Plume

CANADA - PRIVACY AND DATA SECURITY ADDENDUM

Whereas this Privacy and Data Security Addendum (the "**Addendum**") amends and forms part of the written agreement between Plume Design, Inc. ("**Plume**") and [vendor's name] ("**Vendor**") dated as of [date of the Agreement] (the "**Agreement**"), which involves the provision of services by the Vendor as described in the Agreement (the "**Services**");

Whereas Vendor processes, transmits, and/or stores Plume Personal Information (as defined below) in the performance of the Services provided to Plume;

Whereas Plume is subject to data protection laws including the *Personal Information Protection and Electronic Documents Act* pursuant to which it is responsible for the protection of the Plume Personal Information when it is transferred or made available to Vendor for processing; and

Whereas to comply with such laws, Plume must enter into a written agreement with Vendor that includes an acknowledgement that Vendor will collect, use and disclose the Plume Personal Information to provide the Services under the Agreement and that Vendor is responsible for the security of any Plume Personal Information that may be obtained when providing the Services to the Plume.

It is hereby agreed that:

1. Plume Personal Information

For the purposes of this Addendum, "**Plume Personal Information**" includes any information relating to an identified or identifiable individual, regardless of the media in which it is contained, that may be disclosed to or accessed by Vendor in connection with the Services.

2. Privacy and Access Requests

(a) Compliance with Privacy Laws. Vendor shall comply with (i) all applicable legal requirements (federal, state, provincial, local and international laws, rules and regulations and governmental requirements) currently in effect and as they become effective, relating in any way to the privacy, confidentiality or security of Plume Personal Information, including but not limited to the *Personal Information Protection and Electronic Documents Act* (Canada), as amended or supplemented from time to time, and any other applicable law now in force or that may in the future come into force governing the collection, use, disclosure and protection of personal information applicable to either party or to any information collected, used or disclosed in the course of providing or receiving the Services; (ii) all applicable industry standards concerning privacy, data protection, confidentiality or information security; and (iii) applicable privacy policies, statements or notices that are provided to Vendor by Plume in writing, including the Plume Privacy Policy available on Plume's website, as may be amended from time to time.

(b) Limitation on use; ownership. Any use of Plume Personal Information by Vendor shall be limited to the sole purpose expressly authorized by the Agreement (i.e. providing the Services). Any Plume Personal Information, including in any reconfigured format, shall at all times be and remain the sole property of Plume, unless agreed otherwise in writing by Plume.

(c) Limitation on transfer. Vendor shall not share, transfer, disclose or otherwise provide access to any Plume Personal Information to any third party unless Plume has authorized Vendor to do so in writing.

Vendor will ensure that any third party it may authorize to perform any of the Services shall be obligated to have a Security Program equivalent to that required by Plume (which includes all terms of this Addendum). Further, Vendor must ensure by way of a written agreement with its authorized service

providers that they will only use and process Plume Personal Information for the purposes set forth in the Agreement and in accordance with the obligations and restrictions set forth in this Addendum. Vendor will be liable for compliance of its service providers with such obligations and restrictions. Additionally, regarding any Personal Information Incident (as this term is defined in section 3(e)), Vendor shall contractually preserve for itself – or Plume – all such rights as Vendor has under section 4 and enforce such rights at Plume's request for Plume's benefit. Regarding audit rights, Plume shall contractually preserve for itself, or Plume, all such rights as Plume has under section 5 below and enforce such rights at Plume's request for Plume's benefit. Vendor shall only retain third parties that are capable of performing the delegated obligations in accordance with this Addendum.

(d) Cross-border Transfers. Unless expressly authorized by Plume, Vendor shall not store Plume Personal Information outside Canada and shall not transfer or otherwise provide access to Plume Personal Information to any person, albeit Vendor's affiliate or subsidiary, outside Canada.

(e) De-identified Information. If Plume provides Vendor with any aggregated, statistical, anonymized and/or de-identified information derived from Personal Information ("**De-identified Information**") or if Plume allows Vendor to derive De-identified Information from the Plume Personal Information, Vendor shall not make any attempts at re-identifying the De-identified Information. Without limiting the generality of the foregoing, Vendor shall take all necessary measures to avoid the re-identification of the De-identified Information, including: (a) not bringing any other data in the environment of the De-identified Information in order to avoid increasing the risk of re-identification by linkage; (b) destroying any accidentally re-identified Plume Personal Information and informing Plume of any cases of re-identified Plume Personal Information; (c) not disclosing the De-identified Information to any third-party, unless as authorized by Plume.

(f) Individuals' Access and Correction Requests under Privacy Laws. If Vendor receives an individual's request for access to or correction of Personal Information under applicable privacy laws, Vendor shall promptly, and no later than two business days after the receipt of such request, redirect the individual to Plume, notify Plume of all the details about the request in writing, and assist Plume in responding to such request, if applicable.

(g) Notice of Process. In the event Vendor receives a governmental or other regulatory request for any Plume Personal Information, it agrees to immediately, and no later than one business day after the receipt of such request, notify Plume to allow Plume to have the option to defend or answer such request. Vendor shall reasonably cooperate with Plume in such defense or answer.

3. Data Security Program

Vendor shall maintain a comprehensive, written information security program that contains administrative, technical, and physical safeguards that are appropriate to the size, scope and type of Vendor's business, the amount of resources available to Vendor, the type of information that Vendor will store and the need for security and confidentiality of such information ("**Security Program**"). Vendor's Security Program shall be designed to: (a) protect the confidentiality, integrity, and availability of Plume Personal Information in Vendor's possession or control or to which Vendor has access; (b) protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Plume Personal Information; (c) protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Plume Personal Information; (d) protect against accidental loss or destruction of, or damage to, Plume Personal Information; and (e) safeguard Plume Personal Information in compliance with applicable laws, as set forth in section 2.(a).

Without limiting the generality of the foregoing, Vendor's Security Program must include:

(a) Security Awareness and Training. A mandatory annual security awareness and training program for all members of Vendor's workforce (including management), which includes: (i) training on how to implement and comply with its Security Program; and (ii) promoting a culture of security awareness through periodic communications from senior management with employees.

(b) Background Assessment and Monitoring. Policies and procedures to conduct background assessments for all current and prospective members of Vendor's workforce who have access to Plume Personal Information including criminal background verification procedures. Such assessments shall be performed annually to ensure members of Vendor's workforce continue to comply with applicable standards and requirements related thereto.

(c) Access Controls. Policies, procedures, and logical controls: (i) to limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons with a genuine need-to-know; (ii) to ensure that the least amount of Plume Personal Information is made accessible to authorized persons as required to carry out their job-related functions; (iii) to prevent those workforce members and others who should not have access from obtaining access; and (iv) to remove access in a timely manner in the event of a change in job responsibilities or job status or as a result of a failed background assessment. These policies, procedures and logical controls include the use of multi-factor authentication and the implementation of a password policy guaranteeing that passwords are periodically updated and are of a reasonable level of complexity.

(d) Physical and Environmental Security. Controls that provide reasonable assurance that physical access to facilities where Plume Personal Information is stored, including physical servers, is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes. These controls include: (i) logging and monitoring of unauthorized access attempts to Vendor's facilities by security personnel; (ii) camera surveillance systems at critical internal and external entry points of Vendor's facilities; (iii) systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and (d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

(e) Personal Information Incident Procedures. A Personal Information Incident response plan that includes procedures to be followed in the event of any actual or reasonably suspected unauthorized use of, loss of, access to or disclosure of Plume Personal Information (an actual unauthorized use of, loss of, access to or disclosure of Plume Personal Information shall be referred to as a "**Personal Information Incident**"). Such procedures include: (i) formation of an internal incident response team with a response leader; (ii) assessing the risk the incident poses and determining what data was affected, and in particular whether Plume Personal Information has been affected; (iii) internal reporting as well as a notification process in the event of unauthorized disclosure of Plume Personal Information; (iv) keeping a record of what was done and by whom to help in later analysis and possible legal action; and (v) conducting and documenting root cause analysis and remediation plan.

(f) Contingence Planning. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Plume Personal Information or production systems that contain Plume Personal Information. Such procedures include: (i) a policy for performing periodic backups of production file systems and databases containing Plume Personal Information, according to a defined schedule; (ii) a formal disaster recovery plan for Vendor's facilities where Plume Personal Information is stored, including requirements for the disaster plan to be tested on a regular basis and a documented executive summary of the Disaster Recovery testing, at least annually, which is available to Plume upon request to Vendor; (iii) a formal process to

address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

(g) Audit Controls. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information. Such mechanisms must ensure that actions are attributable to an identifiable individual.

(h) Data Integrity. Policies and procedures to ensure the confidentiality, integrity, and availability of Plume Personal Information and protect it from disclosure, improper alteration, or destruction.

(i) Storage and Transmission Security. Security measures to guard against unauthorized access to Plume Personal Information that is being transmitted over a public electronic communications network or stored electronically. Such measures include (i) limiting the use of portable storage devices, such as USB (Universal Serial Bus) drives, to store or transfer Plume Personal Information to the extent demonstrably necessary to fulfill a specific and documented purpose; and (ii) requiring encryption of any Plume Personal Information stored on desktops, laptops or other removable storage devices.

(j) Segmentation. Measures ensuring the segmentation of Plume Personal Information from data of others.

(k) Assigned Security Responsibility. Assigning responsibility for the development, implementation, and maintenance of its Information Security Program, including: (i) designating a security official with overall responsibility; and (ii) defining security roles and responsibilities for individuals with security responsibilities.

(l) Testing. Regularly testing the key controls, systems and procedures of its Security Program to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing must be performed annually by an independent external firm. Where applicable, such testing includes: (i) internal risk assessments; (ii) ISO 27001 and ISO 27018 certifications; and (iii) Service Organization Control 1 (SOC1) and Service Organization Control 2 (SOC2) audit reports (or industry-standard successor reports);

(m) Logging and Monitoring. Active network and systems logging and monitoring, including error logs on servers, disks and security events for any potential problems. Such logging and monitoring includes: (i) reviewing changes affecting systems handling authentication, authorization, and auditing; (ii) reviewing privileged access to Vendor's production systems at regular intervals; and (iii) engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

(n) Change and Configuration Management. Maintaining policies and procedures for managing changes Vendor makes to production systems, applications, and databases. Such policies and procedures must include: (i) a process for documenting, testing and approving the patching and maintenance of the Service; (ii) a security patching process that requires patching systems in a timely manner based on a risk analysis; and (iii) a process for Vendor to utilize a third party to conduct web application level security assessments.

(o) Program Adjustments. Vendor must monitor, evaluate, and adjust, as appropriate, the Security Program in light of: (i) any relevant changes in technology and any internal or external threats to Vendor, the Plume Personal Information; (ii) security and data privacy regulations applicable to Vendor; and (iii) Vendor's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(p) Devices. All laptop and desktop computing devices utilized by Vendor and any subcontractors when accessing Personal Information must: (i) be equipped with a minimum of AES 128 bit full hard disk drive encryption; (ii) have up to date virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and (iii) maintain virus and malware detection and prevention software so as to remain on a supported release. This shall include, but not be limited to, promptly implementing any applicable security-related enhancement or fix made available by the supplier of such software.

4. Liability and Personal Information Incidents

(a) No Limitation of Liability. Notwithstanding anything to the contrary in the Agreement, no limitation of liability shall apply in the case of any claims, demands, actions or proceedings brought against Plume as a result of Vendor's breach of any obligation under this Addendum.

(b) Indemnification. Vendor's obligations in the Agreement with respect to indemnification shall extend to any claims, demands, actions or proceedings brought against Plume as a result of Vendor's breach of any obligation under this Addendum.

(c) Informing Plume of Personal Information Incident. Vendor shall immediately, and no later than twenty-four hours after becoming aware of any reasonably suspected or actual Personal Information Incident, inform Plume about such Personal Information Incident. The notice shall summarize in reasonable detail the nature and scope of the Personal Information Incident (including each data element) and the corrective action already taken or to be taken by Vendor.

While the initial notice may be in summary form, a comprehensive written notice shall be given to Plume. The notice shall be timely supplemented in the detail reasonably requested by Plume, inclusive of relevant forensic reports. Vendor shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with Plume in all reasonable efforts to mitigate the adverse effects of the Personal Information Incident and to prevent its recurrence.

(d) Notice of Personal Information Incident. The parties will collaborate on whether any notice of the Personal Information Incident is required to be given to any person, and if so, the content of that notice.

If Plume reasonably determines that the Personal Information Incident is likely to have substantial adverse impact on Plume's relationship with its customers or associates or otherwise substantially harm its reputation, Plume may suspend the services provided by Vendor under the Agreement or any other contract.

(e) Liability for Personal Information Incident. Without limiting the generality of the foregoing, in the event of any Personal Information Incident, Vendor shall pay the reasonable and documented costs incurred by Plume in connection with the following items: (a) costs of any required forensic investigation to determine the cause of the Personal Information Incident; (b) providing notification of the Personal Information Incident to applicable government and relevant industry self-regulatory agencies, to the media (if required by applicable law) and to individuals whose Personal Information may have been impacted by the Personal Information Incident; (c) providing credit monitoring service to individuals whose Plume Personal Information may have been impacted by the Personal Information Incident for a period of two years after the date on which such individuals were notified of the Personal Information Incident for individuals who elected such credit monitoring service; (d) operating a call center to respond to questions from individuals whose Personal Information may have been impacted by the Personal Information Incident for a period of one year after the date on which such individuals were notified of the Personal Information Incident; and (e) defending a class action brought by the individuals whose Plume Personal Information may have been impacted by the Personal Information Incident and paying any damages awarded by a court in the context of such class action or any settlement amount.

5. Security Review and Audit

(a) Plume may conduct a security review of Vendor's Security Program when determined reasonably required by Plume.

(b) At Plume's request, Vendor will provide Plume copies of its data privacy and security policies and procedures including the Security Program that apply to Plume Personal Information. Subject to

reasonable notice, Vendor shall provide Plume an opportunity to conduct a privacy and security audit of Vendor's Security Program and systems and procedures that are applicable to the Services. Such audit may be conducted on-site by Plume personnel or Plume's contracted third party assessors or through surveys and interviews, at the option of Plume.

(c) In the event Vendor has any security audits or reviews of its own systems, performed by Vendor or a third party, including vulnerability and penetration assessments, it will give Plume notice of any current findings that are likely to adversely impact Plume Personal Information, and will keep Plume timely informed of its remediation efforts.

6. Interpretation, Termination and Secure Disposition

(a) This Addendum shall be an integral part of the Agreement and constitute, with the Agreement, the entire agreement between the parties with respect to the subject matter thereof, and any prior representations, statements, and agreements relating thereto are superseded by the terms of the Agreement. In the event of any inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement, this Addendum shall take precedence over the Agreement or any other agreements.

(b) Vendor shall either return or dispose of Plume Personal Information if no longer needed for Plume's business or legal purposes or upon contract termination or upon Plume's direction which may be given at any time. Any disposal must ensure that Plume Personal Information is rendered permanently unreadable and unrecoverable. Upon reasonable notice and if requested by Plume, Vendor shall provide Plume a certification of compliance with this section by an officer.

(c) Provisions in this Addendum that are intended to survive termination will continue in full force and effect after the termination of this Addendum.

IN WITNESS WHEREOF the Plume and Vendor have executed this Agreement attested to by the signatures of their duly authorized officers in that behalf as of the day and year set out above.

PLUME:

By: Vincent Samuel

Name: Vincent Samuel

Title: Head of Data Protection

VENDOR:

By: _____

Name:

Title: