INFORMATION SECURITY PROGRAM AND POLICY

Kayaku Advanced Materials, Inc., a Massachusetts corporation operating in the Commonwealth of Massachusetts ("KAM"), is committed to safeguarding Personal Information provided to it by individuals irrespective of the manner in which such Personal Information is provided, transmitted, recorded, or stored. All employees (full time, part time, temporary, and contract, collectively, "Employees") are required to maintain the security and confidentiality of such information and to abide by all of the requirements of this Policy. This Policy is designed to comply with the Standards for the Protection of Personal Information of Residents of The Commonwealth, 201 CMR 17 ("Personal Privacy Regulation").

Section 1. Personal Information.

(a) As used in this Policy, the term "Personal Information" means an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual:

(i) social security number;

(ii) driver's license number or state-issued identification card number;

(iii) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to resident's financial account; or

(iv) any information recording or registering any individual's unique biological attribute or measurement that can be used to authenticate the identity of the individual including, without limitation, fingerprints, genetic information, iris or retina patterns, voice recognition, facial characteristics, or hand geometry.

(b) We have evaluated our operations, the limited ways in which we collect and use Personal Information, and determined that we are in a low risk category. We collect Personal Information through various forms or electronic communication for the purpose of the following:

(i) to administer payroll and reimbursements, provide historic information for Employee files, provide Employee benefits, and for contact purposes;

(ii) to issue W-2, 1099, and other tax reports and statements;

(iii) to document the expenditure of monies for supplies and services on behalf of the company and for audit purposes; and

(iv) to generate invoices for goods and services provided to external clients and to conduct collection activities.

Section 2. Administration of this Policy.

(a) The Board of Directors of KAM is charged with the ultimate authority over this Policy, but may delegate any authority and responsibilities to a committee of the Board at any time and from time to time. KAM's President will appoint a Privacy Manager who will periodically report on matters arising under this Policy and its implementation and enforcement to the President and the Board. The President or Privacy Manager may, in their respective discretion or at the request of the Board of Directors, bring to the attention of the Board of Directors matters arising under this Policy and its implementation and enforcement.

(b) The Privacy Manager shall have the general day-to-day authority to administer, enforce, maintain, answer questions about, and ensure compliance with the Policy. Notwithstanding any provision of this Policy, all actions of the Privacy Manager shall remain subject to President and Board review and change.

(c) The Privacy Manager shall monitor the Policy and security measures under the Policy to ensure that the Policy is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Personal Information.

(d) The Privacy Manager shall review the scope of the Policy and the security measures under the Policy at least annually and whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing Personal Information. The Privacy Manager shall be responsible for identifying internal and external risks to security, and detect and prevent security system failures, make recommendations for resolving these problems, and implement or cause to be implemented solutions to address those risks.

(e) The Privacy Manager shall make recommendations to the President as to changes and improvements to the Policy, but is authorized to act in advance of any formal corporate action to upgrade procedures and safeguards as necessary to limit risks.

(f) All Employees are directed to report in writing any breach of security to the Privacy Manager forthwith after discovering such breach. The Privacy Manager shall be charged with investigating any breach of security, identifying corrective or other measures in response, and implementing all such measures in order to ensure the protection of Personal Information. The Privacy Manager shall provide reports of any such breaches to the President and the recommendations made, and measures taken, in response thereto. KAM, by action of its Board of Directors, shall comply with all laws applicable to the reporting of security breaches involving Personal Information or the unauthorized use or accessing of Personal Information.

Section 3. Safeguarding Personal Information.

We take measures to safeguard personal records through the measures listed below.

(a) We do not collect the social security numbers from employment application forms, and, as described below, safeguard all forms such as payroll, tax, and benefit forms which require social security numbers.

(b) We designate specific Employees to handle Personal Information needed to process payroll, cash receipts, and vendor payments, generate invoices and tax forms, and collection activities.

(c) We designate a limited-access facsimile machine for the receipt and transmission of all documents containing Personal Information.

(d) We lock up documents containing Personal Information in file cabinets and a storage room with a locked door. No keys are available to Employees to access these files except authorized personnel.

(e) We conduct training for all Employees regarding the importance of Personal Information security, the Personal Privacy Regulation, and this Policy.

(f) We instruct Employees that Personal Information should never be discussed in a public setting.

(g) We do not share the Personal Information obtained with external/outside party use, except the providers with which we contract to administer the company payroll, benefits, and financial activities.

(h) We do not sell Personal Information.

Section 4. Electronic and Wireless Data Security.

(a) KAM restricts access to electronic data to authorized users only. Such restrictions allow access to files containing Personal Information only to users with a need to access such information in order to perform their job duties as determined by KAM management.

(b) Access to all electronically stored Personal Information is granted through the assignment of unique individual user accounts which are password protected. No two user accounts are identical. User accounts are promptly disabled at the termination of the employer-employee relationship.

(c) Accounts are systematically forced to change their passwords on initial login and subsequently every 180 days. Password rules enforce the use of complex passwords, prevent the use of certain obvious words, and prevent the reuse/renewal of the last three previous passwords.

(d) User accounts will lock-out after 5 incorrect login attempts and will remain locked out for 30 minutes.

(e) User accounts logged in but inactive for more than 10 minutes will lock and require reauthentication to regain access to the login session.

(f) Master IT passwords are stored centrally with tightly controlled access only to users who require such access to perform their job duties.

(g) To access corporate email via a mobile device, each user requires a unique password. The password must be updated every 90 days.

(h) Remote access to the network is allowed for a subset of Employees. This access is controlled via unique VPN accounts which are promptly disabled at the termination of the employer-employee relationship.

Section 5. Network Security.

(a) All applications and operating systems and configurations are updated on a regular basis to protect against newly discovered security risks.

(b) All PCs and servers are running an up-to-date antivirus and malware application.

(c) All IT equipment/software vendor default passwords are changed.

(d) No computer is allowed access to the corporate network without being configured/reviewed by the corporate IT department for compliance with these and other corporate IT standards.

(e) All backups containing Personal Information are done electronically through uploads to the cloud and are encrypted.

(f) All Personal Information stored on corporate laptops and other mobile devices is encrypted.

(g) All records and data containing Personal Information transmitted across public networks or wirelessly are encrypted.

Section 6. Email Security.

(a) Employees must:

(i) select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information;

(ii) remember passwords instead of writing them down and keep them secret;

(iii) change their email password every six months;

(iv) be vigilant for emails that carry malware or phishing attempts;

(v) avoid opening email attachments and clicking on email links when content is not adequately explained;

(vi) be suspicious of clickbait titles;

(vii) check email and names of unknown senders to ensure they are legitimate;

(viii) look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks); and

(ix) if an Employee is unsure about the safety of an email, the Employee should contact the Privacy Manager.

(b) The Privacy Manager will confirm that anti-spam and anti-malware programs are in place and are routinely updated.

Section 7. Disposal of Records

(a) For any records which are no longer required to be kept in accordance with KAM's retention policy, then any such records which contain Personal Information must be disposed of in one of the following manners:

(i) paper documents shall be either redacted, burned, pulverized, or shredded so that Personal Information can no longer be read, reconstructed, or recovered; or

(ii) electronic media and other non-paper media shall be destroyed or erased in such a manner so that Personal Information can no longer be read, reconstructed, or recovered.

(b) KAM may contract with a third party to dispose of any records, including records containing Personal Information, provided that such third party is vetted in accordance with the policies of the following section.

Section 8. Contract Management

(a) For any outside venders which have access to personal information such as to administer payroll, benefits, and financial activities, we use only reputable and qualified firms. Before engaging any such outside vendor, we (1) obtain and review the privacy and cybersecurity, as appropriate, policies and procedures of those outside vendors and (2) require such outside vendors by contract with us to implement and maintain appropriate security measures for handling Personal Information.

(b) Specifically, when negotiating a new contract with an outside vendor who or which will store, maintain, or have access to Personal Information, the outside vendor must have policies, procedures, and safeguards in place to satisfy all requirements of the Personal Privacy Regulation, laws applicable to the disposal of records containing Personal Information, and laws with respect to the reporting of breaches of such laws and regulations, and must meet all such other standards as may be set from time to time by the Board of Directors, the President, and the Privacy Manager.

Section 9. Breach of Policy

We restrict access to Personal Information to those Employees who need to know it in order to operate our business. All Employees are required to maintain the integrity and confidentially of Personal Information in accordance with this Policy and any confidentiality agreement to which the Employee may be a party. When a breach of this Policy occurs, an

incident report will be presented to the President by the Privacy Manager. The President will bring the matter to the attention of the Board of Directors if appropriate. The Employee involved may be subject to discipline up to and including termination and criminal prosecution if such Employee failed to meet the standards required by this Policy or the Personal Privacy Regulation.

Section 10. Other Confidential Information

This Policy is intended to comply with the Personal Privacy Regulation. Nevertheless, it is KAM policy that all confidential information about KAM, its customers, and the users of KAM products and services should be maintained and protected by KAM and its Employees with the same care as Personal Information. All such confidential information must be used only for purposes directly related to the operations of KAM or the provision of KAM products and services to KAM customers and the users of KAM products and services. For the avoidance of doubt, the foregoing applies to KAM's contractors and to arrangements pursuant to which KAM's products or services are provided indirectly or hosted by third parties. KAM shall take all action it deems necessary and appropriate from time to time to enforce these restrictions and limitations including, without limitation, conducting investigations and taking disciplinary or other action against anyone violating this Policy.

END OF POLICY