conducted by Client on up to three (3) internal hosts. Client is responsible for all scanning and remediation activities.

1.7 **IT Security Blueprint Management**. If ordered, Viking Cloud will provide updates to the network and security blueprint when Client makes changes to internal systems or processes affecting the POS security zone. Updates will include updated network designs, rules, whitelists, and application configurations. All firewall rules, configurations and network blueprints are the property of Viking Cloud and will only be provided to a Client for an additional fee, with such fee to be determined at the time of request.

1.8 **Device Care**. If Client's ordered Services include Device Care, Viking Cloud will provide: (a) stocking of Viking Cloud Devices for replacement stock, (b) updates and management of device firmware or Viking Cloud Device licenses during any Term of an existing Subscription Services Agreement, and (c) replacement of failed devices or Viking Cloud Devices that are covered by the device's or Viking Cloud Device's manufacturer's warranty. When Device Care is provided for Client-owned devices, such as Bring Your Own Device, Viking Cloud's scope is limited to sending Client reminders stating when their device license(s) are set to expire, unless otherwise agreed to in the applicable Agreement. Client is responsible for purchase and renewal of all licenses unless an Agreement exists between Client and Viking Cloud for Viking Cloud to provide software licenses as part of Viking Cloud's Services. The following conditions apply to Device Care:

1.8.1 Device Care is only available for currently supported makes (e.g. Meraki) and models (e.g. MX65W) of devices or Viking Cloud Devices for which Viking Cloud is providing Configuration Management and for which Viking Cloud currently stocks the device. A list of devices that are currently supported and eligible for Device Care is included as Attachment 1 hereto. If a Client requests Device Care for a device not currently supported or stocked by Viking Cloud, Viking Cloud may make a comparable replacement with a Viking Cloud Device, but is not required to do so. Viking Cloud will not provide Device Care for any device for which Viking Cloud is not providing Configuration Management Services.

1.8.2 If a device or Viking Cloud Device replacement request is made by Client, and once received by Viking Cloud, the device or Viking Cloud Device is working properly and therefore is not covered under the manufacturer's warranty ("Non-Warranty Device Replacement"), a restocking fee of $100 shall be charged on the first occurrence, and a restocking fee of $800 shall be charged on each subsequent occurrence. Similarly, if a device or Viking Cloud Device replacement request is made by Client, and Client does not return the device or Viking Cloud Device requiring replacement to Viking Cloud within thirty (30) days of Viking Cloud shipping a replacement Viking Cloud Device to Client, Client shall pay the Fees for unreturned equipment as outlined herein.

1.8.3 Viking Cloud will provide no more than one (1) Non-Warranty Device Replacement per Site during a thirty-six (36) month Initial Term, and no more than two (2) Non-Warranty Device Replacements per Site during a sixty (60) month Initial Term.

1.8.4 Viking Cloud will provide next business day replacement for failed devices or Viking Cloud Devices covered under Device Care when the replacement is shipped to an address in the contiguous United States (not including Puerto Rico). Due to shipping and logistical limitations, the "next business day replacement" timeframe shall only apply in situations where Client contacts Viking Cloud for a replacement device by or before one (1) o'clock PM Eastern time on the preceding business day. If Client contacts Viking Cloud for a replacement device after one (1) o'clock PM Eastern time, then the replacement device will be delivered on the 2nd business day after such contact to Viking Cloud is made. All shipping fees are paid by Client. Next business day replacement is not guaranteed for addresses outside of the United States (including Puerto Rico).

1.9 **Hardware Add-On Services.** Hardware Add-On Services are available to Client's Sites that have purchased SecurePCI Services and may include the following:

1.9.1 Hardware Devices. Client may purchase, or rent Viking Cloud provided hardware Devices and licenses.

1.9.1.1 Purchase. If a Client purchases a hardware Viking Cloud Device, and its associated license from Viking Cloud, Client shall own the hardware and license. Client shall be responsible for procurement of any required licenses after the Initial Term of Client's Agreement.

1.9.1.2 Rental. If a Client rents a hardware Viking Cloud Device and its associated license from Viking Cloud, Viking Cloud shall retain ownership of the Viking Cloud Device and license, and Viking Cloud shall be responsible for providing any required licenses during the Initial Term and subsequent Renewal Term(s). Viking Cloud Configuration Management Services are required for each Viking Cloud Device that is rented.

1.9.2 Viking Cloud Configuration Management Services. Client may receive Viking Cloud Configuration Management Services for certain Viking Cloud Devices Client purchases from Viking Cloud. Management Services include:

1.9.2.1 Installation. Remotely assisted self-installation is standard. Clients may select on-site Professional Installation for an additional fee.

1.9.2.2 Change Control. Viking Cloud ensures that all change requests are authorized and documented.

1.9.2.3 Support. Viking Cloud provides a 24x7x365 manned service desk and accepts requests via email, chat, telephone, and the Viking Could Portal.

1.9.2.4 Monitoring/Management. Viking Cloud manages configurations, maintains logs, and performs fault isolation and restoration for failed purchased Viking Cloud Devices.

1.9.2.5 Patching and Updates. Viking Cloud manages patches and firmware updates for all devices.

1.9.2.6 Notifications. Notifications provide Users with information about Viking Cloud Devices including Viking Cloud Device availability information (when available) and/or PCI-required security events. Notifications are available in the Viking Cloud Portal for Client review. Notifications available to a Site depend on the Services to which the Site has subscribed.

1.9.2.7 Alerts. Alerts are messages sent to Users for critical notifications. Alert set-up and maintenance are managed by Clients in Viking Cloud Portal. The default method for alert delivery is email. Alternative delivery options may be available.

1.9.2.8 SCG Configuration Management Services. In addition to standard Viking Cloud Configuration Management Services, SCG Configuration Management Services also include management of a network security device or Viking Cloud Device (firewall) implemented in accordance with PCI DSS to protect the Client's Cardholder Data Environment (CDE). The SCG Management Services include, web filtering, whitelisting, anti-spoofing, network address translation, intrusion detection, rogue wireless detection, anti-malware, PCI-required log and configuration management. Optional Services may be available and purchased separately.

1.9.2.9 WAP Configuration Management Services. In addition to standard Viking Cloud Configuration Management Services, WAP Management Services include management of a WAP device or Viking Cloud Device implemented in accordance with PCI DSS and included log management, configuration management, availability monitoring, fault isolation and restoration, patching, and license management. Optional Services may be available and purchased separately.

1.9.2.10 Switch Configuration Management Services. In addition to standard Viking Cloud Configuration Management Services, Switch Management Services are utilized only with a managed switch, and log management, configuration management, availability monitoring, fault isolation and restoration, patching, and license management. Optional Services may be available and purchased separately.

1.9.3 Client Responsibilities. Client is responsible for certain activities and environmental conditions in order for Viking Cloud Management Services to be provided. These Client responsibilities include, but are not necessarily limited to:

1.9.3.1 Network Connectivity. A continuous connection to the public Internet for each device or Viking Cloud Device under Viking Cloud management. Viking Cloud is not responsible for Service disruptions associated with the Client's Internet connection.

1.9.3.2 Power. All devices or Viking Cloud Devices require an uninterrupted clean power source which is to be provisioned to each device or Viking Cloud Device by the Client. Viking Cloud is not responsible for service disruptions associated with power failure or an incorrect supply of power (such as a power spike).

1.9.3.3 Change Control. Viking Cloud Device Management Services are tailored to the Client computing environment; thus, Viking Cloud must be made aware of changes to the environment. Viking Cloud is not responsible for service disruptions associated with changes to the Client environment (such as an Internet Service Provider (ISP) change.)

1.9.3.4 Operating Environment. Devices and Viking Cloud Devices must be kept in proper operating environments. A proper operating environment includes, but is not necessarily limited to the following:

1.9.3.4.1 Area Preparation and Maintenance. Client should ensure the area in which the devices or Viking Cloud Devices are to be installed always remains clean, dry, and dust-free. Client should inspect the area for hazards such as bare wires and standing water and remove any such hazards. Client must not remove the device cover or Viking Cloud Device cover under any circumstances. Client staff should always remove scarves and neckties, jewelry, and other loose items before moving the hardware.

1.9.3.4.2 Ventilation. Devices or Viking Cloud Devices can generate substantial heat during operation and therefore require adequate ventilation. It is necessary to install devices or Viking Cloud Devices in air-conditioned rooms to ensure that internal cooling systems can maintain acceptable internal temperatures during operation.

1.9.3.4.3 Humidity and Temperature. The environment in which devices or Viking Cloud Devices operate must remain dry at all times. During operation, ambient relative humidity should never exceed eighty percent (80%) and ambient air temperature must remain between 40° F and 85° F (4° C and 29° C).

1.9.3.4.4 Electrical Grounding and UPS. The environment where a device or Viking Cloud Device is installed needs proper electrical grounding. Ensure that the device or Viking Cloud Device is always connected to the ground using a 3-pronged

grounding-type plug. While not required, Viking Cloud strongly recommends that the device or Viking Cloud Device use an uninterruptible power supply (UPS).

1.9.3.4.5 Network Cabling. Client is responsible for all cable runs that must go through any obstructed path (walls, ceilings, floors, etc.).

1.9.3.4.6 Disclaimer. Viking Cloud is not responsible for Services disruptions associated with an improper operating environment.

1.10 **Viking Cloud Endpoint Services**.

1.10.1 **Viking Cloud Endpoint Services**. Viking Cloud Endpoint Services are subscription modules Client can purchase to enhance Client's endpoint protection. Viking Cloud Endpoint Services are cloud-integrated, multi-layered security solutions embedded within a single lightweight software agent that is provisioned via the Viking Cloud Portal.

1.10.2 Configuration Benchmarking (Policy Scanning). Configuration Benchmarking (Policy Scanning) provides comprehensive assessments of endpoint configurations, comparing them against established PCI DSS benchmarks to identify potential vulnerabilities and areas for improvement.

1.10.3 File Integrity Monitoring (FIM) Reporting. File Integrity Monitoring (FIM) Reporting provides Client with weekly FIM reporting available via the Viking Cloud Portal.

1.10.4 Host Ping Command (CMD) allows a user to issue a simple ping from the endpoint to any IP address.

1.10.5 Network Inventory. Network Discovery Scanning scans inventory of all applications, devices and databases in real-time on the Client's network.

1.10.6 Next Generation Anti-Virus (NGAV). NGAV is a service that detects viruses and malicious content on a client's computer and quarantines the offending files to protect the endpoint.

1.10.7 Port Scanning provides visibility about the hosts identified on the network by identifying all open ports, what services are running on those ports, and version information if it can determine it.

1.10.8 Primary Account Number (PAN) Scanning. offers real world web detection/protection, by scanning for malware in HTTP and SMTP traffic types and utilizing URL reputation databases.

1.10.9 SecureEdge DNS Filtering offers real world web detection/protection, by scanning for malware in HTTP and SMTP traffic types and utilizing URL reputation databases.

1.10.10 Software Inventory provides a comprehensive list of software and versions to allow administrators the ability to monitor newly installed software and be an input for the vulnerability detection capability.

1.10.11 Threat Hunting. Threat Hunting is a Service that performs signature and non-signature based detection through heuristic analysis and machine learning.

1.10.12 Vulnerability Detection will hunt to determine if there is any known vulnerable software on the machine by looking at what software is installed as well as looking for known vulnerable or malicious files.

1.10.13 Windows Event Logging (WEL). Event log collection gathers security and firewall logs from a Windows endpoint and sends them to the VikingCloud portal for analysis, correlation and alerting.

1.11 **Onsite Professional Installation**.

1.11.1 Summary. If Client has ordered Onsite Professional Installation, then at Client's request Viking Cloud will provide technicians in the United States *(not including Puerto Rico, and subject to availability and geographic restrictions)* for onsite installation of the applicable Services.

1.11.2 Device Installation procedures.

1.11.2.1 The Viking Cloud Device will be configured and shipped direct to the Site from Viking Cloud or its affiliate(s).

1.11.2.2 The Viking Cloud technician will be scheduled to visit the Site to complete the installation.

1.11.2.3 The fee includes a single dispatch of the Viking Cloud technician. Each additional dispatch will include a minimum of one (1) additional hour of working time per each additional dispatch at Viking Cloud's then current hourly rate.

1.11.2.4 The Viking Cloud technician will not perform any facility modifications or other construction activities (e.g. no drilling into, or mounting of equipment on walls, etc.).

1.11.2.5 Upon completion, the Viking Cloud technician will have a Client or Client Affiliate representative sign an acceptance document confirming the successful installation.

1.11.3 Device Installation Requirements and Conditions.

1.11.3.1 Client is responsible for providing the Viking Cloud Technician with all licenses related to, and all passwords for, Client's computers, routers, networks, etc. needed to perform the installation.

1.11.3.2 Viking Cloud is not providing any software or software licenses for Client's computers, routers, networks, etc. Viking Cloud will not install any unlicensed software whether provided by Client or any other party.

1.11.3.3 Client, Client Affiliate or User delays will be a billable event, including delays due to: (i) any outage of Client's network; (ii) any power outage at the Site; (iii) any outage due to an improper operating environment at the Site, i.e. temperature, moisture, dust or dirt; etc.

1.11.3.4 The requirement for ladders over eight (8) feet must be noted in the service request prior to dispatch.

1.11.3.5 The building and work area must be free of hazardous materials.

1.11.3.6 Regular business hours are 7:00 am to 6:00 pm Monday through Friday in the time zone local to the installation Site.

1.11.3.7 There is a 1.5x hourly rate charge for any work completed outside of regular business hours.

1.11.3.8 Holidays include: New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day and Christmas Day. Service requests on Holidays are billed at 2x the regular hourly rate.

2. **Scheduled Maintenance**. From time to time the Services will be disrupted by scheduled maintenance. Viking Cloud will attempt to ensure that the Client is aware of scheduled maintenance and that the maintenance is performed during off hours.

3. **Viking Cloud Software.** Some of the Services will involve Client's use of Viking Cloud Software on a subscription basis and in object code form only. Use is strictly limited to Client's internal use of the Viking Cloud Software. Client may not, under any circumstances, copy the Viking Cloud Software in whole or in part, except as expressly authorized in writing by Viking Cloud.

4. **Viking Cloud Devices.** Some of the Services may involve Client's use of Viking Cloud Devices. All Viking Cloud Devices provided by Viking Cloud to Client in connection with the Services, shall at all times be and remain the sole property of Viking Cloud or its licensors unless Client has Purchased a Device and completed all payments. For the avoidance of doubt, any device that is included with a Service as part of the overall fees and charges of that Service is considered to be a Viking Cloud Device unless the device is specifically designated on an invoice from Viking Cloud or a contract between Client and Viking Cloud that explicitly states and shows that Client purchased the device rather than rented it. Absent any such invoice or contract, each such device shall be considered a Viking Cloud Device and shall be treated as such for purposes of any Agreement and/or these or any other applicable Terms and Conditions. Client shall bear all risk of loss of, or damage to, all Viking Cloud Devices provided to Client (ordinary wear and tear excepted) from the time of delivery to Client until return delivery to Viking Cloud or Viking Cloud's designee.

5. **Restrictions.** Some of the Services will run on Viking Cloud's server at Viking Cloud's secure hosting facility and be accessed by Client through a secure tunnel based upon one or more passwords provided to Client by Viking Cloud. Client may not copy any of the Services, in whole or in part. Client shall not itself, nor permit any other party to: (a) develop methods to enable any third party to use the Services, in whole or in part; (b) incorporate all or any portion of the Services into any other service or product or create any derivative work of the Services; (c) use the Services for timesharing, service bureau,

subscription service, or rental use, or; (d) publish or otherwise disseminate any results of any tests or operating results of the Services.

6. **Support.**

6.1 **Initial login**. For each User that will receive the Services, Client shall guide its and its Client Affiliates' Users through the initial login. After the completion of the initial login, Viking Cloud support will apply, as needed.

6.2 **Viking Cloud support**. Viking Cloud support includes:

6.2.1 Guiding Users through the Portal's base functionality.

6.2.2 Guiding Users through routine issues concerning the Services.

6.2.3 The information for contacting the Viking Cloud's Service Desk team is posted on Viking Cloud's or its affiliate's web site.

7 **Fees and charges; billing; payment; taxes.**

7.1 **Fees and charges**. Client shall pay to Viking Cloud the applicable fees and charges for the Services ordered.

7.2 **Billing**. All recurring charges ("RC") shall be invoiced in advance of the start of the billing term frequency indicated in the Ordering Agreement (annually, quarterly, or monthly) beginning on the "Billing Date" which shall be: (i) for Sites that receive Services that include an SCG, WAP or Switch Device, the earlier of (a) the date of installation of any of the SCG, WAP or Switch Devices, or (b) thirty (30) days after the date Viking Cloud has shipped any of the SCG, WAP or Switch Devices to the Site; (ii) for Sites that receive Services that do not include an SCG, WAP or Switch device, five (5) days after written Agreement of the Parties to add such Sites, and; (iii) for Sites where an ownership change of the Sites is being documented by the signing of a new Subscription Services Agreement with Viking Cloud, the Effective Date of that new Subscription Services Agreement. For the avoidance of doubt, all recurring charges shall be billed recurringly at the frequency indicated in the Ordering Agreement (annually, quarterly, or monthly) from the Billing Date until the Site Term is terminated in accordance with the terms herein.

7.2.1 All non-recurring charges ("NRC"), and other one-time fees and charges shall be invoiced as incurred unless otherwise explicitly stated on the Ordering Agreement.

7.2.2 Viking Cloud may change the fees and charges to existing products and services at least one (1) time per calendar year. In the case where a Viking Cloud supplier discontinues a solution previously available to Viking Cloud resulting in a price increase for a replacement solution, or the supplier unexpectedly increases its pricing for Viking Cloud to procure its solution, Viking Cloud may immediately pass along such price increase to Client.

7.3 **Site Term**. The initial term for a Site (the "Site Initial Term") commences on the Billing Date for such Site and continues thereafter for the period of time set forth in the Agreement. After the Site Initial Term, the Site Term shall automatically renew for successive twelve (12) month renewal terms (the "Site Renewal Term(s)") on each anniversary of the applicable Billing Date. The Site Initial Term and Site Renewal Terms are collectively called the "Site Term". The Parties may agree to subsequent Renewal Terms for the Agreement where additional Fees and Charges will apply.

7.3.1 **Site Term Extension**. If, during a Site Term, Client elects to add on any additional Viking Cloud Products or Services (the "Add-On Services") to the Products and Services from Client's initial order (the "Existing Services"), and the Site Term for the Add-On Services extends beyond the end date of the Site Term of the Existing Services, then the Site Term for the Existing Services shall be extended to become co-terminus with the Site Term of the Add-On Services, creating one co-terminus Site Term for all Products and Services for the Site. By way of illustration and not limitation, if Client 's initial order was for a SecurePCI Services bundle for a Site Initial Term of thirty-six months on 1/1/2020, and during month twelve of that Site Initial Term (12/1/2020) Client elects to add on High Availability Services for a Site Initial Term of thirty-six months, then the Site Initial Term for the SecurePCI Services bundle would be extended to match the end date of the Site Initial Term of the High Availability Services (11/30/2023). For the avoidance of doubt, if the Site Term for the Add-On Services does not extend beyond the end date of the Site Term for the Existing Services, then Site Term for the Existing Services shall remain unchanged and shall not be adjusted to be co-terminus with the Site Term of the Add-On Services.

7.4 **Termination of a Site**. Either Party may terminate the Site Term for a given Site effective at the end of the applicable Site Initial Term or Site Renewal Term, by providing the other Party at least one hundred twenty (120) days' prior written notice. After termination for a given Site, the applicable Agreement shall remain in effect for the remaining Sites.

7.5 **Termination of Agreement**. An Agreement shall terminate upon the termination of all Site Terms and/or Agreements.

7.6 **Effects of Termination**.

7.6.1 Site. Upon termination of the Site Term for a Site: (i) Viking Cloud shall cease to provide the Services to the Site; (ii) Client shall immediately pay all fees and charges owed hereunder applicable to the Site, and; (iii) Within seven (7) business days Client shall return to Viking Cloud all Viking Cloud Devices (in good working order, ordinary wear and tear excepted) and all Viking Cloud Software applicable to the Site at Client's expense.

7.6.2 Agreement. Upon termination of an Agreement: (i) Viking Cloud shall cease to provide all Services; (ii) Client shall immediately pay all fees and charges owed hereunder, and; (iii) Within thirty (30) days (the "Device Return Deadline") Client shall return to Viking Cloud all Viking Cloud Devices (in good working order, ordinary wear and tear excepted) and all Viking Cloud Software.

7.6.3 Fees for Unreturned Viking Cloud Devices or Viking Cloud Devices Returned After the Device Return Deadline. Pursuant to the applicable Agreement, if Client is obligated to return Viking Cloud Devices but does not comply, Client returns the Viking Cloud Devices in any condition other than in good working order, (ordinary wear and tear excepted), or Client returns the Viking Cloud Devices after the Device Return Deadline, then Client shall be required to pay to Viking Cloud a Non-Return Fee in the amount of $1,500 per SCG Device, $1,000 per Wireless Access Point (WAP) Device, $2,500 per Managed Switch Device, and $650 per LTE Device. For the avoidance of doubt, once Client has paid the Non-Return Fee, Viking Cloud shall have no obligation to refund it, even if Client subsequently returns the Viking Cloud Devices to Viking Cloud.

8 **Franchisee Data.** When a Client's Site is operated as a franchisee location of a franchisor with which Viking Cloud has a business relationship, Viking Cloud may disclose to such franchisor certain data about franchisee Client Sites related to compliance, network security, or WiFi connectivity and use.

9 **Definitions.** The following terms shall have the meanings set forth below, unless the context requires otherwise:

9.1 *"Bank Card"* means a financial transaction card, including a debit card, credit card or prepaid card, issued by a Card Association or a financial institution as a member of a Card Association.

9.2 *"Business Associate"* means a contractor, subcontractor, and other contracted entity, not otherwise excluded, that are not an employee of a Covered Entity but that requires access to Protected Health Information as part of providing services to the Covered Entity. Business Associate does not include: life insurance companies; health insurance companies; employers liability or workers compensation insurers; hospitals; health plans (including HMO, company health plan, and certain governmental programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs; schools or educational institutions; state agencies; law enforcement agencies; or municipalities and municipal offices.

9.3 *"Card Association"* means each of the following entities formed to administer and promote cards: MasterCard International, Inc.; VISA U.S.A., Inc.; VISA International, Inc.; Discover Financial Services; American Express; JCB International Credit Card Company, Ltd., and any similar credit or debit card association that is a participating organization of the PCI Security Standards Council.

9.4 *"Card Association Assessment"* means: (i) a monetary assessment, fee, fine or penalty levied against a Merchant by a Card Association as the result of a PCI Security Event, or a security assessment conducted as a result of a PCI Security Event, and; (ii) shall not exceed the maximum monetary assessment, fee fine or penalty permitted upon the occurrence of a PCI Security Event by the applicable rules or Agreement for such Card Association.

9.5 *"Card Replacement Expenses"* means the costs that the Merchant is required to pay by the Card Association to replace compromised Bank Cards as the result of a PCI Security Event, or a security assessment conducted as a result of a PCI Security Event.

9.6 *"Covered Entity"* means any of the following entities, not otherwise excluded, which is subject to the requirements of HIPAA and has ordered HIPAA DBP-Services under this Agreement: Host Health Care Providers meaning doctors, clinics, psychologists, chiropractors, allied health providers, nursing homes, pharmacies, and dentists. Covered Entity does not include: life insurance companies; health insurance companies; employers liability or workers compensation insurers; hospitals; health plans (including HMO, company health plan, and certain governmental programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs; schools or educational institutions; state agencies; law enforcement agencies; or municipalities and municipal offices.

9.7 *"Client"* is the Party named on the first page of this Agreement which is a Covered Entity and/or a Merchant.

9.8 *"Client Affiliate"* means any entity that is a Covered Entity and/or a Merchant, and which directly, or indirectly through one or more intermediaries, controls or is controlled by, or is under common control with Client.

9.9 *"Data Security Event"* collectively means any HIPAA Security Event, PCI Security Event, PII Security Event, Ransomware Security Event, Telecommunications Theft Event, or Social Engineering Fraud Security Event. Continuous or repeated actions or exposure to substantially the same general harmful condition, injury or damage shall be deemed a single Data Security Event. All HIPAA Expenses, PCI Expenses, PII Expenses, Ransomware Expenses, Telecommunications Theft Loss and Social Engineering Fraud Expenses resulting from the same, continuous, related or repeated event or which arise from the same, related or common nexus of facts, will be deemed to arise out of the first such Data Security Event.

9.10 *"E-Theft"* means the transfer of the Client's or insured entity's money, securities, or other property of value to a person, place, or account beyond the Client's or insured entity's control as a direct result of a Data Security Event. E-Theft loss means theft of money, securities, or other property of value transferred by the Client or insured entity as a result of an E-Theft event.

9.11 *"Forensic and Legal Expenses"* means the reasonable cost of the following services incurred by or on behalf of the Client or insured entity in excess of the Client or insured entity's normal operating costs and with prior written approval of the insurer: (i) a system investigation, (ii) services performed by a licensed legal professional retained by the Client or insured entity for the purposes of determining and advising the Client or insured entity on the applicability of any notice requirements under any Privacy Regulation, or; determining and developing the form of notification to comply with applicable notice requirements under any Privacy Regulation.

9.12 *"Forensic Audit Expenses"* means the costs of a security assessment conducted by a Qualified Security Assessor approved by a Card Association or the PCI Security Standards Council to determine the cause and extent of a PCI Security Event. For the Forensic Audit Expenses to be reimbursed, the Client must be notified in writing by Client's Card Association or Acquiring Bank, that the Forensic Audit is mandatory.

9.13 *"HIPAA"* means the Health Insurance Portability and Accountability Act of 1966, Public Law 103-191, as amended, and the rules and regulations promulgated thereunder.

9.14 *"HIPAA Civil Penalty"* means regulatory fines and penalties assessed by the Regulator against the Covered Entity as the result of HIPAA Security Event, and does not include: criminal penalties; economic damage to any party; legal and other expenses; punitive or exemplary damages; the cost to restore consumer identities or monitor or verify the creditworthiness, credit accuracy or damage to credit of any consumer; or the cost of hardware or software upgrades.

9.15 *"HIPAA Expenses"* means the sum of all HIPAA Civil Penalties, HIPAA Legal Expenses, and HIPAA Notification Expenses incurred as the direct result of a given HIPAA Security Event.

9.16 *"HIPAA Legal Expenses"* means attorney fees and all other reasonable fees, costs and expenses directly associated with the investigation, defense, appeal or settlement of a HIPAA Security Event with the Regulator. HIPAA Legal Expenses shall not include expenses incurred in the defense, appeal or settlement of any civil or criminal action by or against an entity other than the Regulator; declaratory judgment expenses; or independent monitoring or Cumis Counsel expenses.

9.17 *"HIPAA Notification Expenses"* means all expenses associated with mandatory notification following a HIPAA Security Event as required under the HIPAA Breach Notification Rule.

9.18 *"HIPAA Security Event"* means the actual or suspected unauthorized access to or use of "Protected Health Information" (as defined under HIPAA), arising out of a Client's possession of or access to such Protected Health Information.

9.19 *"Merchant"* means a party that accepts Bank Cards in the course of its business.

9.20 *"Merchant Identification Number"* or *"MID"* is a unique number assigned to a Merchant account to identify it throughout the course of processing activities.

9.21 *"PCI Expenses"* means the sum of all Forensic Audit Expenses, Card Replacement Expenses, Card Association Assessments, and Post PCI Security Event Expenses, incurred as the direct result of a given PCI Security Event.

9.22 *"PCI Re-Certification Services"* means the services of a third party computer security expert to re-certify the Client's compliance with the PCI Security Standards Council's payment card industry data security standards after PCI Security Event, provided that: (i) such recertification is required under the terms of the Insured Entity's Merchant Services Agreement with a credit or debit card issuing company' and; (ii) such PCI Security Event comprises one of the events described in the definition thereof and directly results in the release, disclosure, theft, loss, alteration, corruption, destruction, deletion or damage to PII. PCI Re-Certification Services does not mean any services or activities performed to update, upgrade, enhance, or replace the Insured Entity's computer system, nor to identify or remove software program errors, computer viruses or vulnerabilities.

9.23 *"PCI Security Event"* means the actual or suspected unauthorized access to or use of cardholder information, arising out of a Merchant's possession of or access to such cardholder information which has been reported: (i) to a Card Association by such Merchant, or; (ii) to such Merchant by a Card Association.

9.24 *"Personally Identifiable Information" ("PII")* shall include:

9.24.1 social security number;

9.24.2 medical service or healthcare data;

9.24.3 driver's license or state identification number;

9.24.4 account, credit card, or debit card number, alone or in combination with any information that permits access to an individual's financial information, including, but not limited to, security or access code or password, and;

9.24.5 other-non-public information to the extent prescribed under Privacy Regulations.

9.24.6 However, PII does not mean publicly available information that is lawfully in the public domain or information available to the general public from government records.

9.25 *"Portal Start Date"* means the date on which Viking Cloud provides the credentials for the use of the Viking Cloud Portal at the applicable Site(s).

9.26 *"Privacy Regulations"* mean any of the following statutes and regulations associated with the care, custody, control or use of personally identifiable financial, medical or other sensitive personal information:

9.26.1 General Data Protection Regulation (Regulation (EU) 2016/679), and any amendments thereto (GDPR);

9.26.2 California Consumer Privacy Act of 2018 (California Civil Code § 1798.100 - 1798.199), and any amendments thereto (CCPA);

9.26.3 Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191);

9.26.4 Health Information Technology for Economic and Clinical Health Act of 2009, and its related regulations;

9.26.5 Gramm-Leach-Bliley Act of 1999;

9.26.6 California Database Breach Act (SB1386);

9.26.7 Minnesota Plastic Card Security Act; or

9.26.8 other state, federal and foreign identity theft and privacy protection statutes, rules and regulations similar to 1-5 above that require commercial entities that collect, process, or store personal information (as defined in such statutes, rules and regulations, as applicable) to post privacy policies, adopt specific privacy controls, or to notify natural persons and/or organizations in the event that such personal information has been comprised or potentially compromised.

9.27 *"Post PCI Security Event Expenses"* means reasonable fees and expenses incurred by the Merchant with prior written consent for any service: (i) specifically approved in writing, including without limitation, identity theft education and assistance and credit file monitoring, and; (ii) which approved service is provided (a) by or on behalf of the Merchant within one (1) year following the discovery of the PCI Security Event to a cardholder whose cardholder information is the subject of the PCI Security Event, and (b) for the primary purpose of mitigating the effect of the PCI Security Event.

9.28 *"Ransomware Security Event"* means the insertion of malware by a third party perpetrator on computer hardware, software or components thereof linked together through network of devices accessible through the internet or the Client's intranet or connected with data storage or other peripheral devices and operated by and owned by a Client that prevents or limits an Client's ability to access data thereon for the purpose of obtaining a ransom from the Insured to end or remove the attack.

9.29 *"Ransomware Expenses"* means those funds paid by the Client to the perpetrators of the Ransomware Security Event to end the attack. For payments to be covered, Client must obtain Viking Cloud's prior approval for any payments.

9.30 *"Regulator"* means the Department of Health and Human Services, Office of Civil Rights or any governmental body or official authorized by them that is responsible for regulating and enforcing HIPAA and the rules and regulations promulgated thereunder against Covered Entities.

9.31 *"Remote Access Destination Site"* means a single Client or Client Affiliate Site which has Remote Access software installed on up to three (3) Workstations, for the purpose of connecting Users using the Secure Remote Access Services to the Client Workstations at that location.

9.32 *"Secure Cloud Gateway"* or *"SCG"* means the security device which is installed at each Site for which a Premium Services Bundle is ordered, and which includes both Viking Cloud Devices and Viking Cloud Software.

9.33 *"Secure Remote Access Services"* means the Viking Cloud services that enable Users to connect to their corporate Workstations from outside their office.

9.34 *"Service Contractor"* means any organization to which the Client has given care, custody or control of, or access to, PII pursuant to a written contract or Agreement with the Client, but only while acting within the scope of its duties performed on behalf of the Client.

9.35 *"Services"* means the services ordered by Client and provided by Viking Cloud on a subscription basis pursuant to this Agreement or any other valid written Agreement duly executed by the Parties.

9.36 *"Site"* means a physical Client or Client Affiliate location that will receive the Services, with each Site identified by a unique MID.

9.37 *"Social Engineering Fraud Event"* means the transfer of the Client's Money or Securities to a person, place or account beyond the Client's control by an employee of the Client acting in good faith reliance upon a verbal, written or electronic instruction that purported to be a legitimate Transfer Instruction, but instead was, in fact, fraudulent.

9.38 *"Social Engineering Fraud Loss"* means loss of Money or Securities transferred by the Client in a Social Engineering Fraud Event.

9.39 "*Telecommunications*" means telephone, fax, or data transmission services provided to the Client by others for compensation.

9.40 "*Telecommunications Theft Event*" means a third party's intentional, unauthorized and fraudulent use of the Client's Telecommunications Services.

9.41 "*Telecommunications Theft Loss*" means telephone service charges and fees incurred by the Client because of a Telecommunications Theft Event, in excess of the Client's normal operating costs.

9.42 *"User"* means each individual Client or Client Affiliate employee, contractor, agent or representative who is authorized by Client and Viking Cloud to receive and use Services under this Agreement.

9.43 *"Viking Cloud Device"* means any device or equipment deployed to Client to enable Viking Cloud to provide the Services which is either: (i) owned by Viking Cloud, or; (ii) owned by Viking Cloud's agents, suppliers or subcontractors, and as between Viking Cloud and Client shall be deemed owned by Viking Cloud.

9.44 *"Viking Cloud Portal"* means the portal through which Client accesses various features of the Services.

9.45 *"Viking Cloud Software"* means the firmware, plug-ins and software provided by Viking Cloud (which may include third party software) that is included in or associated with the Services, along with all updates, upgrades, patches, and bug fixes thereto. The Viking Cloud Software may include features that prevent use of the related Services after the expiration or termination of the applicable Site Term, and/or upon improper use of the Viking Cloud Software.

Attachment 1

Viking Cloud Supported Devices eligible for Device Care:

- Meraki MX Series Firewalls up to MX68
- Meraki MR Series WAPs up to MR74
- Fortinet Firewalls up to FortiGate 60F
- Fortinet Wireless Access Points: FortiAP 221B, FortiAP 221E, FortiAP 224E
- Viking Cloud NGFW
- Non-Managed Switches