KAISER PERMANENTE

PAYMENT CARD INDUSTRY REQUIREMENTS
FOR VENDORS, CONTRACTORS AND SUPPLIERS

Supplier will maintain compliance with the applicable requirements of the then-current Payment Card Industry Data Security Standard ("PCI DSS") or Payment Application Data Security Standard ("PA-DSS") promulgated by the Payment Card Industry Security Standards Council and available at https://www.pcisecuritystandards.org/ in accordance with the terms of these Payment Card Industry Requirements for Vendors, Contractors and Suppliers ("PCI Requirements").

A. Definitions: Capitalized terms used but not defined in these PCI Requirements have the meaning set forth in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms available at the website noted above.

"*Agreement*" means the services agreement between Supplier and Kaiser to which these PCI Requirements are applicable.

"Handles" or "*Handling*" means to perform any operation or set of operations upon Cardholder Data, whether manually or by automatic means, including but not limited to processing, collection, recording, sorting or organization, structuring, accessing, storage, adaptation or alteration, retrieval, consultation, use, transfer, disclosure by transmission, dissemination or otherwise making available, erasure or destruction.

"*Kaiser*" means Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, Kaiser Permanente Insurance Company, and the subsidiaries, affiliates and successors of the foregoing.

"Managed Services" means Supplier's management and assumption of responsibility for providing services through systems, networks, processes, and or personnel ("Assets") controlled and or hosted by the Supplier, whether or not those Assets are in a Kaiser or Supplier facility.

"*Supplier*" means a vendor, contractor or supplier who is providing goods or services to Kaiser.

B. Applicability:
In the event Supplier Handles credit card, debit card, or other Cardholder Data (such as "Primary Account Numbers" and "Sensitive Authentication Data" as defined under PCI DSS), or to the extent Supplier's services impact any Cardholder Data environment, Supplier acknowledges and agrees to maintain compliance with the requirements referenced in Section C below.

C. Requirements:
A Supplier Handling Cardholder Data, or providing Managed Services that involves the Handling of Cardholder Data on behalf of or for Kaiser, agrees as follows:

1) Supplier will comply with all rules and regulations of Visa, Mastercard, American Express, Discover and any other payment card association or network (each a "Payment Card Association"), including PCI DSS and/or PA-DSS (as applicable) and any other Payment Card Association data security, disaster recovery, or similar programs or requirements ("Card Association Requirements"). Supplier is responsible for accurately determining the compliance validation level applicable to Supplier and maintaining compliance in accordance with the Card Association Requirements most current version.

2) Prior to Supplier Handling any credit, debit, or other Cardholder Data, and on each anniversary of the effective date of the Agreement, Supplier will submit to Kaiser a summary of its PCI DSS assessment results and any current or planned remediation efforts in the form of an Attestation

of Compliance in accordance with the PCI DSS requirements (which may include a Report on Compliance prepared by a Qualified Security Assessor ("QSA")). If applicable, Supplier shall maintain and provide proof of certification by the PCI Security Standards Council of any payment application provided to Kaiser or used by Supplier in its provision of the Services.

3) Supplier agrees to promptly: (a) provide to Kaiser any other data security reports as required by any Payment Card Association; (b) pay to such Payment Card Association any fines and penalties for any failure of Supplier to comply with any data security requirements; and (c) provide full cooperation and access to permit such Payment Card Association to conduct a security review of Supplier's policies and procedures.

A Supplier Handling Cardholder Data on behalf of Kaiser through Staff Augmentation Services must comply with Kaiser's PCI-DSS policies and procedures. For purposes of these PCI Requirements, "Staff Augmentation Services" means Supplier's provision of systems, networks, processes, and or personnel that will support or augment Kaiser processes.

Supplier is liable to Kaiser and to any third-party claiming damages through Kaiser for all fees, costs, penalties and fines should a confirmed Data Breach or incident occur involving Cardholder Data on the POS system, technology systems and/or broadband internet connectivity or Services provided by Supplier.

D. Data Breach and Notification:

Supplier shall notify Kaiser, per the terms of the Agreement or applicable governing law, after Supplier has knowledge that there is, or reasonably believes that there has been a Data Breach. For purposes of these PCI Requirements, "Data Breach" means any actual or suspected unauthorized access to, disclosure, theft, modification, use or destruction of Cardholder Data, including, without limitation, as a result of any intrusion into Supplier's computer systems or networks.

E. Non-Compliance and Remediation:

Supplier shall immediately notify Kaiser if it is not in compliance with any of the PCI-DSS or PA-DSS requirements or security assessment procedures that apply to the Services being provided. In such event, Supplier agrees to work with Kaiser in good faith to develop a mutually agreeable remediation plan. Supplier acknowledges that uncured non-compliance with the PCI-DSS or PA-DSS requirements or security assessment procedures that apply to the Services being provided shall constitute a material breach of the Agreement.