



COLGATE BRIGHT SMILES BRIGHT FUTURES® SCHOOL DISTRICT AGREEMENT

THIS AGREEMENT (“Agreement”) is made effective on **January 6, 2025** (the “Effective Date”) by and between **COLGATE-PALMOLIVE COMPANY**, having its principal place of business at 300 Park Avenue, New York, NY 10022 (“Colgate”), and **AZUSA UNIFIED SCHOOL DISTRICT**, having its principal location at **546 South Citrus Avenue, Azusa, CA. 91702** (“School”). Colgate and School are each referred to in this Agreement as a “Party” and collectively the “Parties.”

WHEREAS, Colgate established its Bright Smiles Bright Futures® (“BSBF”) program in 1991, and wishes to help improve health and wellbeing for children, families and communities served by BSBF.

WHEREAS, School desires to work with Colgate’s BSBF program on oral health and wellness initiatives for its students;

NOW, THEREFORE, in consideration of the mutual covenants contained herein, the Parties agree as follows:

1. BSBF Program. Colgate’s BSBF program (“Program”) will provide the following at School, on a mutually agreed day/time, in exchange for School’s provision of the activities/obligations set forth in Section 3:

a. School Program/Curriculum. BSBF will provide the following students: **TK, Kindergarten classes, K-5** with free, fun and engaging educational kits containing tools to teach children healthy practices for oral health care. The BSBF website, www.colgatebsbf.com, contains intra-sites for parents, teachers and kids. Many valuable educational tools can be easily downloaded from this website.

b. BSBF Mobile Van Program. BSBF will provide students with free dental screenings, education and treatment referral.

c. Community Awareness Programs. BSBF mobile vans and staff participate in community events with a focus on raising awareness on oral health care.

2. Colgate BSBF Activities. In connection with providing its Program to School, Colgate will do the following:

a. Provide forms required by Colgate for students to participate in program activities;

b. Offer van visits to School students participating in the Program, as determined by the Parties (depending on timing of onsite visits);

c. Provide students in the Program who obtain written consent of their parent or guardian the opportunity to receive free dental screenings and oral health education aboard the mobile van unit (screenings based on availability and number of students that obtain required consents);

d. Provide a treatment referral list to every School RN or contact after each visit;

e. Send a pre-visit packet to the School to help them prepare for the visit;



- f. Provide all screened students with an oral care kit (toothbrush, toothpaste and educational materials);
- g. Provide parents or guardians of screened students a screening report card of their child; and
- h. Provide School contact with a log of all students screened at the conclusion of the Colgate visit, such log will include the number of students screened and the number of students listed with respective classification I, II, III or IV (the classifications are described in Exhibit B attached hereto).

3. School's Responsibilities. In exchange for Colgate performing the Program-related activities set forth in Section 2, School will do the following:

- a. Distribute and gather all Colgate required forms, including the parent/guardian consent forms, provided by Colgate;
- b. Post flyers and other promotional material announcing the scheduled dental screenings or virtual visits;
- c. Provide students with a safe setting to receive dental screenings;
- d. Identify elementary schools, children's centers and/or Head Start programs to participate in BSBF activities;
- e. Provide a list of site contacts at the School;
- f. Provide a list of eligible students to receive dental screenings;
- g. Assist in assuring confirmation to screen at least 100 students at the School;
- h. Provide a mutually acceptable place to allow Colgate or its agents to park the Colgate BSBF mobile van unit to provide students with the dental screenings (van dimensions are 36 ft. L x 15 ft. H x 14 ft. W); and
- i. Assist in identifying staff and parents to help as liaisons/volunteers during the Colgate BSBF mobile van visit at the agreed upon site.

4. Term. This Agreement shall commence on the Effective Date and shall expire on **June 30, 2027** (the "Term").

5. Termination. Either Party may terminate this Agreement (a) for convenience upon 60 days prior written notice to the other Party, or (b) if the other Party commits a material breach or default under this Agreement and such breach or default remains uncured for thirty (30) days after receipt of written notice from the non-breaching Party.



6. Confidentiality. Unless otherwise required by law, the specific terms and conditions of this Agreement are to be considered to be confidential and proprietary and will not be disclosed by either Party to any third party without the prior written consent of the other Party hereto. In addition, any information provided by either Party to the other Party in connection with this Agreement that constitutes valuable and proprietary information of the disclosing Party shall be held in confidence by the receiving Party and not be disclosed to any third party or used for any purpose other than pursuant to this Agreement. Each Party agrees it shall only disclose such confidential information only to its employees, contractors and/or service providers requiring such information in the performance of this Agreement and who are bound by obligations of nondisclosure and limited use at least as stringent as those contained herein. The aforementioned confidentiality obligations shall not apply to any information (a) already available in the public domain; (b) already known to the receiving Party from sources other than the disclosing Party; (c) made known to the receiving Party by a third party having no contractual or legal obligation of nondisclosure to the disclosing Party; (d) independently developed by the receiving Party without the use, aid or application of the disclosing Party's confidential information; or (e) any disclosure required by law of a governmental agency or made pursuant to an order of a court of competent jurisdiction. In the event a Party is required to disclose the other Party's confidential information pursuant to clause (e) above, the Party will give prompt notice to the other Party who may contest such disclosure at its own expense.

7. Compliance with Laws and Colgate Policies.

a. Both Parties shall comply with applicable state and federal law in performing their respective obligations under this Agreement. Each Party shall obtain, provide and maintain all governmental, regulatory or local approvals, notices, permits, licenses or similar requirements that are necessary for the applicable Party to commence and perform its obligations under this Agreement.

b. School represents and warrants that it is in compliance with Colgate-Palmolive Company's Anti-Bribery Policy as of the Effective Date and shall remain in compliance throughout the term of this Agreement with such policy and any amendments to such policy in the form: (a) provided by Colgate to School throughout the term of this Agreement or (b) updated throughout the term of this Agreement at <https://www.colgatepalmolive.com/en-us/core-values/our-policies/anti-bribery-policy>.

c. School represents and warrants that it is in compliance with Colgate-Palmolive Company's Third Party Code of Conduct as of the Effective Date and shall remain in compliance throughout the term of this Agreement with Colgate-Palmolive Company's Third Party Code of Conduct and any subsequent amendments thereto in the form (a) provided by Colgate to School throughout the term of this Agreement or (b) updated throughout the term of this Agreement at <https://www.colgatepalmolive.com/en-us/corp/about/governance/third-party-code-of-conduct>, including the requirement of strict compliance with the letter and spirit of applicable environmental laws and regulations and the public policies they represent.

d. In the event personal data will be processed by School on behalf of Colgate or as a benefit to Colgate, School represents and warrants that it is in compliance with the Data Privacy and Security obligations set forth in the attached Exhibit A as of the execution date of this Agreement, and will remain in compliance throughout the remainder of the Term and thereafter as set forth in Exhibit A, and is in compliance with applicable data privacy and data security laws.

8. Indemnification.



a. Colgate and School each agree it shall indemnify, defend and hold harmless the other Party, its affiliates and their respective officers, directors, employees and agents, from and against any and all claims, demands, losses, damages, costs and expenses (including reasonable attorney's fees, costs and expenses incidental thereto), connected with or resulting from: (i) a breach by the Indemnifying Party of any agreements, covenants, representations or warranties made in this Agreement, (ii) the gross negligence, willful misconduct, fraud or bad faith of the Indemnifying Party or its officers, directors, employees, subcontractors or agents, or (iii) damage to property and injuries (including death) to any persons caused by the Indemnifying Party or its affiliates or any of their respective employees, subcontractors or agents in the performance of the Indemnifying Party's obligations hereunder.

b. A Party seeking indemnification under this Agreement (the "Indemnified Party") shall notify the other Party (the "Indemnifying Party") in writing promptly after receipt by the Indemnified Party of any claim that is brought that would entitle an Indemnified Party to indemnification hereunder; *provided* that any failure to give such prompt notice shall not relieve the Indemnifying Party of its indemnification obligation hereunder, except to the extent it is materially prejudiced thereby.

c. The Indemnifying Party shall have the sole right and discretion to settle, compromise or otherwise dispose of the claim; *provided* that: (i) the Indemnified Party, at its own expense, shall have the right to participate in, but not control, the defense of the claim and all negotiations for settlement, compromise or other disposal of the claim (a "Settlement") and (ii) without the prior written consent of the Indemnified Party (such consent not to be unreasonably withheld, conditioned, or delayed), the Indemnifying Party shall not enter into: (A) any non-monetary Settlement or any monetary Settlement that is not satisfied in full by the Indemnifying Party; (B) any Settlement that requires any Indemnified Party to admit fault; (C) any Settlement that does not contain an unconditional release of the Indemnified Parties or (D) any Settlement that likely to materially and adversely affect the business of the Indemnified Party, as reasonably determined by the Indemnified Party.

9. Insurance. School shall maintain at all times during the term of this Agreement, and at its sole expense, such policy or policies of insurance, including a general liability, worker's compensation or equivalent state plan and employers liability, as are necessary to cover all loss, destruction or damage for which School has assumed responsibility under the terms of this Agreement, and shall name Colgate as an additional insured with respect to the general liability policy. School shall cause its insurance policies to provide a waiver of subrogation in favor of Colgate. The policies shall be with at least a Standard & Poor's A+ rated company providing limits of appropriate amount. Such limits can be satisfied with a primary policy or a combination of a primary and excess / umbrella policies. School shall promptly furnish upon request certificates of insurance to Colgate evidencing that the insurance required by this paragraph is in full force and effect.

10. Notice. Any notices given pursuant to this Agreement shall be in writing and shall be deemed to have been duly given on the date of such delivery if personally delivered or on the date of receipt or refusal indicated on the delivery or return receipt if delivered by a reputable overnight courier or if mailed by registered or certified mail, postage prepaid (return receipt requested) respectively, as follows:



If to School: **Azusa Unified School District**
546 South Citrus Avenue
Azusa, CA. 91702
USA
Attention: **Jennifer Wiebe, Director of Community**
Schools / Educational Services Department Phone
No.: **626.858.4267**

If to Colgate Colgate-Palmolive Company
300 Park Avenue
New York, NY 10022
Attention: Robert Wilson
SVP, Professional Engagement & Public Health,
Enterprise Oral Care

With a copy to: Chief Legal Officer
(which copy will
not constitute
notice)

11. Miscellaneous.

a. No liability shall result to Colgate or School from any delay in performance or from nonperformance to the extent caused by acts of God, fire, flood, explosion, war, acts of terrorism, labor disputes involving the labor of a third party, action of governmental authority or any other unforeseeable circumstances of a similar nature beyond the reasonable control of the Party affected; provided that the delayed or nonperforming Party: (i) promptly notifies the other Party of the existence of such cause and its probable duration and (ii) continues to make all reasonable efforts to prevent, limit and remove the effects of any such cause.

b. This Agreement shall be governed by, and construed and enforced in accordance with the laws of the State of New York without regard to its provisions concerning conflicts or choice of law.

c. Colgate may perform its obligations under this Agreement through one or more subcontractors. Each Party is responsible for its use of subcontractors hereunder, including any wrongful act or omission of such subcontractor(s).

d. Nothing in this Agreement is intended to or shall be construed to constitute or establish any endorsement, joint venture, partnership or fiduciary relationship between the Parties and no Party shall have the right or authority to act for or on behalf of the other Party.

e. This Agreement and the exhibits attached hereto contain the entire understanding between Colgate and School. This Agreement supersedes all prior and contemporaneous agreements and communications and may not be modified or amended unless both Parties agree in writing.



f. Any provision of this Agreement which by its express terms or by its nature is intended to survive the expiration or termination of this Agreement shall survive any such expiration or termination of this Agreement.


g. All covenants, terms and provisions of this Agreement shall be binding upon and inure to the benefit of Colgate and School and their respective successors and, to the extent specifically permitted herein, assigns.

h. This Agreement may be executed in counterparts, which may be transmitted electronically, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

[Signature Page Follows]

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their respective duly authorized representatives as of the Effective Date.

COLGATE-PALMOLIVE COMPANY

DocuSigned by:

By: BE67C06D157E45C...

Name: Robert Wilson

Title: SVP, Professional Engagement & Public Health,
Enterprise Oral Care
11/5/2024

AZUSA UNIFIED SCHOOL DISTRICT

By: _____

Name: Norma Carvajal Camacho

Title: Assistant Superintendent, Educational Services

Date:

EXHIBIT A

DATA PRIVACY AND SECURITY

During the course of providing Services, Supplier may obtain, access or otherwise Process Personal Data. Supplier agrees to protect all Personal Data as detailed in this Exhibit. For purposes of this Agreement, “Supplier” as used herein means School as defined above, and “Company” means Colgate-Palmolive Company.

1) DEFINITIONS

- a) “**Applicable Privacy Laws**” means all applicable privacy, information security, data protection, and data breach notification laws and regulations.
- b) “**Cardholder Information**” means any information: (a) relating to a payment card_(including credit or debit cards), the account holder’s name, account number, service code, card validation code/value, PIN or PIN block, expiration dates and magnetic stripe data; or (b) relating to a payment card transaction that is identifiable with a specific account. Cardholder Information is also included in the definition of Sensitive Personal Data.
- c) “**Information Security Program**” means a comprehensive written information security program which complies with Applicable Privacy Laws, and contains appropriate administrative, technical, and physical safeguards to protect Personal Data against anticipated threats or hazards to its security, confidentiality or integrity (such as unauthorized access, collection, use, copying, modification, disposal or disclosure, unauthorized, unlawful, or accidental loss, destruction, acquisition, or damage or any other unauthorized form of Processing).
- d) “**Personal Data**” means any information in any form, format or media (including paper, electronic and other records), that identifies an individual or relates to an identifiable individual that (i) is provided by or on behalf of Company (or its employees, contractors or agents), (ii) Supplier provided to or obtained for Company or (iii) Supplier Processes, in each case, in connection with the Services.
- e) “**Process**” or “**Processing**” or “**Processed**” means the collection, recording, organization, structuring, alteration, use, access, disclosure, copying, transfer, storage, deletion, combination, restriction, adaptation, retrieval, consultation, destruction, disposal or other use of Personal Data. The applicable SOW describes the scope of the Supplier’s Processing.
- f) “**Security Incident**” means any accidental or unauthorized access, acquisition, use, modification, disclosure, loss, destruction of or damage to Personal Data, or any other unauthorized Processing of Personal Data.
- g) “**Sensitive Personal Data**” means any of the following types of Personal Data: (i) social security number, taxpayer identification number, passport number, driver’s license number or other government-issued identification number; (ii) payment card (including credit or debit card) details

or financial account number, with or without any code or password that would permit access to the account or credit history; or (iii) information on race, religion, ethnicity, sex life or practices or sexual orientation, medical or health information, genetic or biometric information, biometric templates, political or philosophical beliefs, political party or trade union membership, background check information or judicial data such as criminal records or information on other judicial or administrative proceedings.

2) DATA PROCESSING AND PROTECTION

- a) **Compliance with Applicable Privacy Laws.** Supplier will comply with Applicable Privacy Laws relating to Supplier's performance under this Agreement and each applicable SOW.
- b) **Limitations on Use.** Supplier will Process Personal Data only on Company's behalf to deliver Services in accordance with this Agreement or Company's other documented instructions, whether in written or electronic form, such as an applicable SOW. The duration of the Processing will be the same as the duration of this Agreement or applicable SOW, if any, except as otherwise agreed to in this Agreement, the applicable SOW, or in writing by the Parties.
- a) **Information Security Program.** Supplier will implement, maintain, monitor and, where necessary, update an Information Security Program that will include the measures listed in the Security Standards attached hereto as Appendix 1.
- b) **Data Integrity.** Supplier will ensure that all Personal Data created or maintained by Supplier on Company's behalf is accurate and, where appropriate, kept up to date, and will erase or rectify inaccurate or incomplete Personal Data in accordance with Company's instructions.
- c) **Cross-Border Transfers.** Supplier will ensure that Personal Data is not physically transferred to, accessed by or otherwise processed by its Supplier Personnel in any country other than those specified in the applicable SOW, if specified, unless Company agrees in writing. If applicable, at Company's request, Supplier (and if relevant, Supplier's affiliates or subcontractors) will enter into an appropriate data processing agreement that incorporates the European Commission Standard Contractual Clauses between Controllers and Processors, or any similar agreement relating to other countries, with Company to allow Company's international offices to transfer Personal Data to Supplier or such affiliates and/or subcontractors.
- d) **Subcontracting.** Notwithstanding, and expressly in limitation of, anything to the contrary in the Agreement, Supplier will not disclose or transfer Personal Data to, or allow access to Personal Data by, (each, a "**Disclosure**") any third party without Company's express prior written consent; *provided*, however, that Supplier may Disclose Personal Data to its affiliates and subcontractors for purposes of providing the Services to Company, subject to the following conditions: (i) Supplier will maintain a list of the affiliates and subcontractors to which it makes such Disclosures and will provide this list to Company upon Company's request; (ii) Supplier will provide Company at least 30 days' prior notice of the addition of any affiliate or subcontractor to this list and the opportunity to object to such addition(s); and (iii) if Company makes such an objection on reasonable grounds and Supplier is unable to modify the Services to prevent

Disclosure of Personal Data to the additional affiliate or subcontractor, Company will have the right to terminate the relevant Processing. Supplier will, prior to any Disclosure, ensure that such third party is bound by contractual obligations that are at least as restrictive as this Exhibit. A copy of such contractual obligations will be provided to Company upon request. Supplier will be liable for all actions by such third parties with respect to such Personal Data so Disclosed.

- e) **Requests or Complaints from Individuals.** Supplier will notify Company in writing, without undue delay (and in any event within 24 hours), unless specifically prohibited by laws applicable to Supplier, if Supplier receives: (i) any requests from an individual with respect to Personal Data Processed by or on behalf of Supplier, such as opt-out requests, requests for access and/or rectification, erasure, restriction, requests for data portability, and all similar requests; or (ii) any complaint relating to the Processing of Personal Data, including allegations that the Processing infringes on an individual's rights. Supplier (i) will not respond to any such request or complaint unless expressly authorized to do so by Company, (ii) will cooperate with Company with respect to any action taken relating to such request or complaint, whether received by Supplier or Company, and (iii) will implement appropriate processes (including technical and organizational measures) to assist Company in responding to requests or complaints from individuals.
- f) **Audit.** Supplier will provide to Company, its authorized representatives, and such independent inspection body as Company may appoint, for the purpose of auditing Supplier's compliance with its obligations under this Exhibit, on reasonable notice: (i) access to Supplier's information, processing premises, and records; (ii) reasonable assistance and cooperation of Supplier Personnel; and (iii) reasonable facilities at Supplier's premises.
- g) **Regulatory Investigations.** Upon request by Company, Supplier will assist and support Company in the event of an investigation by any regulator or authority, including a data protection authority, if and to the extent that such investigation relates to Personal Data Processed by Supplier on Company's behalf in accordance with this Exhibit.
- h) **Security Incident.** Supplier will notify Company in writing without undue delay (and in any event within 24 hours) whenever Supplier reasonably believes a Security Incident has occurred. After providing notice, Supplier will investigate the Security Incident, take all necessary steps to eliminate or contain the exposure of the Personal Data, and keep Company informed of the status of the Security Incident and all related matters. Supplier further agrees to provide reasonable assistance and cooperation requested by Company and/or Company's designated representatives, in the furtherance of any correction, remediation or investigation of any Security Incident and the mitigation of any potential damage, including any notification that Company may determine appropriate to send to affected individuals, regulators or third parties, and/or the provision of any credit reporting service that Company deems appropriate to provide to affected individuals. Supplier will be responsible for all costs associated with such activities and will reimburse Company for the reasonable cost of notification to affected individuals, fielding feedback and questions from those notified, and any other reasonable associated costs that Company may incur in connection with responding to or managing the Security Incident, including, for example, costs relating to obtaining contact information for affected individuals, attorney's fees and legal costs, call center services and forensics services, credit monitoring, and other remediation costs. Unless

required by law applicable to Supplier, Supplier will not notify any individual or any third party other than law enforcement of any potential Security Incident involving Personal Data in any manner that would identify, or is reasonably likely to identify or reveal the identity of, Company, without first obtaining written permission of Company.

- i) **Return or Disposal of Personal Data.** Upon termination or expiration of its obligations under this Agreement or upon request of Company, whichever comes first, Supplier shall (i) cease all Processing of and return to Company or, at the written request of Company, securely dispose of or securely destroy all Personal Data in the custody and control of the Supplier (or agents or subcontractors, as applicable), in each case using appropriate physical, administrative and technical safeguards to protect such Personal Data against loss, theft and unauthorized access, disclosure, copying, use, or modification, and (ii) certify to Company, in writing, that Supplier has complied with its obligations under this Section.
- j) **Assistance.** Supplier will provide appropriate information and assistance requested by Company to demonstrate Supplier's compliance with its obligations under this Exhibit and assist Company in meeting its obligations under Applicable Privacy Laws regarding: (i) registration and notification; (ii) ensuring the security of the Personal Data; and (iii) carrying out privacy and data protection impact assessments and related consultations with data protection authorities. In addition, when Supplier is responding to Company's requests, Supplier will inform Company if Supplier believes that any Company instructions regarding the Processing of Personal Data would violate applicable law.
- k) **Cardholder Information.** If Supplier has access to Cardholder Information, Supplier must at all times comply with the security standards for the protection of Cardholder Information, with which payment card companies require merchants to comply, such as the Payment Card Industry Data Security Standards currently in effect and as may be updated from time to time ("**PCI Standards**"). Supplier will promptly provide, at Company's request, current certification of compliance with the PCI Standards by an authority recognized by the payment card industry for that purpose. If, during the term of this Agreement, Supplier undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI Standards, Supplier will promptly notify Company in writing of such circumstances. Supplier will not take any actions that would compromise Company's ability to comply with the PCI Standards.

1) AMENDMENT. In the event that this Exhibit, or any actions to be taken or contemplated to be taken in performance of this Exhibit, do not or would not satisfy either party's obligations under Applicable Privacy Laws, the parties will negotiate in good faith to execute an appropriate amendment to this Exhibit.

2) INDEMNIFICATION. Without limitation on any other indemnification obligations set forth in this Agreement, Supplier hereby agrees to defend, indemnify and hold Company and its subsidiaries, and their respective employees, directors, officers, agents and equity holders, harmless from and against any and all Claims that arise out of a Security Incident. Further, Supplier hereby agrees to defend, indemnify and hold Company and its subsidiaries, and their respective employees, directors, officers,

agents and equity holders, harmless from and against any and all Claims that arise out of a breach of the representations and warranties contained in Section 6 of this Exhibit.

- 3) **SURVIVAL.** The obligations of Supplier under this Exhibit will continue for so long as Supplier continues to Process or possess Personal Data, even if all agreements between Supplier and Company have expired or have been terminated.

- 4) **PERSONAL DATA PROVIDED BY SUPPLIER.** As part of the Services provided under this Agreement, Supplier may provide Company with Personal Data. Supplier represents and warrants that: (a) it has collected all such Personal Data in compliance with all applicable laws; (b) where required by law, it has provided notices to and received consents from individuals and that such notices or consents include the intended uses or disclosures of the Personal Data under this Agreement (including Processing by the Company for direct marketing to individuals); and (c) its sharing of Personal Data with Company and Company's use of Personal Data in accordance with the terms of this Agreement will not violate any Applicable Privacy Laws.

APPENDIX 1

SECURITY STANDARDS

At a minimum, Supplier will take the security measures set forth in this Appendix.

1. **Physical Control Access /Physical Security.** Supplier will take industry standard steps designed to prevent unauthorized persons from gaining access to Personal Data processing systems by maintaining industry standard physical security controls at all Supplier sites at which an information system that uses or houses Personal Data is located.
2. **Logical/Data Access Control.** Supplier will maintain appropriate access controls designed to prevent Personal Data processing systems from being used without proper authorization, including:
 - a) restricting access to Personal Data to only authorized Supplier Personnel who require such access in order to perform the Services and providing the lowest level of access required in accordance with the “least privilege” approach and to the minimum number; and
 - b) implementing industry standard physical and electronic security measures to protect passwords or other access controls.

Further, Supplier will:

- c) Maintain user administration procedures: define user roles and their privileges; define how access is granted, changed and terminated; address appropriate segregation of duties; and define the logging/monitoring requirements and mechanisms; and
 - d) Ensure that all employees of Supplier and its subcontractors are assigned unique User-IDs.
3. **Data Transfer Control/Network Security.** Supplier will ensure that: (a) Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control). Supplier will maintain network security using industry standard equipment and industry standard techniques, including firewalls, intrusion detection and prevention systems, and routing protocols; (b) it utilizes industry standard anti-virus and malware protection software to protect Personal Data from anticipated threats or hazards and protect against unauthorized access to or use; and (c) it utilizes industry-standard encryption tools (not less than 128-bit key utilizing an encryption method approved by Company) and other secure technologies in connection with any and all Personal Data that Supplier: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or storage media; or (iii) stores on portable devices, where technically feasible (including safeguarding the security and confidentiality of all encryption keys associated with encrypted Sensitive Personal Data).

4. **Availability Control/Separation Control.** Supplier will implement appropriate policies and procedures to ensure that: (a) it Processes Personal Data in accordance with Company's instructions; (b) it Processes separately Personal Data collected for different purposes; and (c) Personal Data is protected against accidental destruction or loss.

5. **Organizational Security.**
 - a) Supplier will maintain security policies and procedures to classify sensitive or confidential information, clarify security responsibilities and promote awareness for employees by, among other things: (i) maintaining adequate procedures regarding the use, archiving, or disposal of media containing Personal Data; and (ii) managing Security Incidents in accordance with appropriate incident response procedures.
 - b) Prior to providing access to Personal Data to Supplier personnel, Supplier will require Supplier personnel to comply with its Information Security Program.
 - c) Supplier will maintain a security awareness program to train personnel about their security obligations. This program will include training about data classification obligations, physical security controls, security practices, and security incident reporting.
 - d) Supplier will maintain procedures such that (i) when media are to be disposed of or reused, any subsequent retrieval of any Personal Data stored on them before they are withdrawn from the inventory will be prevented; and (ii) when media are to leave the premises at which the files are located as a result of maintenance operations, any undue retrieval of Personal Information stored on them will be prevented.

6. **Business Continuity.** Supplier will maintain appropriate back-up, disaster recovery and business resumption plans, business continuity plan and risk assessment, and review and test these plans regularly to ensure that they are up to date and effective. Supplier will maintain procedures for reconstructing lost Personal Data in Supplier's possession or under Supplier's control, and correct, at Company's request, any destruction, loss or alteration of any of Personal Data caused by Supplier, or arising out of Supplier's breach of this Agreement.

7. **Security Manager.** Supplier will designate an employee ("Security Manager") who will be responsible for managing and coordinating the performance of Supplier's obligations set forth in its Information Security Program and in this Exhibit.

8. **Risk Assessments.** Supplier will conduct periodic risk assessments and reviews and, as appropriate, update its Information Security Program; *provided* that Supplier will not modify its Information Security Program in a manner that would weaken or compromise the confidentiality, availability or integrity of Personal Data.

EXHIBIT B

CLASSIFICATION OF TREATMENT NEEDS*

- Class I. No Visible Dental Problems
- Individuals apparently require no dental treatment related to the type of visual examination or inspection performed.
- Class II. Mild Dental Problems
- Individuals requiring treatment but not of an urgent nature, such as:
- a. Dental caries: Pinhead size cavities, not generalized or advanced.
 - b. Gingivitis: red, puffy or tender gums in localized areas, not extensive.
 - c. Moderate plaque and calculus accumulation: oral prophylaxis recommended. (see interpretation sheet)
 - d. Other oral conditions requiring corrective or preventive measures.
- Class III. Severe Dental Problems
- Individuals requiring early treatment of such conditions as:
- a. Dental caries: appearance of large cavities the size of small green pea and/or extensive pinhead cavities.
 - b. Gingivitis/periodontal disease: extensive gingival inflammation, bleeding gums.
 - c. Chronic abscess(es).
 - d. Chronic oral infection.
 - e. Heavy calculus accumulation.
 - f. Insufficient number of teeth for mastication.
- Class IV. Emergency Dental Treatment Required
- Individuals requiring emergency dental treatment for such conditions as:
- a. Injuries.
 - b. Acute oral infections (periodontal and periapical abscesses, Vincent's infection, acute stomatitis, etc.)
 - c. Painful conditions
- Orthodontic Problems

Refer a child to the dentist or orthodontist if severe or if the child appears not to have seen a dentist.

*Source: American Dental Association, "Official Policies of the American Dental Association on Dental Health Programs". Chicago, 1957.